ETSI TS 123 501 V16.5.1 (2020-09)

5G;
System architecture for the 5G System (5GS)
(3GPP TS 23.501 version 16.5.1 Release 16)

Reference
RTS/TSGS-0223501vg51

Keywords
5G

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the Stage 2 system architecture for the 5G System. The 5G System provides data connectivity and services.

This specification covers both roaming and non-roaming scenarios in all aspects, including interworking between 5GS and EPS, mobility within 5GS, QoS, policy control and charging, authentication and in general 5G System wide features e.g. SMS, Location Services, Emergency Services.

ITU-T Recommendation I.130 [11] describes a three-stage method for characterisation of telecommunication services, and ITU-T Recommendation Q.65 [12] defines Stage 2 of the method.

TS 23.502 [3] contains the stage 2 procedures and flows for 5G System and it is a companion specification to this specification.

TS 23.503 [45] contains the stage 2 Policy Control and Charging architecture for 5G System and it is a companion specification to this specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for next generation new services and markets; Stage 1".

[3] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[4] 3GPP TS 23.203: "Policies and Charging control architecture; Stage 2".

[5] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS); Stage 2".

[6] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface: Stage 3".

[7] IETF RFC 7157: "IPv6 Multihoming without Network Address Translation".

[8] IETF RFC 4191: "Default Router Preferences and More-Specific Routes".

[9] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[10] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[11] ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".

[12] ITU-T Recommendation Q.65: "The unified functional methodology for the characterization of services and network capabilities".

[13] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS): Stage 3".

[14] IETF RFC 3736: "Stateless DHCP Service for IPv6".

[15] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[16] 3GPP TS 22.173: "IMS Multimedia Telephony Service and supplementary services; Stage 1".

[17] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station in idle mode".

[18] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS) emergency sessions".

[19] 3GPP TS 23.003: "Numbering, Addressing and Identification".

[20] IETF RFC 7542: "The Network Access Identifier".

[21] 3GPP TS 23.002: "Network Architecture".

[22] 3GPP TS 23.335: "User Data Convergence (UDC); Technical realization and information flows; Stage 2".

[23] 3GPP TS 23.221: "Architectural requirements".

[24] 3GPP TS 22.153: "Multimedia priority service".

[25] 3GPP TS 22.011: "Service Accessibility".

[26] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[27] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description".

[28] 3GPP TS 38.331: "NR; Radio Resource Control (RRC); Protocol Specification".

[29] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[30] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[31] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[32] 3GPP TS 23.214: "Architecture enhancements for control and user plane separation of EPC nodes; Stage 2".

[33] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Service aspects; Service principles".

[34] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[35] 3GPP TS 33.126: "Lawful Interception Requirements".

[36] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[37] 3GPP TS 22.280: "Mission Critical Services Common Requirements (MCCoRe); Stage 1".

[38] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[39] 3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[40] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[41] 3GPP TS 32.240: "Charging management; Charging architecture and principles".

[42] 3GPP TS 38.401: "NG-RAN Architecture description".

[43] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[44] IETF RFC 4960: "Stream Control Transmission Protocol".

[45] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

[46] 3GPP TS 23.041: "Public Warning System".

[47] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[48] 3GPP TS 24.502: "Access to the 5G System (5GS) via non-3GPP access networks; Stage 3".

[49] 3GPP TS 29.500: "5G System; Technical Realization of Service Based Architecture; Stage 3".

[50] 3GPP TS 38.304: "NR; User Equipment (UE) procedures in idle mode".

[51] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[52] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[53] Void.

[54] IETF RFC 4861: "Neighbor Discovery for IP version 6 (IPv6)".

[55] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)".

[56] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[57] IETF RFC 4555: "IKEv2 Mobility and Multihoming Protocol (MOBIKE)".

[58] 3GPP TS 29.510: "5G System: Network function repository services; Stage 3".

[59] 3GPP TS 29.502: "5G System: Session Management Services: Stage 3".

[60] IETF RFC 7296: "Internet Key Exchange Protocol Version 2 (IKEv2) ".

[61] 3GPP TS 23.380: "IMS Restoration Procedures".

[62] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[63] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) centralized services; Stage 2".

[64] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs".

[65] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane Nodes; Stage 3".

[66] 3GPP TS 32.421: "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements".

[67] 3GPP TS 32.290: "5G system; Services, operations and procedures of charging using Service Based Interface (SBI)".

[68] 3GPP TS 32.255: "5G Data connectivity domain charging; Stage 2".

[69] 3GPP TS 38.306: "NR; User Equipment -UE) radio access capabilities".

[70] 3GPP TS 36.306: "Evolved Universal Terrestrial Radio Access -E-UTRA); User Equipment -UE) radio access capabilities".

[71] 3GPP TS 29.518: "5G System; Access and Mobility Management Services; Stage 3".

[72] 3GPP TS 23.285: "Architecture enhancements for V2X services".

[73] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".

[74] IETF RFC 3162: "RADIUS and IPv6".

[75] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[76] 3GPP TS 26.238: "Uplink streaming".

[77] 3GPP TR 26.939: "Guidelines on the Framework for Live Uplink Streaming (FLUS)".

[78] International Telecommunication Union (ITU), Standardization Bureau (TSB): "Operational Bulletin No. 1156"; http://handle.itu.int/11.1002/pub/810cad63-en (retrieved October 5, 2018).

[79] 3GPP TS 28.533: "Management and orchestration; Architecture framework".

[80] 3GPP TS 24.250: "Protocol for Reliable Data Service; Stage 3".

[81] IETF RFC 8684: "TCP Extensions for Multipath Operation with Multiple Addresses".

[82] draft-ietf-tcpm-converters-14: "0-RTT TCP Convert Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[83] IEEE 802.1CB-2017: "IEEE Standard for Local and metropolitan area networks-Frame Replication and Elimination for Reliability".

[84] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[85] WiFi Alliance Technical Committee, Hotspot 2.0 Technical Task Group: "Hotspot 2.0 (Release 2) Technical Specification".

[86] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[87] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[88] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[89] CableLabs DOCSIS MULPI: "Data-Over-Cable Service Interface Specifications DOCSIS 3.1, MAC and Upper Layer Protocols Interface Specification".

[90] BBF TR-124 issue 5: "Functional Requirements for Broadband Residential Gateway Devices".

[91] BBF TR-101 issue 2: "Migration to Ethernet-Based Broadband Aggregation".

[92] BBF TR-178 issue 1: "Multi-service Broadband Network Architecture and Nodal Requirements".

[93] BBF WT-456: "AGF Functional Requirements".

[94] BBF WT-457: "FMIF Functional Requirements".

Editor's note: The references to BBF WT-456 and WT-457 will be revised when finalized by BBF.

[95] IEEE P802.1Qcc: "Standard for Local and metropolitan area networks - Bridges and Bridged Networks - Amendment: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[96] Void.

[97] IEEE Std 802.1AB-2016: "IEEE Standard for Local and metropolitan area networks -- Station and Media Access Control Connectivity Discovery".

[98] IEEE P802.1Q: "Standard for Local and metropolitan area networks--Bridges and Bridged Networks".

[99] 3GPP TS 38.423: "NG-RAN; Xn Application Protocol (XnAP)".

[100] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[101] 3GPP TS 29.274: "Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[102] 3GPP TS 23.632: "User Data Interworking, Coexistence and Migration; stage 2".

[103] 3GPP TS 29.563: "5G System (5GS); HSS services for interworking with UDM; Stage 3".

[104] IEEE Std 802.1AS-Rev/D7.3, August 2018: "IEEE Standard for Local and metropolitan area networks--Timing and Synchronization for Time-Sensitive Applications".

[105] 3GPP TS 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[106] IEEE Std 802.11-2012: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[107] IEEE 1588-2008: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control".

[108] 3GPP TS 28.552: "Management and orchestration; 5G performance measurements".

[109] 3GPP TS 24.193: "Access Traffic Steering, Switching and Splitting; Stage 3".

[110] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".

[111] 3GPP TS 22.186: "Enhancement of 3GPP support for V2X scenarios; Stage 1".

[112] 3GPP TR 38.824: "Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC)".

[113] IEEE: "Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)", https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/tutorials/eui.pdf.

[114] 3GPP TS 32.256: "Charging Management; 5G connection and mobility domain charging; Stage 2".

[115] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[116] 3GPP TS 38.415: "PDU Session User Plane Protocol".

[117] 3GPP TS 24.535: "Device-side Time-Sensitive Networking (TSN) Translator (DS-TT) to network-side TSN Translator (NW-TT) protocol aspects; Stage 3".

[118] 3GPP TS 32.274: "Charging Management; Short Message Service (SMS) charging".

[119] 3GPP TS 23.008: "Organization of subscriber data".

[120] 3GPP TS 38.314: "NR; Layer 2 measurements".

[121] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[122] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

5GLAN Group: A set of UEs using private communication for 5G LAN-type service.

5G Access Network: An access network comprising a NG-RAN and/or non-3GPP AN connecting to a 5G Core Network.

5G Core Network: The core network specified in the present document. It connects to a 5G Access Network.

5G LAN-Type Service: A service over the 5G system offering private communication using IP and/or non-IP type communications.

5G LAN-Virtual Network: A virtual network over the 5G system capable of supporting 5G LAN-type service.

5G QoS Flow: The finest granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receive the same forwarding treatment (e.g. scheduling policy, queue management policy, rate shaping policy, RLC configuration, etc.). Providing different QoS forwarding treatment requires separate 5G QoS Flow.

5G QoS Identifier: A scalar that is used as a reference to a specific QoS forwarding behaviour (e.g. packet loss rate, packet delay budget) to be provided to a 5G QoS Flow. This may be implemented in the access network by the 5QI referencing node specific parameters that control the QoS forwarding treatment (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

5G System: 3GPP system consisting of 5G Access Network (AN), 5G Core Network and UE.

5G-BRG: The 5G-BRG is a 5G-RG defined in BBF.

5G-CRG: The 5G-CRG is a 5G-RG specified in DOCSIS MULPI [89].

5G-RG: A 5G-RG is a RG capable of connecting to 5GC playing the role of a UE with regard to the 5G core. It supports secure element and exchanges N1 signalling with 5GC. The 5G-RG can be either a 5G-BRG or 5G-CRG.

Access Traffic Steering: The procedure that selects an access network for a new data flow and transfers the traffic of this data flow over the selected access network. Access traffic steering is applicable between one 3GPP access and one non-3GPP access.

Access Traffic Switching: The procedure that moves all traffic of an ongoing data flow from one access network to another access network in a way that maintains the continuity of the data flow. Access traffic switching is applicable between one 3GPP access and one non-3GPP access.

Access Traffic Splitting: The procedure that splits the traffic of a data flow across multiple access networks. When traffic splitting is applied to a data flow, some traffic of the data flow is transferred via one access and some other traffic of the same data flow is transferred via another access. Access traffic splitting is applicable between one 3GPP access and one non-3GPP access.

Allowed NSSAI: NSSAI provided by the Serving PLMN during e.g. a Registration procedure, indicating the S-NSSAIs values the UE could use in the Serving PLMN for the current Registration Area.

Allowed Area: Area where the UE is allowed to initiate communication as specified in clause 5.3.2.3.

AMF Region: An AMF Region consists of one or multiple AMF Sets.

AMF Set: An AMF Set consists of some AMFs that serve a given area and Network Slice(s). AMF Set is unique within an AMF Region and it comprises of AMFs that support the same Network Slice(s). Multiple AMF Sets may be defined per AMF Region. The AMF instances in the same AMF Set may be geographically distributed but have access to the same context data.

Application identifier: An identifier that can be mapped to a specific application traffic detection rule.

AUSF Group ID: This refers to one or more AUSF instances managing a specific set of SUPIs. An AUSF Group consists of one or multiple AUSF Sets.

Binding Indication: Information included by a NF service producer to a NF service consumer in request responses or notifications to convey the scope within which selection/reselection of target NF/NF Services may be performed, or information included by the NF service consumer in requests or subscriptions to convey the scope within which selection/reselection of notification targets or the selection of other service(s) that the NF consumer produces for the same data context may be performed. See clause 6.3.1.0.

Configured NSSAI: NSSAI provisioned in the UE applicable to one or more PLMNs.

CHF Group ID: This refers to one or more CHF instances managing a specific set of SUPIs.

Delegated Discovery: This refers to delegating the discovery and associated selection of NF instances or NF service instances to an SCP.

Direct Communication: This refers to the communication between NFs or NF services without using an SCP.

DN Access Identifier (DNAI): Identifier of a user plane access to one or more DN(s) where applications are deployed.

Emergency Registered: A UE is considered Emergency Registered over an Access Type in a PLMN when registered for emergency services only over this Access Type in this PLMN.

Endpoint Address: An address in the format of an IP address or FQDN, which is used to determine the host/authority part of the target URI. This Target URI is used to access an NF service (i.e. to invoke service operations) of an NF service producer or for notifications to an NF service consumer.

En-gNB: as defined in TS 37.340 [31].

Expected UE Behaviour: Set of parameters provisioned by an external party to 5G network functions on the foreseen or expected UE behaviour, see clause 5.20.

Fixed Network Residential Gateway: A Fixed Network RG (FN-RG) is a RG that it does not support N1 signalling and it is not 5GC capable.

Fixed Network Broadband Residential Gateway: A Fixed Network RG (FN-BRG) is a FN-RG specified in BBF TR-124 [90].

Fixed Network Cable Residential Gateway: A Fixed Network Cable RG (FN-CRG) is a FN-RG with cable modem specified in DOCSIS MULPI [89].

Forbidden Area: An area where the UE is not allowed to initiate communication as specified in clause 5.3.2.3.

GBR QoS Flow: A QoS Flow using the GBR resource type or the Delay-critical GBR resource type and requiring guaranteed flow bit rate.

IAB-donor: This is a NG-RAN node that supports Integrated access and backhaul (IAB) feature and provides connection to the core network to IAB-nodes. It supports the CU function of the CU/DU architecture for IAB defined in TS 38.401 [42].

IAB-node: A relay node that supports wireless in-band and out-of-band relaying of NR access traffic via NR Uu backhaul links. It supports the UE function and the DU function of the CU/DU architecture for IAB defined in TS 38.401 [42].

Indirect Communication: This refers to the communication between NFs or NF services via an SCP.

Initial Registration: UE registration in RM-DEREGISTERED state as specified in clause 5.3.2.

Intermediate SMF (I-SMF): An SMF that is inserted to support a PDU session as the UE is located in an area which cannot be controlled by the original SMF because the UPF(s) belong to a different SMF Service Area.

Local Area Data Network: a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.

Local Break Out (LBO): Roaming scenario for a PDU Session where the PDU Session Anchor and its controlling SMF are located in the serving PLMN (VPLMN).

LTE-M: a 3GPP RAT type Identifier used in the Core Network only, which is a sub-type of E-UTRA RAT type, and defined to identify in the Core Network the E-UTRA when used by a UE indicating Category M.

MA PDU Session: A PDU Session that provides a PDU connectivity service, which can use one access network at a time, or simultaneously one 3GPP access network and one non-3GPP access network.

Mobility Pattern: Network concept of determining within the AMF the UE mobility parameters as specified in clause 5.3.2.4.

Mobility Registration Update: UE re-registration when entering new TA outside the TAI List as specified in clause 5.3.2.

MPS-subscribed UE: A UE having a USIM with MPS subscription.

NB-IoT UE Priority: Numerical value used by the NG-RAN to prioritise between different UEs accessing via NB-IoT.

NGAP UE association: The logical per UE association between a 5G-AN node and an AMF.

NGAP UE-TNLA-binding: The binding between a NGAP UE association and a specific TNL association for a given UE.

Network Function: A 3GPP adopted or 3GPP defined processing function in a network, which has defined functional behaviour and 3GPP defined interfaces.

NOTE 1: A network function can be implemented either as a network element on a dedicated hardware, as a software instance running on a dedicated hardware, or as a virtualised function instantiated on an appropriate platform, e.g. on a cloud infrastructure.

Network Instance: Information identifying a domain. Used by the UPF for traffic detection and routing.

Network Slice: A logical network that provides specific network capabilities and network characteristics.

Network Slice instance: A set of Network Function instances and the required resources (e.g. compute, storage and networking resources) which form a deployed Network Slice.

Non-GBR QoS Flow: A QoS Flow using the Non-GBR resource type and not requiring guaranteed flow bit rate.

NSI ID: an identifier for identifying the Core Network part of a Network Slice instance when multiple Network Slice instances of the same Network Slice are deployed, and there is a need to differentiate between them in the 5GC.

NF instance: an identifiable instance of the NF.

NF service: a functionality exposed by a NF through a service based interface and consumed by other authorized NFs.

NF service instance: an identifiable instance of the NF service.

NF service operation: An elementary unit a NF service is composed of.

NF Service Set: A group of interchangeable NF service instances of the same service type within an NF instance. The NF service instances in the same NF Service Set have access to the same context data.

NF Set: A group of interchangeable NF instances of the same type, supporting the same services and the same Network Slice(s). The NF instances in the same NF Set may be geographically distributed but have access to the same context data.

NG-RAN: A radio access network that supports one or more of the following options with the common characteristics that it connects to 5GC:

1) Standalone New Radio.
2) New Radio is the anchor with E-UTRA extensions.
3) Standalone E-UTRA.
4) E-UTRA is the anchor with New Radio extensions.

Non-Allowed Area: Area where the UE is allowed to initiate Registration procedure but no other communication as specified in clause 5.3.2.3.

Non-Public Network: See definition in TS 22.261 [2].

Non-Seamless Non-3GPP offload: The offload of user plane traffic via non-3GPP access without traversing either N3IWF/TNGF or UPF.

PCF Group ID: This refers to one or more PCF instances managing a specific set of SUPIs. A PCF Group consists of one or multiple PCF Sets.

Pending NSSAI: NSSAI provided by the Serving PLMN during a Registration procedure, indicating the S-NSSAI(s) for which the network slice-specific authentication and authorization procedure is pending.

PDU Connectivity Service: A service that provides exchange of PDUs between a UE and a Data Network.

PDU Session: Association between the UE and a Data Network that provides a PDU connectivity service.

PDU Session Type: The type of PDU Session which can be IPv4, IPv6, IPv4v6, Ethernet or Unstructured.

Periodic Registration Update: UE re-registration at expiry of periodic registration timer as specified in clause 5.3.2.

Private communication: See definition in TS 22.261 [2].

Public network integrated NPN: A non-public network deployed with the support of a PLMN.

(Radio) Access Network: See 5G Access Network.

RAT type: Identifies the transmission technology used in the access network for both 3GPP accesses and non-3GPP Accesses, for example, NR, NB-IOT, Untrusted Non-3GPP, Trusted Non-3GPP, Trusted IEEE 802.11 Non-3GPP access, Wireline, Wireline-Cable, Wireline-BBF, etc.

Requested NSSAI: NSSAI provided by the UE to the Serving PLMN during registration.

Residential Gateway: The Residential Gateway (RG) is a device providing, for example voice, data, broadcast video, video on demand, to other devices in customer premises.

Routing Binding Indication: Information included in a request or notification and that can be used by the SCP for discovery and associated selection to of a suitable target. See clauses 6.3.1.0 and 7.1.2

Routing Indicator: Indicator that allows together with SUCI/SUPI Home Network Identifier to route network signalling to AUSF and UDM instances capable to serve the subscriber.

SCP Domain: A configured group of one or more SCPs that can reach certain NF instances or SCPs directly, i.e. without passing through an intermediate SCP.

SNPN enabled UE: A UE configured to use stand-alone Non-Public Networks.

SNPN access mode: A UE operating in SNPN access mode only selects stand-alone Non-Public Networks over Uu.

Service based interface: It represents how a set of services is provided/exposed by a given NF.

Service Continuity: The uninterrupted user experience of a service, including the cases where the IP address and/or anchoring point change.

Service Data Flow Filter: A set of packet flow header parameter values/ranges used to identify one or more of the packet (IP or Ethernet) flows constituting a Service Data Flow.

Service Data Flow Template: The set of Service Data Flow filters in a policy rule or an application identifier in a policy rule referring to an application detection filter, required for defining a Service Data Flow.

Session Continuity: The continuity of a PDU Session. For PDU Session of IPv4 or IPv6 or IPv4v6 type "session continuity" implies that the IP address is preserved for the lifetime of the PDU Session.

SMF Service Area: The collection of UPF Service Areas of all UPFs which can be controlled by one SMF.

Stand-alone Non-Public Network: A non-public network not relying on network functions provided by a PLMN

Subscribed S-NSSAI: S-NSSAI based on subscriber information, which a UE is subscribed to use in a PLMN

Time Sensitive Communication (TSC): A communication service that supports deterministic communication and/or isochronous communication with high reliability and availability. It is about providing packet transport with QoS characteristics such as bounds on latency, loss, and reliability, where end systems and relay/transmit nodes can be strictly synchronized.

TSN working domain: Synchronization domain for a localized set of devices collaborating on a specific task or work function in a TSN network, corresponding to a gPTP domain defined in IEEE 802.1AS [104].

UDM Group ID: This refers to one or more UDM instances managing a specific set of SUPIs. An UDM Group consists of one or multiple UDM Sets.

UDR Group ID: This refers to one or more UDR instances managing a specific set of SUPIs. An UDR Group consists of one or multiple UDR Sets.

UPF Service Area: An area consisting of one or more TA(s) within which PDU Session associated with the UPF can be served by (R)AN nodes via a N3 interface between the (R)AN and the UPF without need to add a new UPF in between or to remove/re-allocate the UPF.

Uplink Classifier: UPF functionality that aims at diverting Uplink traffic, based on filter rules provided by SMF, towards Data Network.

WB-E-UTRA: In the RAN, WB-E-UTRA is the part of E-UTRA that excludes NB-IoT. In the Core Network, WB-E-UTRA also excludes LTE-M.

Wireline 5G Access Network: The Wireline 5G Access Network (W-5GAN) is a wireline AN that connects to a 5GC via N2 and N3 reference points. The W-5GAN can be either a W-5GBAN or W-5GCAN.

Wireline 5G Cable Access Network: The Wireline 5G Cable Access Network (W-5GCAN) is the Access Network defined in CableLabs.

Wireline BBF Access Network: The Wireline 5G BBF Access Network (W-5GBAN) is the Access Network defined in BBF.

Wireline Access Gateway Function (W-AGF): The Wireline Access Gateway Function (W-AGF) is a Network function in W-5GAN that provides connectivity to the 5G Core to 5G-RG and FN-RG.

NOTE 2: If one AUSF/PCF/UDR/UDM group consists of multiple AUSF/PCF/UDR/UDM Sets, AUSF/PCF/UDR/UDM instance from different Set may be selected to serve the same UE. The temporary data which is not shared across different Sets may be lost, e.g. the event subscriptions stored at one UDM instance are lost if another UDM instance from different Set is selected and no data shared across the UDM Sets.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

5GC	5G Core Network
5GLAN	5G Local Area Network
5GS	5G System
5G-AN	5G Access Network
5G-AN PDB	5G Access Network Packet Delay Budget
5G-EIR	5G-Equipment Identity Register
5G-GUTI	5G Globally Unique Temporary Identifier
5G-BRG	5G Broadband Residential Gateway
5G-CRG	5G Cable Residential Gateway
5G GM	5G Grand Master
5G-RG	5G Residential Gateway
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
5G VN	5G Virtual Network
5QI	5G QoS Identifier
AF	Application Function
AMF	Access and Mobility Management Function
AS	Access Stratum
ATSSS	Access Traffic Steering, Switching, Splitting
ATSSS-LL	ATSSS Low-Layer
AUSF	Authentication Server Function
BMCA	Best Master Clock Algorithm
BSF	Binding Support Function
CAG	Closed Access Group

CAPIF	Common API Framework for 3GPP northbound APIs
CHF	Charging Function
CN PDB	Core Network Packet Delay Budget
CP	Control Plane
DAPS	Dual Active Protocol Stacks
DL	Downlink
DN	Data Network
DNAI	DN Access Identifier
DNN	Data Network Name
DRX	Discontinuous Reception
DS-TT	Device-side TSN translator
ePDG	evolved Packet Data Gateway
EBI	EPS Bearer Identity
EUI	Extended Unique Identifier
FAR	Forwarding Action Rule
FN-BRG	Fixed Network Broadband RG
FN-CRG	Fixed Network Cable RG
FN-RG	Fixed Network RG
FQDN	Fully Qualified Domain Name
GFBR	Guaranteed Flow Bit Rate
GMLC	Gateway Mobile Location Centre
GPSI	Generic Public Subscription Identifier
GUAMI	Globally Unique AMF Identifier
HR	Home Routed (roaming)
IAB	Integrated access and backhaul
IMEI/TAC	IMEI Type Allocation Code
IPUPS	Inter PLMN UP Security
I-SMF	Intermediate SMF
I-UPF	Intermediate UPF
LADN	Local Area Data Network
LBO	Local Break Out (roaming)
LMF	Location Management Function
LoA	Level of Automation
LPP	LTE Positioning Protocol
LRF	Location Retrieval Function
MCX	Mission Critical Service
MDBV	Maximum Data Burst Volume
MFBR	Maximum Flow Bit Rate
MICO	Mobile Initiated Connection Only
MPS	Multimedia Priority Service
MPTCP	Multi-Path TCP Protocol
N3IWF	Non-3GPP InterWorking Function
N5CW	Non-5G-Capable over WLAN
NAI	Network Access Identifier
NEF	Network Exposure Function
NF	Network Function
NGAP	Next Generation Application Protocol
NID	Network identifier
NPN	Non-Public Network
NR	New Radio
NRF	Network Repository Function
NSI ID	Network Slice Instance Identifier
NSSAA	Network Slice-Specific Authentication and Authorization
NSSAAF	Network Slice-Specific Authentication and Authorization Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSP	Network Slice Selection Policy
NW-TT	Network-side TSN translator
NWDAF	Network Data Analytics Function
PCF	Policy Control Function
PDB	Packet Delay Budget
PDR	Packet Detection Rule

PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PER	Packet Error Rate
PFD	Packet Flow Description
PNI-NPN	Public Network Integrated Non-Public Network
PPD	Paging Policy Differentiation
PPF	Paging Proceed Flag
PPI	Paging Policy Indicator
PSA	PDU Session Anchor
PTP	Precision Time Protocol
QFI	QoS Flow Identifier
QoE	Quality of Experience
RACS	Radio Capabilities Signalling optimisation
(R)AN	(Radio) Access Network
RG	Residential Gateway
RIM	Remote Interference Management
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
RSN	Redundancy Sequence Number
SA NR	Standalone New Radio
SBA	Service Based Architecture
SBI	Service Based Interface
SCP	Service Communication Proxy
SD	Slice Differentiator
SEAF	Security Anchor Functionality
SEPP	Security Edge Protection Proxy
SMF	Session Management Function
SMSF	Short Message Service Function
SN	Sequence Number
SNPN	Stand-alone Non-Public Network
S-NSSAI	Single Network Slice Selection Assistance Information
SSC	Session and Service Continuity
SSCMSP	Session and Service Continuity Mode Selection Policy
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
SV	Software Version
TNAN	Trusted Non-3GPP Access Network
TNAP	Trusted Non-3GPP Access Point
TNGF	Trusted Non-3GPP Gateway Function
TNL	Transport Network Layer
TNLA	Transport Network Layer Association
TSC	Time Sensitive Communication
TSCAI	TSC Assistance Information
TSN	Time Sensitive Networking
TSN GM	TSN Grand Master
TSP	Traffic Steering Policy
TT	TSN Translator
TWIF	Trusted WLAN Interworking Function
UCMF	UE radio Capability Management Function
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function
UL	Uplink
UL CL	Uplink Classifier
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communication
URRP-AMF	UE Reachability Request Parameter for AMF
URSP	UE Route Selection Policy
VID	VLAN Identifier
VLAN	Virtual Local Area Network
W-5GAN	Wireline 5G Access Network

W-5GBAN Wireline BBF Access Network
W-5GCAN Wireline 5G Cable Access Network
W-AGF Wireline Access Gateway Function

4 Architecture model and concepts

4.1 General concepts

The 5G System architecture is defined to support data connectivity and services enabling deployments to use techniques such as e.g. Network Function Virtualization and Software Defined Networking. The 5G System architecture shall leverage service-based interactions between Control Plane (CP) Network Functions where identified. Some key principles and concept are to:

- Separate the User Plane (UP) functions from the Control Plane (CP) functions, allowing independent scalability, evolution and flexible deployments e.g. centralized location or distributed (remote) location.
- Modularize the function design, e.g. to enable flexible and efficient network slicing.
- Wherever applicable, define procedures (i.e. the set of interactions between network functions) as services, so that their re-use is possible.
- Enable each Network Function and its Network Function Services to interact with other NF and its Network Function Services directly or indirectly via a Service Communication Proxy if required. The architecture does not preclude the use of another intermediate function to help route Control Plane messages (e.g. like a DRA).
- Minimize dependencies between the Access Network (AN) and the Core Network (CN). The architecture is defined with a converged core network with a common AN - CN interface which integrates different Access Types e.g. 3GPP access and non-3GPP access.
- Support a unified authentication framework.
- Support "stateless" NFs, where the "compute" resource is decoupled from the "storage" resource.
- Support capability exposure.
- Support concurrent access to local and centralized services. To support low latency services and access to local data networks, UP functions can be deployed close to the Access Network.
- Support roaming with both Home routed traffic as well as Local breakout traffic in the visited PLMN.

4.2 Architecture reference model

4.2.1 General

This specification describes the architecture for the 5G System. The 5G architecture is defined as service-based and the interaction between network functions is represented in two ways.

- A service-based representation, where network functions (e.g. AMF) within the Control Plane enables other authorized network functions to access their services. This representation also includes point-to-point reference points where necessary.
- A reference point representation, shows the interaction exist between the NF services in the network functions described by point-to-point reference point (e.g. N11) between any two network functions (e.g. AMF and SMF).

Service-based interfaces are listed in clause 4.2.6. Reference points are listed in clause 4.2.7.

Network functions within the 5GC Control Plane shall only use service-based interfaces for their interactions.

NOTE 1: The interactions between NF services within one NF are not specified in this Release of the specification.

NOTE 2: UPF does not provide any services in this Release of the specification, but can consume services provided by 5GC Control Plane NFs.

NFs and NF services can communicate directly, referred to as Direct Communication, or indirectly via the SCP, referred to as Indirect Communication. For more information on communication options, see Annex E and clauses under 6.3.1 and 7.1.2.

4.2.2 Network Functions and entities

The 5G System architecture consists of the following network functions (NF).

- Authentication Server Function (AUSF).
- Access and Mobility Management Function (AMF).
- Data Network (DN), e.g. operator services, Internet access or 3rd party services.
- Unstructured Data Storage Function (UDSF).
- Network Exposure Function (NEF).
- Network Repository Function (NRF).
- Network Slice Specific Authentication and Authorization Function (NSSAAF).
- Network Slice Selection Function (NSSF).
- Policy Control Function (PCF).
- Session Management Function (SMF).
- Unified Data Management (UDM).
- Unified Data Repository (UDR).
- User Plane Function (UPF).
- UE radio Capability Management Function (UCMF).
- Application Function (AF).
- User Equipment (UE).
- (Radio) Access Network ((R)AN).
- 5G-Equipment Identity Register (5G-EIR).
- Network Data Analytics Function (NWDAF).
- CHarging Function (CHF).

NOTE: The functional description of the CHF is specified in TS 32.240 [41].

The 5G System architecture also comprises the following network entities:

- Service Communication Proxy (SCP).
- Security Edge Protection Proxy (SEPP).

The functional descriptions of these Network Functions and entities are specified in clause 6.

- Non-3GPP InterWorking Function (N3IWF).
- Trusted Non-3GPP Gateway Function (TNGF).
- Wireline Access Gateway Function (W-AGF).
- Trusted WLAN Interworking Function (TWIF).

4.2.3 Non-roaming reference architecture

Figure 4.2.3-1 depicts the non-roaming reference architecture. Service-based interfaces are used within the Control Plane.

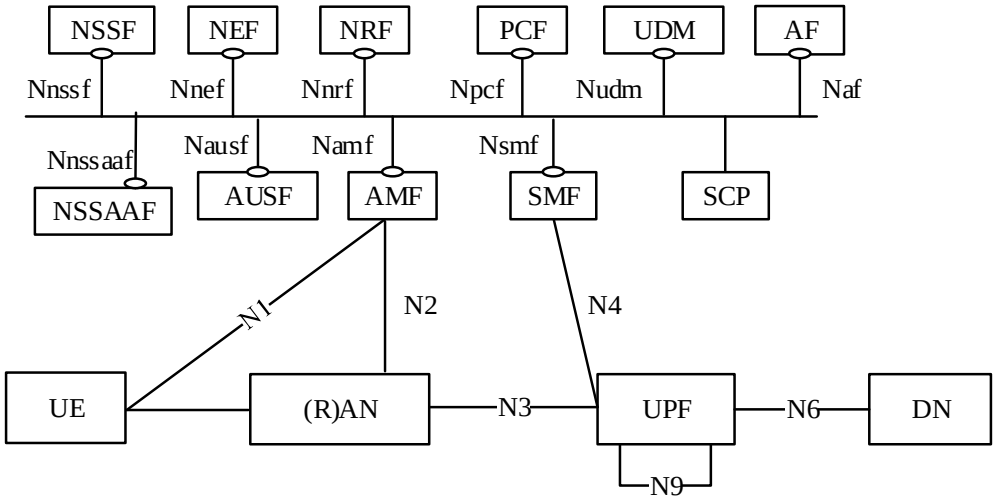
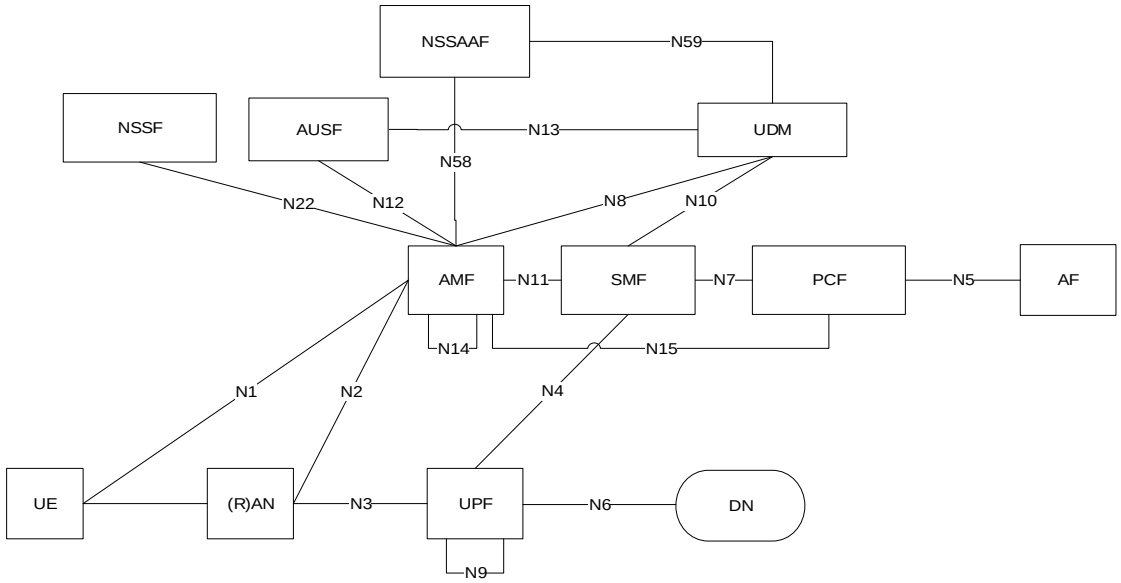


Figure 4.2.3-1: 5G System architecture

NOTE: If an SCP is deployed it can be used for indirect communication between NFs and NF services as described in Annex E. SCP does not expose services itself.

Figure 4.2.3-2 depicts the 5G System architecture in the non-roaming case, using the reference point representation showing how various network functions interact with each other.



NOTE 1: N9, N14 are not shown in all other figures however they may also be applicable for other scenarios.
NOTE 2: For the sake of clarity of the point-to-point diagrams, the UDSF, NEF and NRF have not been depicted. However, all depicted Network Functions can interact with the UDSF, UDR, NEF and NRF as necessary.
NOTE 3: The UDM uses subscription data and authentication data and the PCF uses policy data that may be stored in UDR (refer to clause 4.2.5).
NOTE 4: For clarity, the UDR and its connections with other NFs, e.g. PCF, are not depicted in the point-to-point and service-based architecture diagrams. For more information on data storage architectures refer to clause 4.2.5.
NOTE 5: For clarity, the NWDAF and its connections with other NFs, e.g. PCF, are not depicted in the point-to-point and service-based architecture diagrams. For more information on network data analytics architecture refer to TS 23.288 [86].

Figure 4.2.3-2: Non-Roaming 5G System Architecture in reference point representation

Figure 4.2.3-3 depicts the non-roaming architecture for UEs concurrently accessing two (e.g. local and central) data networks using multiple PDU Sessions, using the reference point representation. This figure shows the architecture for multiple PDU Sessions where two SMFs are selected for the two different PDU Sessions. However, each SMF may also have the capability to control both a local and a central UPF within a PDU Session.

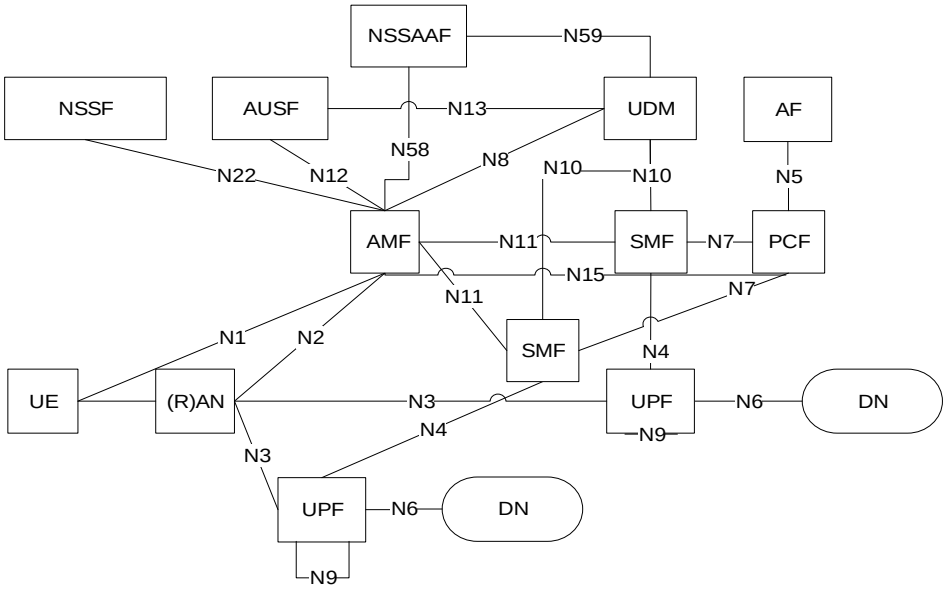


Figure 4.2.3-3: Applying non-roaming 5G System architecture for multiple PDU Session in reference point representation

Figure 4.2.3-4 depicts the non-roaming architecture in the case of concurrent access to two (e.g. local and central) data networks is provided within a single PDU Session, using the reference point representation.

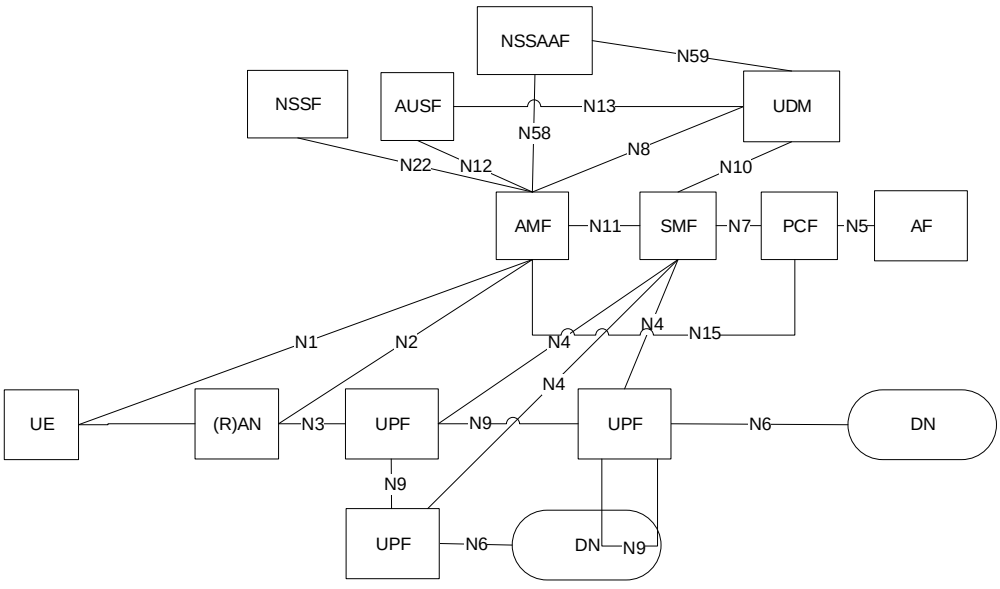


Figure 4.2.3-4: Applying non-roaming 5G System architecture for concurrent access to two (e.g. local and central) data networks (single PDU Session option) in reference point representation

Figure 4.2.3-5 depicts the non-roaming architecture for Network Exposure Function, using reference point representation.

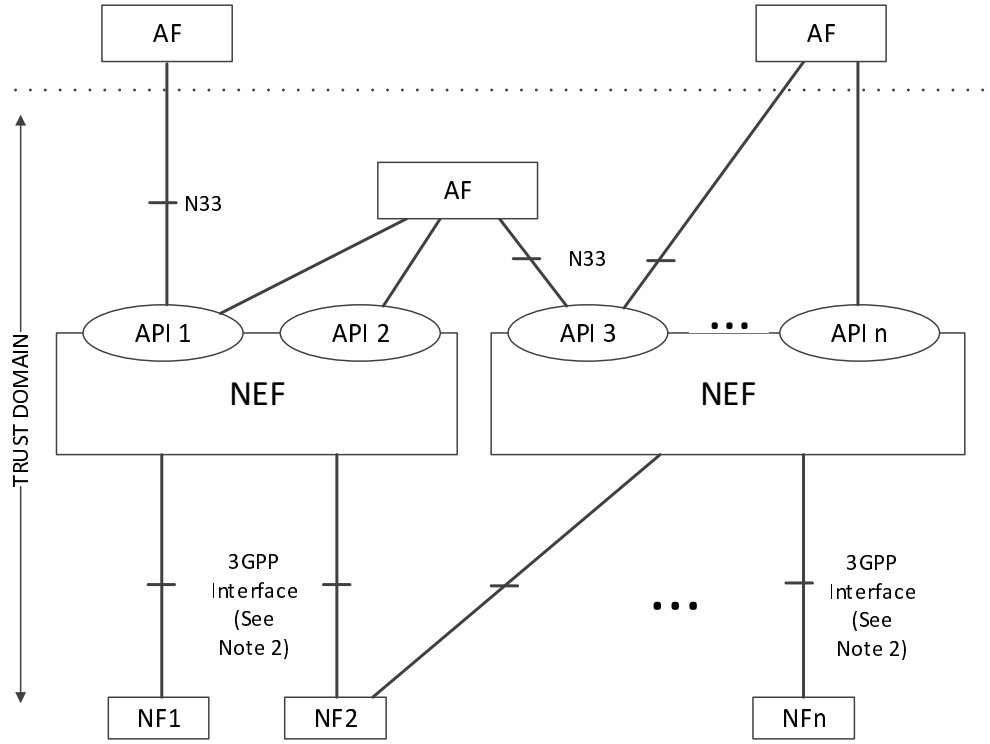


Figure 4.2.3-5: Non-roaming architecture for Network Exposure Function in reference point representation

NOTE 1: In figure 4.2.3-5, Trust domain for NEF is same as Trust domain for SCEF as defined in TS 23.682 [36].

NOTE 2: In figure 4.2.3-5, 3GPP Interface represents southbound interfaces between NEF and 5GC Network Functions e.g. N29 interface between NEF and SMF, N30 interface between NEF and PCF, etc. All southbound interfaces from NEF are not shown for the sake of simplicity.

4.2.4 Roaming reference architectures

Figure 4.2.4-1 depicts the 5G System roaming architecture with local breakout with service-based interfaces within the Control Plane.

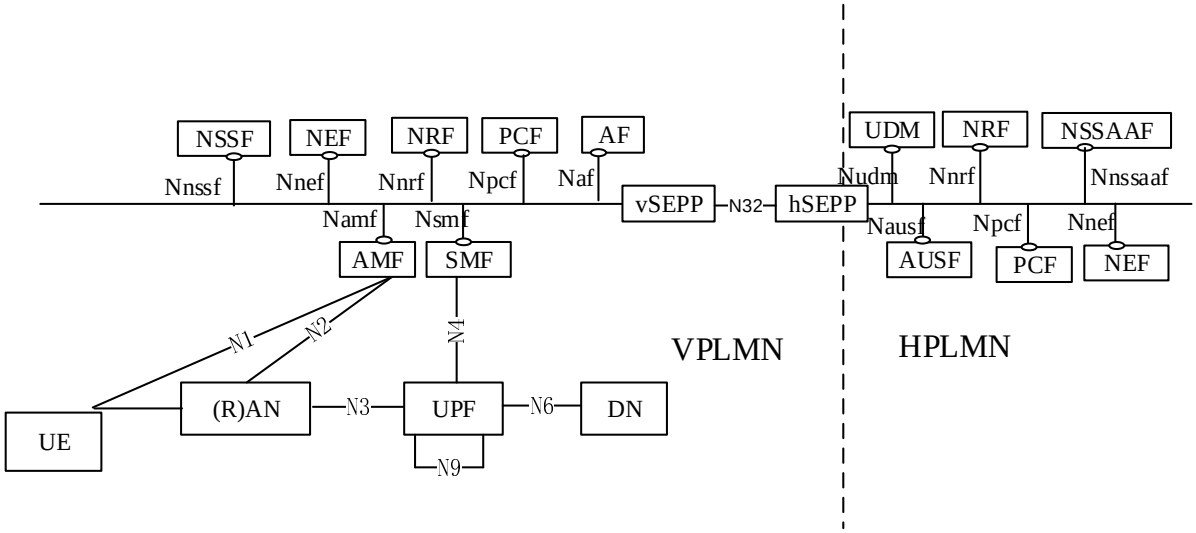


Figure 4.2.4-1: Roaming 5G System architecture- local breakout scenario in service-based interface representation

NOTE 1: In the LBO architecture. The PCF in the VPLMN may interact with the AF in order to generate PCC Rules for services delivered via the VPLMN. The PCF in the VPLMN uses locally configured policies according to the roaming agreement with the HPLMN operator as input for PCC Rule generation. The PCF in VPLMN has no access to subscriber policy information from the HPLMN.

NOTE 2: An SCP can be used for indirect communication between NFs and NF services within theVPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

Figure 4.2.4-3 depicts the 5G System roaming architecture in the case of home routed scenario with service-based interfaces within the Control Plane.

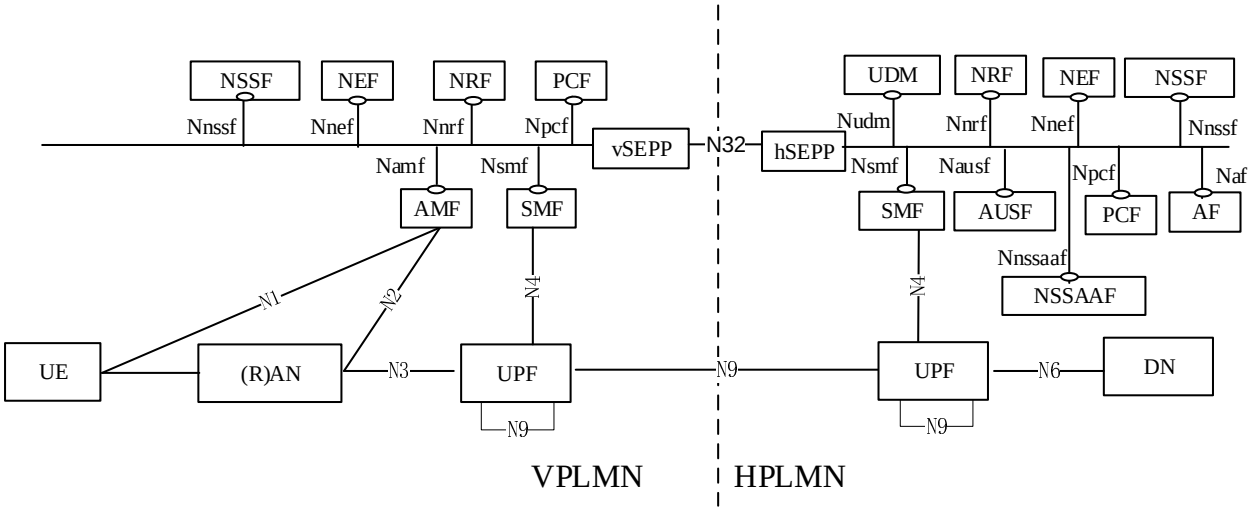


Figure 4.2.4-3: Roaming 5G System architecture - home routed scenario in service-based interface representation

NOTE 3: An SCP can be used for indirect communication between NFs and NF services within the VPLMN, within the HPLMN, or in within both VPLMN and HPLMN. For simplicity, the SCP is not shown in the roaming architecture.

NOTE 4: UPFs in the home routed scenario can be used also to support the IPUPS functionality (see clause 5.8.2.14).

Figure 4.2.4-4 depicts 5G System roaming architecture in the case of local break out scenario using the reference point representation.

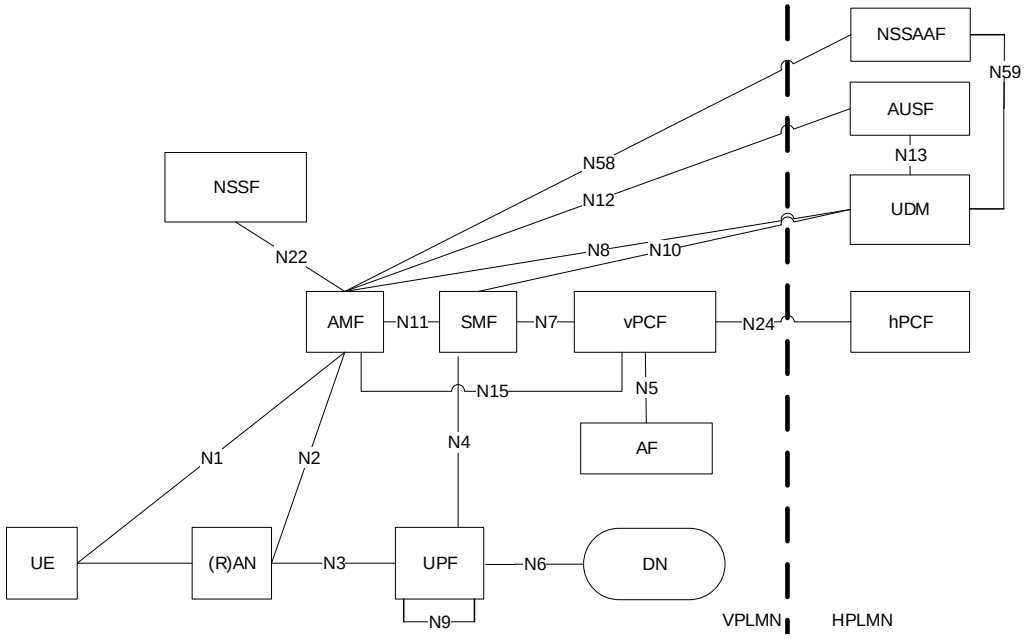


Figure 4.2.4-4: Roaming 5G System architecture - local breakout scenario in reference point representation

NOTE 5: The NRF is not depicted in reference point architecture figures. Refer to Figure 4.2.4-7 for details on NRF and NF interfaces.

NOTE 6: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

The following figure 4.2.4-6 depicts the 5G System roaming architecture in the case of home routed scenario using the reference point representation.

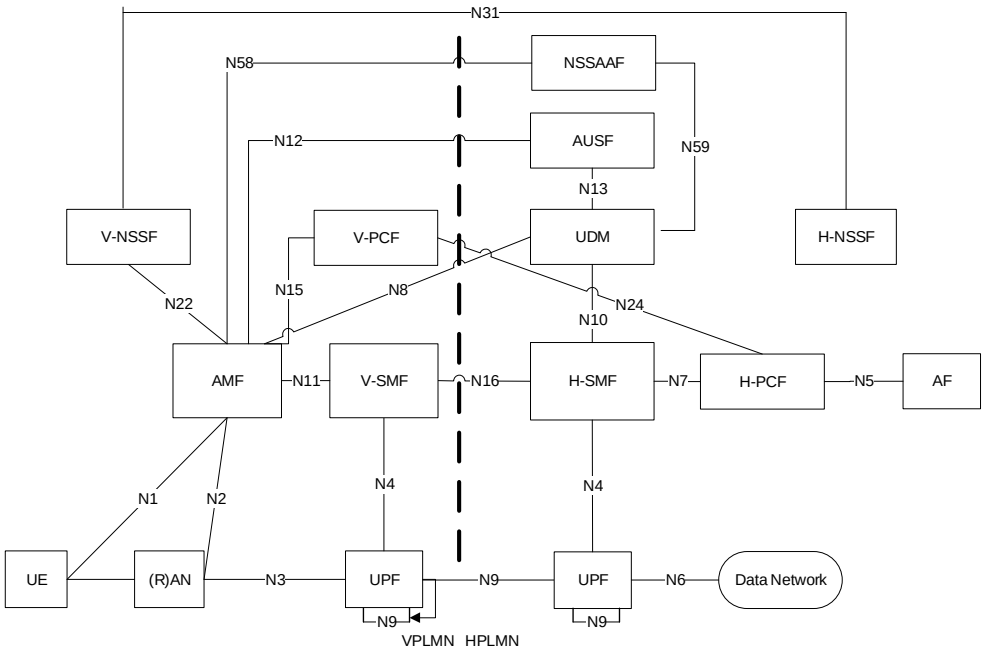


Figure 4.2.4-6: Roaming 5G System architecture - Home routed scenario in reference point representation

For the roaming scenarios described above each PLMN implements proxy functionality to secure interconnection and hide topology on the inter-PLMN interfaces.

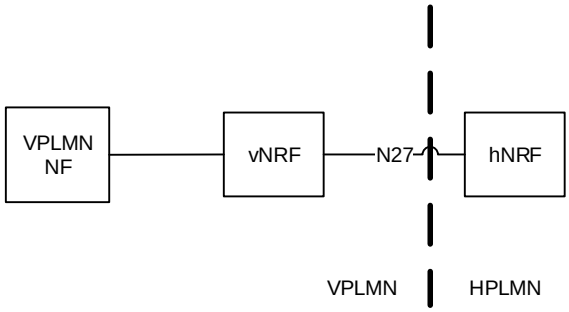


Figure 4.2.4-7: NRF Roaming architecture in reference point representation

NOTE 7: For the sake of clarity, SEPPs on both sides of PLMN borders are not depicted in figure 4.2.4-7.

Figure 4.2.4-8: Void

Operators can deploy UPFs supporting the Inter PLMN UP Security (IPUPS) functionality at the border of their network to protect their network from invalid inter PLMN N9 traffic in home routed roaming scenarios. The UPFs supporting the IPUPS functionality in VPLMN and HPLMN are controlled by the V-SMF and the H-SMF of that PDU Session respectively. A UPF supporting the IPUPS functionality terminates GTP-U N9 tunnels. The SMF can activate the IPUPS functionality together with other UP functionality in the same UPF, or insert a separate UPF for the IPUPS functionality in the UP path (which e.g. may be dedicated to be used for IPUPS functionality). Figure 4.2.4-9 depicts the home routed roaming architecture where a UPF is inserted in the UP path for the IPUPS functionality. Figure 4.2.4-3 depicts the home routed roaming architecture where the two UPFs perform the IPUPS functionality and other UP functionality for the PDU Session.

NOTE 8: Operators are not prohibited from deploying the IPUPS functionality as a separate Network Function from the UPF, acting as a transparent proxy which can transparently read N4 and N9 interfaces. However, such deployment option is not specified and needs to take at least into account very long lasting PDU Sessions with infrequent traffic and Inter-PLMN handover.

The IPUPS functionality is specified in clause 5.8.2.14 and TS 33.501 [29].

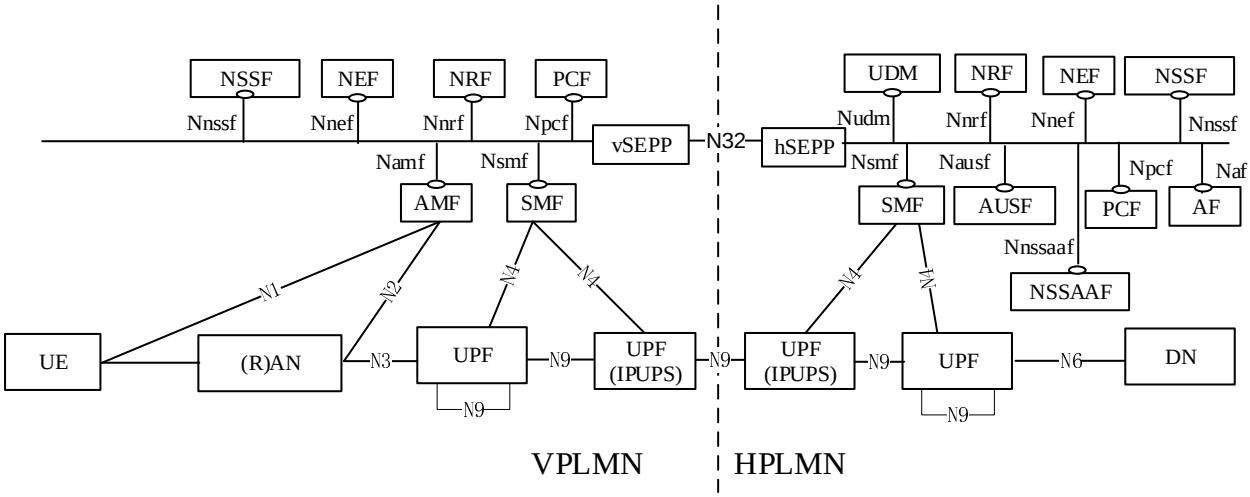


Figure 4.2.4-9: Roaming 5G System architecture - home routed roaming scenario in service-based interface representation employing UPF dedicated to IPUPS

4.2.5 Data Storage architectures

As depicted in Figure 4.2.5-1, the 5G System architecture allows any NF to store and retrieve its unstructured data into/from a UDSF (e.g. UE contexts). The UDSF belongs to the same PLMN where the network function is located. CP NFs may share a UDSF for storing their respective unstructured data or may each have their own UDSF (e.g. a UDSF may be located close to the respective NF).

NOTE 1: Structured data in this specification refers to data for which the structure is defined in 3GPP specifications. Unstructured data refers to data for which the structure is not defined in 3GPP specifications.

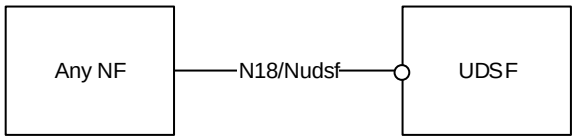


Figure 4.2.5-1: Data storage architecture for unstructured data from any NF

NOTE 2: 3GPP will specify (possibly by referencing) the N18/Nudsf interface.

As depicted in Figure 4.2.5-2, the 5G System architecture allows the UDM, PCF and NEF to store data in the UDR, including subscription data and policy data by UDM and PCF, structured data for exposure and application data (including Packet Flow Descriptions (PFDs) for application detection, AF request information for multiple UEs) by the NEF. UDR can be deployed in each PLMN and it can serve different functions as follows:

- UDR accessed by the NEF belongs to the same PLMN where the NEF is located.
- UDR accessed by the UDM belongs to the same PLMN where the UDM is located if UDM supports a split architecture.
- UDR accessed by the PCF belongs to the same PLMN where the PCF is located.

NOTE 3: The UDR deployed in each PLMN can store application data for roaming subscribers.

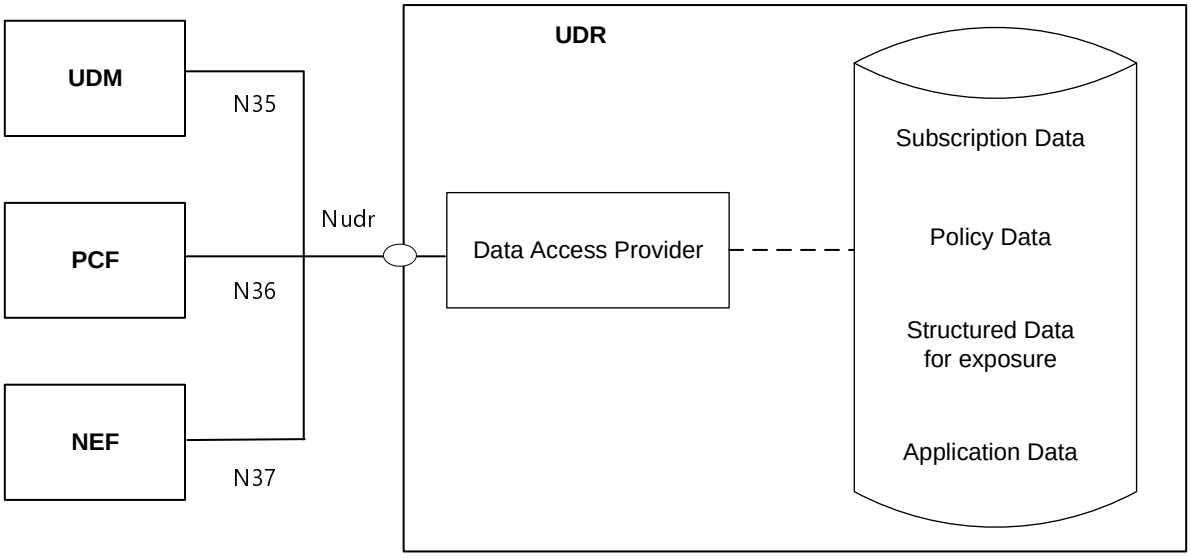


Figure 4.2.5-2: Data storage architecture

NOTE 4: There can be multiple UDRs deployed in the network, each of which can accommodate different data sets or subsets, (e.g. subscription data, subscription policy data, data for exposure, application data) and/or serve different sets of NFs. Deployments where a UDR serves a single NF and stores its data, and, thus, can be integrated with this NF, can be possible.

NOTE 5: The internal structure of the UDR in figure 4.2.5-2 is shown for information only.

The Nudr interface is defined for the network functions (i.e. NF Service Consumers), such as UDM, PCF and NEF, to access a particular set of the data stored and to read, update (including add, modify), delete, and subscribe to notification of relevant data changes in the UDR.

Each NF Service Consumer accessing the UDR, via Nudr, shall be able to add, modify, update or delete only the data it is authorised to change. This authorisation shall be performed by the UDR on a per data set and NF service consumer basis and potentially on a per UE, subscription granularity.

The following data in the UDR sets exposed via Nudr to the respective NF service consumer and stored shall be standardized:

- Subscription Data,
- Policy Data,
- Structured Data for exposure,
- Application data: Packet Flow Descriptions (PFDs) for application detection and AF request information for multiple UEs, as defined in clause 5.6.7.

The service based Nudr interface defines the content and format/encoding of the 3GPP defined information elements exposed by the data sets.

In addition, it shall be possible to access operator specific data sets by the NF Service Consumers from the UDR as well as operator specific data for each data set.

NOTE 6: The content and format/encoding of operator specific data and operator specific data sets are not subject to standardization.

NOTE 7: The organization of the different data stored in the UDR is not to be standardized.

4.2.5a Radio Capabilities Signalling optimisation

Figure 4.2.5a-1 depicts the AMF to UCMF reference point and interface. Figure 4.2.5a-2 depicts the related interfaces in AMF and UCMF for the Radio Capabilities Signalling optimisation in the roaming architecture.

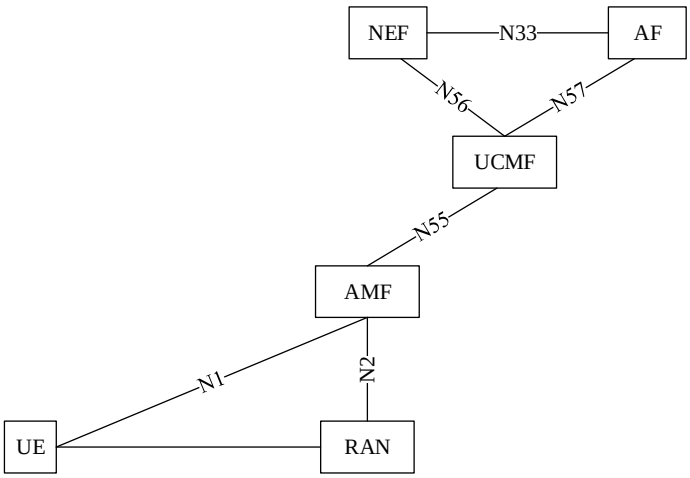
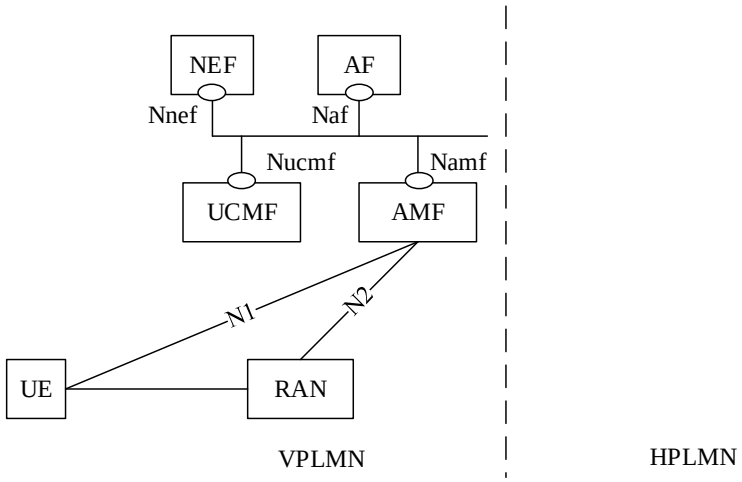


Figure 4.2.5a-1: Radio Capability Signalling optimisation architecture



NOTE: The AF in the VPLMN (i.e. the one having a relationship with the VPLMN NEF) is the one which provisions Manufacturer Assigned UE radio capability IDs in the VPLMN UCMF. RACS is a serving PLMN only feature (it requires no specific support in the roaming agreement with the UE HPLMN to operate).

Figure 4.2.5a-2: Roaming architecture for Radio Capability Signalling optimisation

4.2.6 Service-based interfaces

The 5G System Architecture contains the following service-based interfaces:

Namf: Service-based interface exhibited by AMF.

Nsmf: Service-based interface exhibited by SMF.

Nnef: Service-based interface exhibited by NEF.

Npcf: Service-based interface exhibited by PCF.

Nudm: Service-based interface exhibited by UDM.

Naf: Service-based interface exhibited by AF.

Nnrf: Service-based interface exhibited by NRF.

Nnssaaf: Service-based interface exhibited by NSSAAF.

Nnssf: Service-based interface exhibited by NSSF.

Nausf: Service-based interface exhibited by AUSF.

Nudr: Service-based interface exhibited by UDR.

Nudsf: Service-based interface exhibited by UDSF.

N5g-eir: Service-based interface exhibited by 5G-EIR.

Nnwdaf: Service-based interface exhibited by NWDAF.

Nchf: Service-based interface exhibited by CHF.

Nucmf: Service-based interface exhibited by UCMF.

NOTE: The Service-based interface exhibited by CHF is defined in TS 32.240 [41].

4.2.7 Reference points

The 5G System Architecture contains the following reference points:

N1: Reference point between the UE and the AMF.

N2: Reference point between the (R)AN and the AMF.

N3: Reference point between the (R)AN and the UPF.

N4: Reference point between the SMF and the UPF.

N6: Reference point between the UPF and a Data Network.

NOTE 1: The traffic forwarding details of N6 between a UPF acting as an uplink classifier and a local data network are not specified in this Release of the specification.

N9: Reference point between two UPFs.

The following reference points show the interactions that exist between the NF services in the NFs. These reference points are realized by corresponding NF service-based interfaces and by specifying the identified consumer and producer NF service as well as their interaction in order to realize a particular system procedure.

N5: Reference point between the PCF and an AF.

N7: Reference point between the SMF and the PCF.

N8: Reference point between the UDM and the AMF.

N10: Reference point between the UDM and the SMF.

N11: Reference point between the AMF and the SMF.

N12: Reference point between AMF and AUSF.

N13: Reference point between the UDM and Authentication Server function the AUSF.

N14: Reference point between two AMFs.

N15: Reference point between the PCF and the AMF in the case of non-roaming scenario, PCF in the visited network and AMF in the case of roaming scenario.

N16: Reference point between two SMFs, (in roaming case between SMF in the visited network and the SMF in the home network).

N16a: Reference point between SMF and I-SMF.

N17: Reference point between AMF and 5G-EIR.

N18: Reference point between any NF and UDSF.

N19: Reference point between two PSA UPFs for 5G LAN-type service.

N22: Reference point between AMF and NSSF.

N23: Reference point between PCF and NWDAF.

N24: Reference point between the PCF in the visited network and the PCF in the home network.

N27: Reference point between NRF in the visited network and the NRF in the home network.

N28: Reference point between PCF and CHF.

N29: Reference point between NEF and SMF.

N30: Reference point between PCF and NEF.

NOTE 2: The functionality of N28 and N29 and N30 reference points are defined in TS 23.503 [45].

N31: Reference point between the NSSF in the visited network and the NSSF in the home network.

NOTE 3: in some cases, a couple of NFs may need to be associated with each other to serve a UE.

In addition to the reference points above, there are interfaces/reference point(s) between SMF and the CHF. The reference point(s) are not depicted in the architecture illustrations in this specification.

NOTE 4: The functionality of these interface/reference points are defined in TS 32.240 [41].

N32: Reference point between SEPP in the visited network and the SEPP in the home network.

NOTE 5: The functionality of N32 reference point is defined in TS 33.501 [29].

N33: Reference point between NEF and AF.

N34: Reference point between NSSF and NWDAF.

N35: Reference point between UDM and UDR.

N36: Reference point between PCF and UDR.

N37: Reference point between NEF and UDR.

N38: Reference point between I-SMFs.

N40: Reference point between SMF and the CHF.

NOTE 6: The reference points from N40 up to and including N49 are reserved for allocation and definition in TS 23.503 [45].

N50: Reference point between AMF and the CBCF.

N51: Reference point between AMF and NEF.

N52: Reference point between NEF and UDM.

N55: Reference point between AMF and the UCMF.

N56: Reference point between NEF and the UCMF.

N57: Reference point between AF and the UCMF.

NOTE 7: The Public Warning System functionality of N50 reference point is defined in TS 23.041 [46].

N58: Reference point between AMF and the NSSAAF.

N59: Reference point between UDM and the NSSAAF.

The reference points to support SMS over NAS are listed in clause 4.4.2.2.

The reference points to support Location Services are listed in TS 23.273 [87].

The reference points to support SBA in IMS (N5, N70 and N71) are described in TS 23.228 [15].

4.2.8 Support of non-3GPP access

4.2.8.0 General

In this Release of the specification, the following types of non-3GPP access networks are defined:

- Untrusted non-3GPP access networks;
- Trusted non-3GPP access networks; and
- Wireline access networks.

The architecture to support Untrusted and Trusted non-3GPP access networks is defined in clause 4.2.8.2. The architecture to support Wireline access networks is defined in 4.2.8.2.4 and in TS 23.316 [84].

4.2.8.1 General Concepts to Support Trusted and Untrusted Non-3GPP Access

The 5G Core Network supports connectivity of UEs via non-3GPP access networks, e.g. WLAN access networks.

Only the support of non-3GPP access networks deployed outside the NG-RAN is described in this clause.

The 5G Core Network supports both untrusted non-3GPP access networks and trusted non-3GPP access networks (TNANs).

An untrusted non-3GPP access network shall be connected to the 5G Core Network via a Non-3GPP InterWorking Function (N3IWF), whereas a trusted non-3GPP access network shall be connected to the 5G Core Network via a Trusted Non-3GPP Gateway Function (TNGF). Both the N3IWF and the TNGF interface with the 5G Core Network CP and UP functions via the N2 and N3 interfaces, respectively.

A non-3GPP access network may advertise the PLMNs for which it supports trusted connectivity and the type of supported trusted connectivity (e.g. "5G connectivity"). Therefore, the UEs can discover the non-3GPP access networks that can provide trusted connectivity to one or more PLMNs. This is further specified in clause 6.3.12 (Trusted Non-3GPP Access Network selection).

The UE decides to use trusted or untrusted non-3GPP access for connecting to a 5G PLMN by using procedures not specified in this document. Examples of such procedures are defined in clause 6.3.12.1.

When the UE decides to use untrusted non-3GPP access to connect to a 5G Core Network in a PLMN:

- the UE first selects and connects with a non-3GPP access network; and then
- the UE selects a PLMN and an N3IWF in this PLMN. The PLMN/N3IWF selection and the non-3GPP access network selection are independent. The N3IWF selection is defined in clause 6.3.6.

When the UE decides to use trusted non-3GPP access to connect to a 5G Core Network in a PLMN:

- the UE first selects a PLMN; and then
- the UE selects a non-3GPP access network (a TNAN) that supports trusted connectivity to the selected PLMN. In this case, the non-3GPP access network selection is affected by the PLMN selection.

A UE that accesses the 5G Core Network over a non-3GPP access shall, after UE registration, support NAS signalling with 5G Core Network control-plane functions using the N1 reference point.

When a UE is connected via a NG-RAN and via a non-3GPP access, multiple N1 instances shall exist for the UE i.e. there shall be one N1 instance over NG-RAN and one N1 instance over non-3GPP access.

A UE simultaneously connected to the same 5G Core Network of a PLMN over a 3GPP access and a non-3GPP access shall be served by a single AMF in this 5G Core Network.

When a UE is connected to a 3GPP access of a PLMN, if the UE selects a N3IWF and the N3IWF is located in a PLMN different from the PLMN of the 3GPP access, e.g. in a different VPLMN or in the HPLMN, the UE is served separately by the two PLMNs. The UE is registered with two separate AMFs. PDU Sessions over the 3GPP access are served by V-SMFs different from the V-SMF serving the PDU Sessions over the non-3GPP access. The same can be true when the UE uses trusted non-3GPP access, i.e. the UE may select one PLMN for 3GPP access and a different PLMN for trusted non-3GPP access.

The PLMN selection for the 3GPP access does not depend on the PLMN that is used for non-3GPP access. In other words, if a UE is registered with a PLMN over a non-3GPP access, the UE performs PLMN selection for the 3GPP access independently of this PLMN.

A UE shall establish an IPsec tunnel with the N3IWF or with the TNGF in order to register with the 5G Core Network over non-3GPP access. Further details about the UE registration to 5G Core Network over untrusted non-3GPP access and over trusted non-3GPP access are described in clause 4.12.2 and in clause 4.12.2a in TS 23.502 [3], respectively.

It shall be possible to maintain the UE NAS signalling connection with the AMF over the non-3GPP access after all the PDU Sessions for the UE over that access have been released or handed over to 3GPP access.

N1 NAS signalling over non-3GPP accesses shall be protected with the same security mechanism applied for N1 over a 3GPP access.

User plane QoS differentiation between UE and N3IWF is supported as described in clause 5.7 and TS 23.502 [3] clause 4.12.5. QoS differentiation between UE and TNGF is supported as described in clause 5.7 and TS 23.502 [3] clause 4.12a.5.

4.2.8.1A General Concepts to support Wireline Access

Wireline 5G Access Network (W-5GAN) shall be connected to the 5G Core Network via a Wireline Access Gateway Function (W-AGF). The W-AGF interfaces the 5G Core Network CP and UP functions via N2 and N3 interfaces, respectively.

For the scenario of 5G-RG connected via NG RAN the specification for UE defined in this TS, TS 23.502 [3] and TS 23.503 [45] are applicable as defined for UE connected to 5GC via NG RAN unless differently specified in this TS and in TS 23.316 [84].

When a 5G-RG is connected via a NG-RAN and via a W-5GAN, multiple N1 instances shall exist for the 5G-RG i.e. there shall be one N1 instance over NG-RAN and one N1 instance over W-5GAN.

A 5G-RG simultaneously connected to the same 5G Core Network of a PLMN over a 3GPP access and a W-5GAN access shall be served by a single AMF in this 5G Core Network.

5G-RG shall maintain the NAS signalling connection with the AMF over the W-5GAN after all the PDU Sessions for the 5G-RG over that access have been released or handed over to 3GPP access.

The 5G-RG connected to 5GC via NG-RAN is specified in TS 23.316 [84].

For the scenario of FN-RG, which is not 5G capable, connected via W-5GAN to 5GC, the W-AGF provides the N1 interface to AMF on behalf of the FN-RG.

An UE connected to a 5G-RG or FN-RG can access to the 5GC via the N3IWF or via the TNGF where the combination of 5G-RG/FN-RG, W-AGF and UPF serving the 5G-RG or FN-RG is acting respectively as Untrusted Non-3GPP access network or as a Trusted Non-3GPP access network defined in clause 4.2.8.2; for example a UE is connecting to 5G-RG by means of WLAN radio access and connected to 5GC via N3IWF. The detailed description is specified in TS 23.316 [84].

The roaming architecture for 5G-BRG, FN-BRG, 5G-CRG and FN-CRG with the W-5GAN is not specified in this Release. The Home Routed roaming scenario is supported for 5G-RG connected via NG RAN, while Local Breakout scenario is not supported.

5G Multi-Operator Core Network (5G MOCN) is supported for 5G-RG connected via NG RAN as defined in clause 5.18

4.2.8.2 Architecture Reference Model for Trusted and Untrusted Non-3GPP Accesses

4.2.8.2.1 Non-roaming Architecture

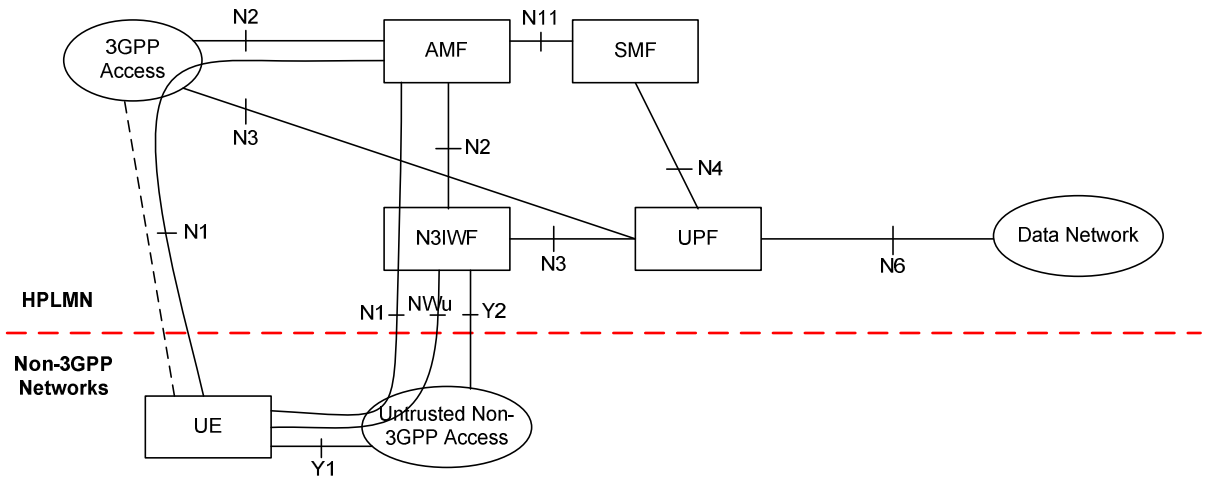


Figure 4.2.8.2.1-1: Non-roaming architecture for 5G Core Network with untrusted non-3GPP access

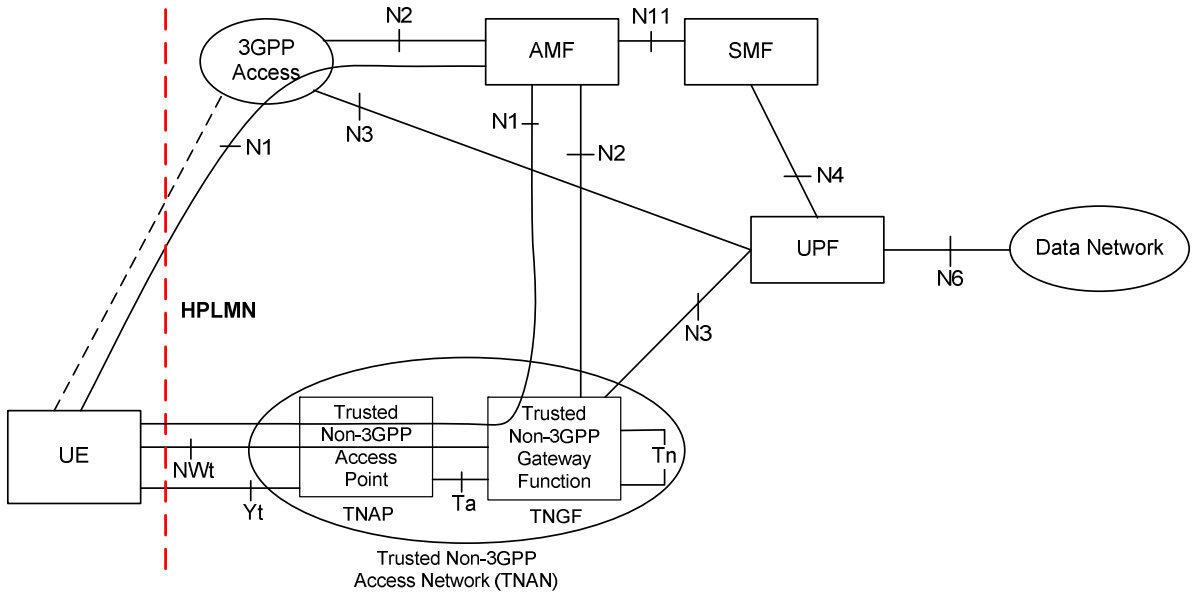


Figure 4.2.8.2.1-2: Non-roaming architecture for 5G Core Network with trusted non-3GPP access

NOTE 1: The reference architecture in Figure 4.2.8.2.1-1 and in Figure 4.2.8.2.1-2 only shows the architecture and the network functions directly connected to non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The reference architecture in Figure 4.2.8.2.1-1 and in Figure 4.2.8.2.1-2 supports service based interfaces for AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.8.2.1-1 and in Figure 4.2.8.2.1-2 terminate to a single AMF for a UE which is simultaneously connected to the same 5G Core Network over 3GPP access and non-3GPP access.

NOTE 4 The two N3 instances in Figure 4.2.8.2.1-1 and in Figure 4.2.8.2.1-2 may terminate to different UPFs when different PDU Sessions are established over 3GPP access and non-3GPP access.

4.2.8.2.2 LBO Roaming Architecture

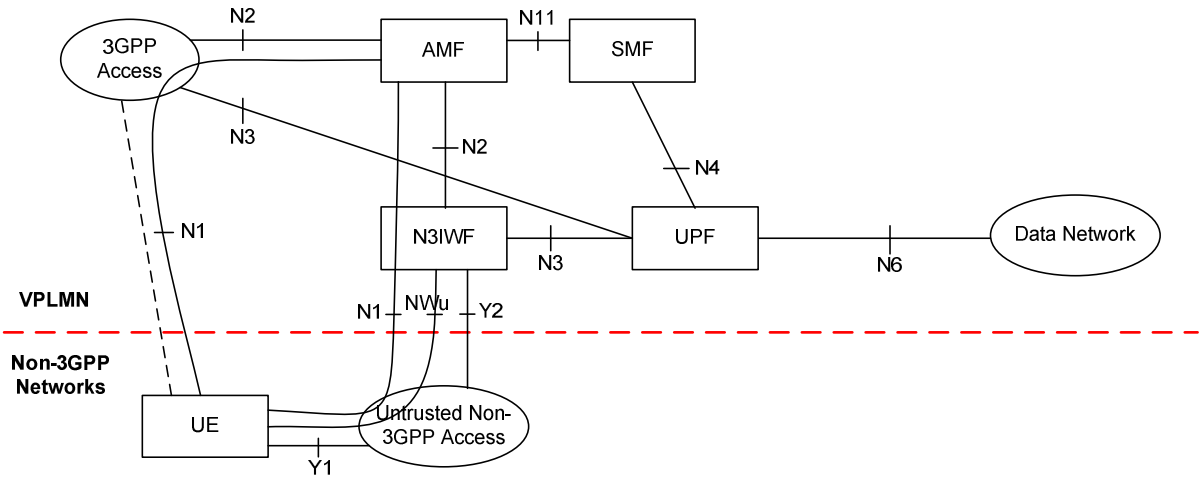


Figure 4.2.8.2.2-1: LBO Roaming architecture for 5G Core Network with untrusted non-3GPP access - N3IWF in the same VPLMN as 3GPP access

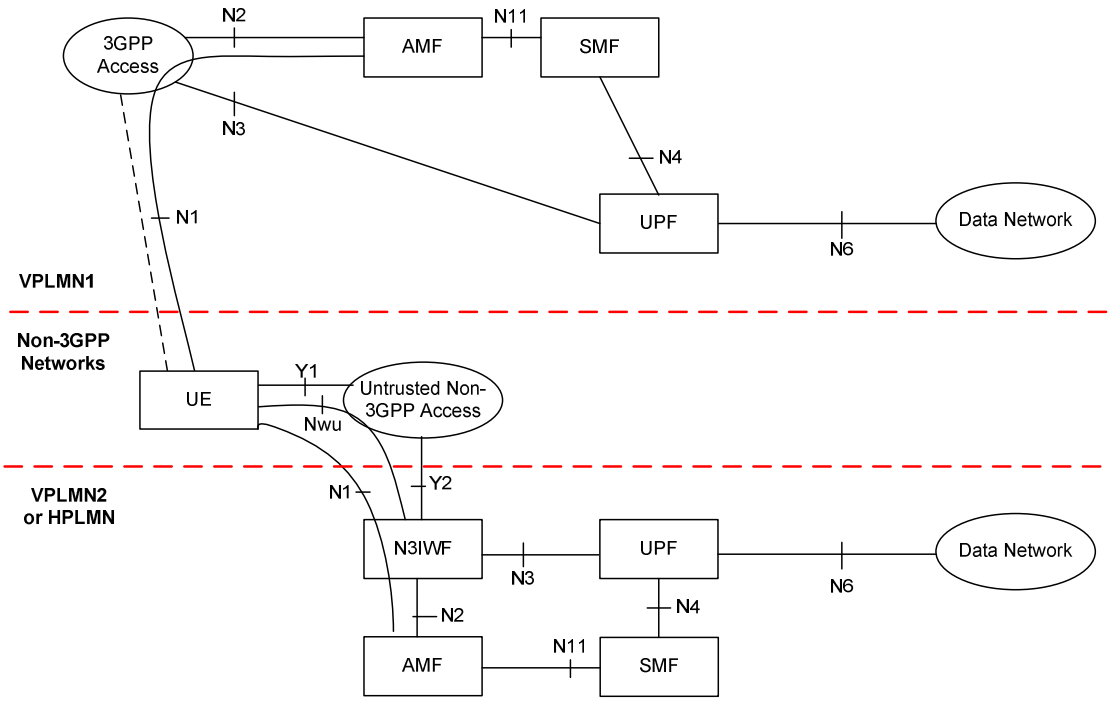


Figure 4.2.8.2.2-2: LBO Roaming architecture for 5G Core Network with untrusted non-3GPP access - N3IWF in a different PLMN from 3GPP access

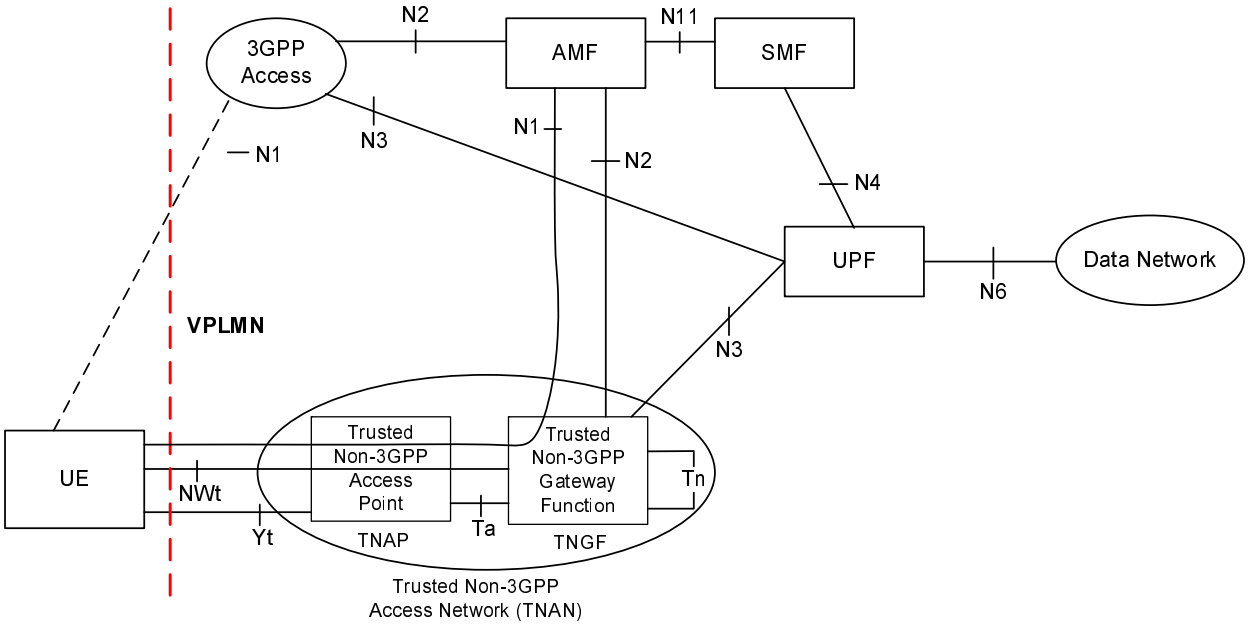


Figure 4.2.8.2.2-3: LBO Roaming architecture for 5G Core Network with trusted non-3GPP access using the same VPLMN as 3GPP access

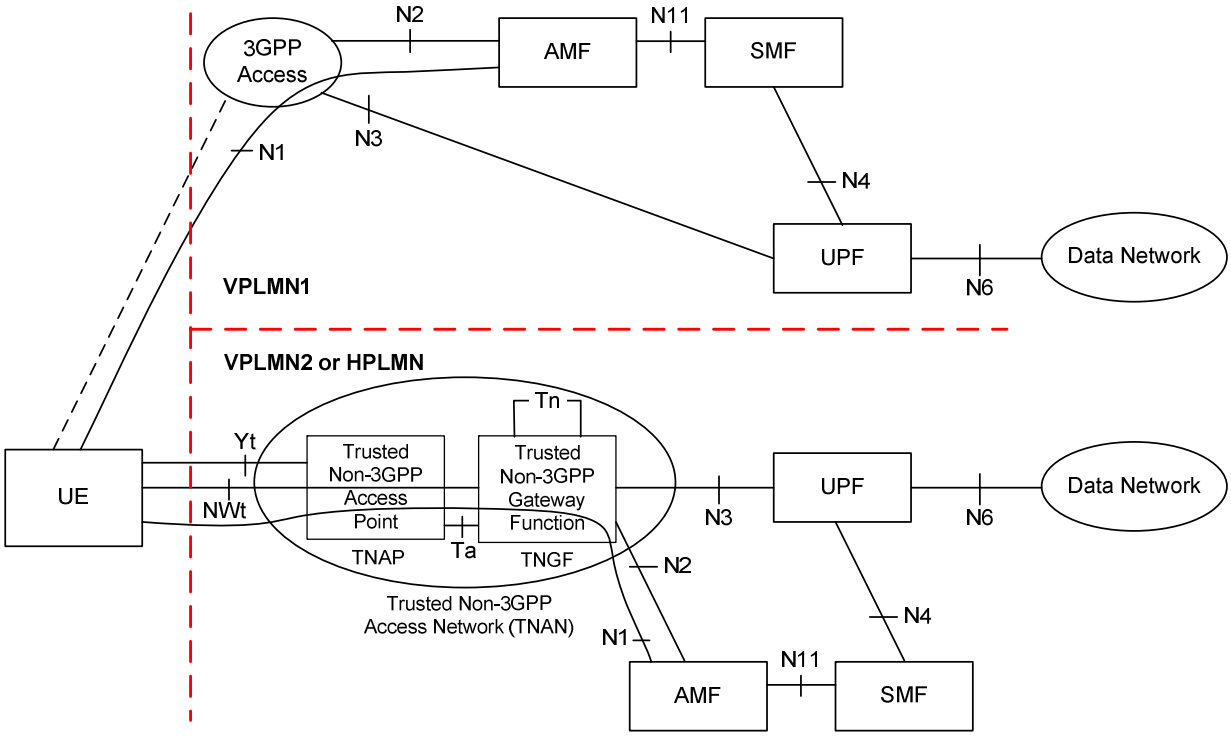


Figure 4.2.8.2.2-4: LBO Roaming architecture for 5G Core Network with trusted non-3GPP access using a different PLMN than 3GPP access

NOTE 1: The reference architecture in all above figures only shows the architecture and the network functions directly connected to support non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The reference architecture in all above figures supports service based interfaces for AMF, SMF and other NFs not represented in the figures.

NOTE 3: The two N2 instances in Figure 4.2.8.2.2-1 and in Figure 4.2.8.2.2-3 terminate to a single AMF for a UE which is connected to the same 5G Core Network over 3GPP access and non-3GPP access simultaneously.

NOTE 4: The two N3 instances in Figure 4.2.8.2.2-1 and in Figure 4.2.8.2.2-3 may terminate to different UPFs when different PDU Sessions are established over 3GPP access and non-3GPP access.

4.2.8.2.3 Home-routed Roaming Architecture

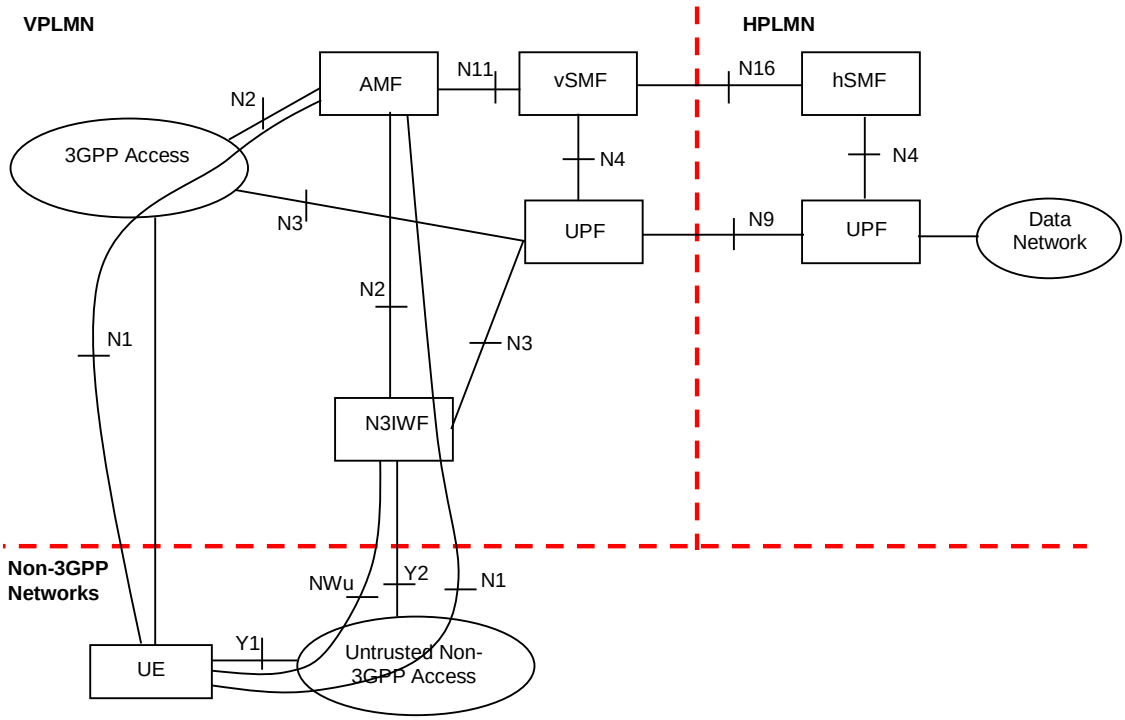


Figure 4.2.8.2.3-1: Home-routed Roaming architecture for 5G Core Network with untrusted non-3GPP access - N3IWF in the same VPLMN as 3GPP access

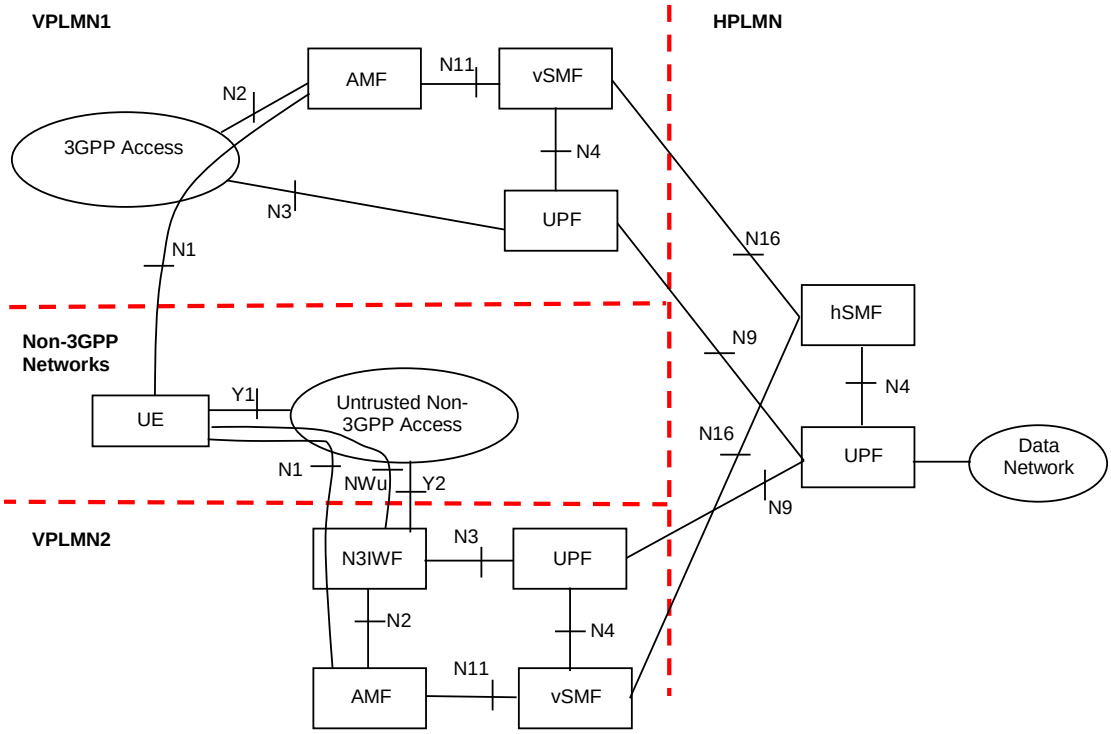


Figure 4.2.8.2.3-2: Home-routed Roaming architecture for 5G Core Network with untrusted non-3GPP access - N3IWF in a different VPLMN than 3GPP access

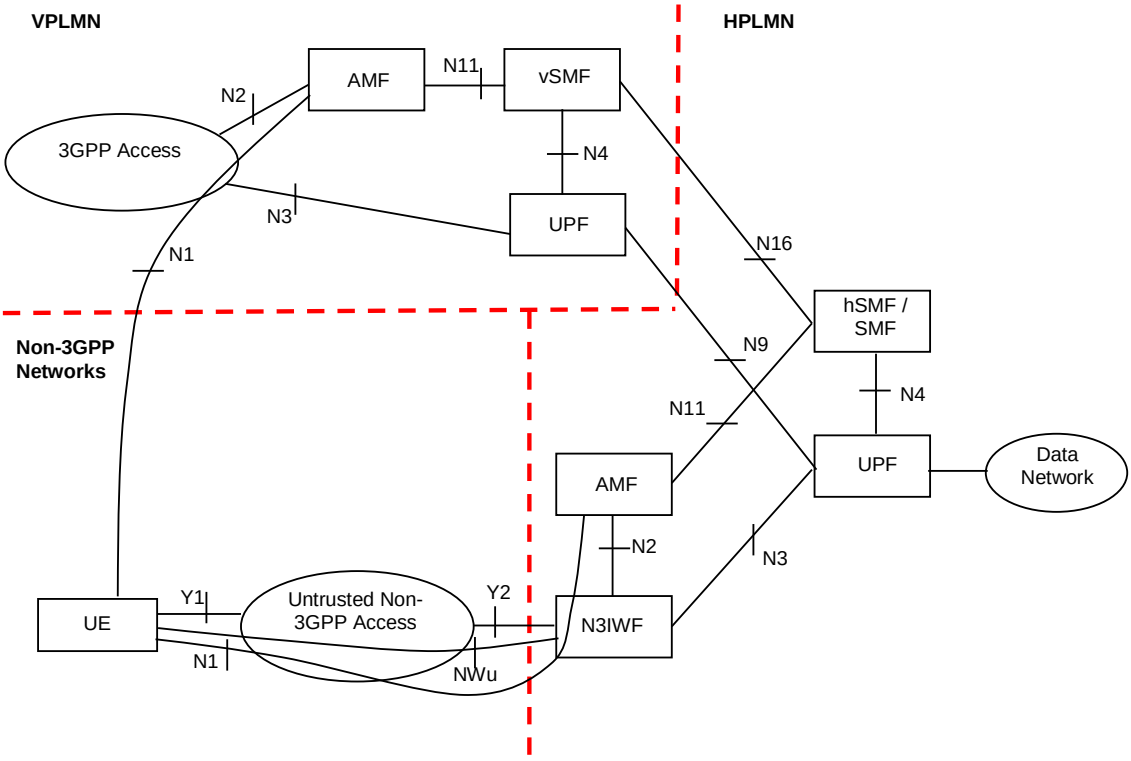


Figure 4.2.8.2.3-3: Home-routed Roaming architecture for 5G Core Network with untrusted non-3GPP access - N3IWF in HPLMN

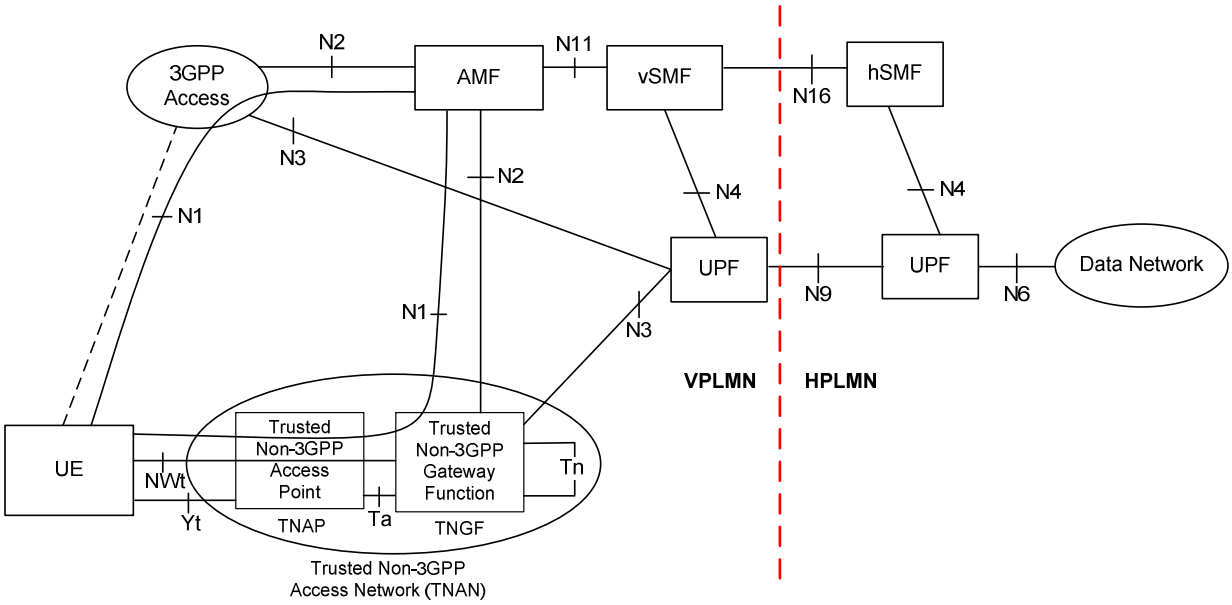


Figure 4.2.8.2.3-4: Home-routed Roaming architecture for 5G Core Network with trusted non-3GPP access using the same VPLMN as 3GPP access

NOTE 1: The reference architecture in all above figures only shows the architecture and the network functions directly connected to support non-3GPP access, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The two N2 instances in Figure 4.2.8.2.3-1 and in Figure 4.2.8.2.3-4 terminate to a single AMF for a UE which is connected to the same 5G Core Network over 3GPP access and non-3GPP access simultaneously.

4.2.8.3 Reference Points for Non-3GPP Access

4.2.8.3.1 Overview

The description of the reference points specific for the non-3GPP access:

N2, N3, N4, N6: these are defined in clause 4.2.

Y1 Reference point between the UE and the untrusted non-3GPP access (e.g. WLAN). This depends on the non-3GPP access technology and is outside the scope of 3GPP.

Y2 Reference point between the untrusted non-3GPP access and the N3IWF for the transport of NWu traffic.

Y4 Reference point between the 5G-RG and the W-AGF which transports the user plane traffic and the N1 NAS protocol. The definition of this interface is outside the scope of 3GPP.

Y5 Reference point between the FN-RG and the W-AGF. The definition of this interface is outside the scope of 3GPP.

Yt Reference point between the UE and the TNAP. See e.g. Figure 4.2.8.2.1-2.

Yt' Reference point between the N5CW devices and the TWAP. It is defined in clause 4.2.8.5.

NWu Reference point between the UE and N3IWF for establishing secure tunnel(s) between the UE and N3IWF so that control-plane and user-plane exchanged between the UE and the 5G Core Network is transferred securely over untrusted non-3GPP access.

NWt Reference point between the UE and the TNGF. A secure NWt connection is established over this reference point, as specified in TS 23.502 [3], clause 4.12a.2.2. NAS messages between the UE and the AMF are transferred via this NWt connection.

Ta A reference point between the TNAP and the TNGF, which is used to support an AAA interface. Ta requirements are documented in clause 4.2.8.3.2.

Tn A reference point between two TNGFs, which is used to facilitate UE mobility between different TNGFs (inter-TNGF mobility).

Tn and inter-TNGF mobility are not specified in this Release of the specification.

4.2.8.3.2 Requirements on Ta

Ta shall be able to

- Carry EAP-5G traffic and user location information before the NWt connection is established between the UE and the TNGF.
- Allow the UE and the TNGF to exchange IP traffic.

In deployments where the TNAP does not allocate the local IP addresses to UE(s), Ta shall be able to:

- Allow the UE to request and receive IP configuration from the TNAN (including a local IP address), e.g. with DHCP. This is to allow the UE to use an IP stack to establish a NWt connection between the UE and the TNGF.

NOTE: The "local IP address" is the IP address that allows the UE to contact the TNGF; the entity providing this local IP address is part of TNAN and out of 3GPP scope

In this Release of the specification, Ta is not specified.

4.2.8.4 Architecture Reference Model for Wireline Access network

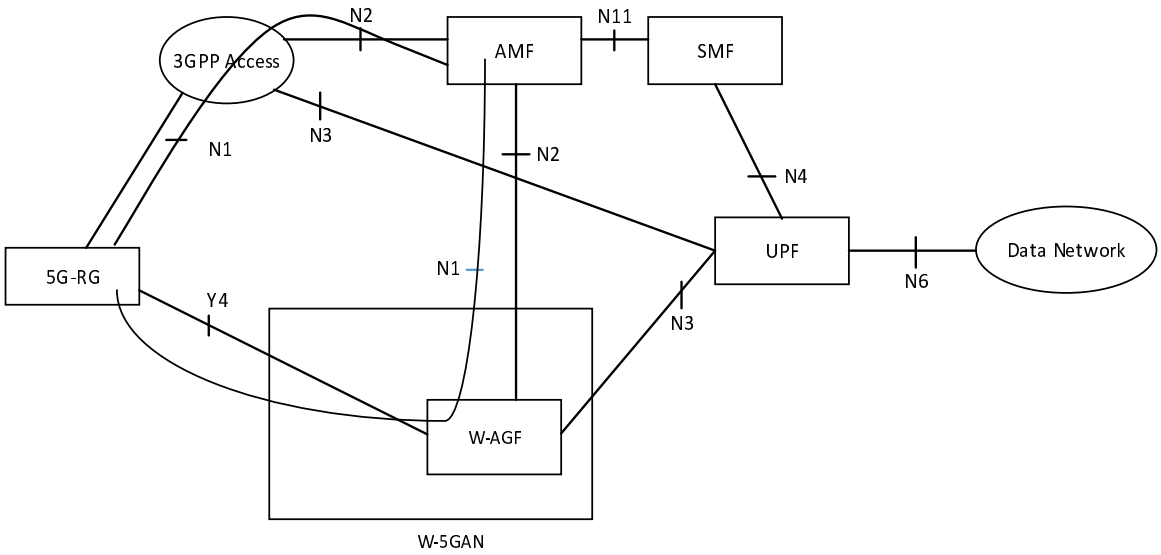


Figure 4.2.8.4-1: Non- roaming architecture for 5G Core Network for 5G-RG with Wireline 5G Access network and NG RAN

The 5G-RG can be connected to 5GC via W-5GAN, NG RAN or via both accesses.

NOTE 1: The reference architecture in figure 4.2.8.4-1 only shows the architecture and the network functions directly connected to Wireline 5G Access Network, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 2: The reference architecture in figure 4.2.8.4-1 supports service based interfaces for AMF, SMF and other NFs not represented in the figure.

NOTE 3: The two N2 instances in Figure 4.2.8.4-1 apply to a single AMF for a 5G-RG which is simultaneously connected to the same 5G Core Network over 3GPP access and Wireline 5G Access Network.

NOTE 4 The two N3 instances in Figure 4.2.8. 4-1 may apply to different UPFs when different PDU Sessions are established over 3GPP access and Wireline 5G Access Network.

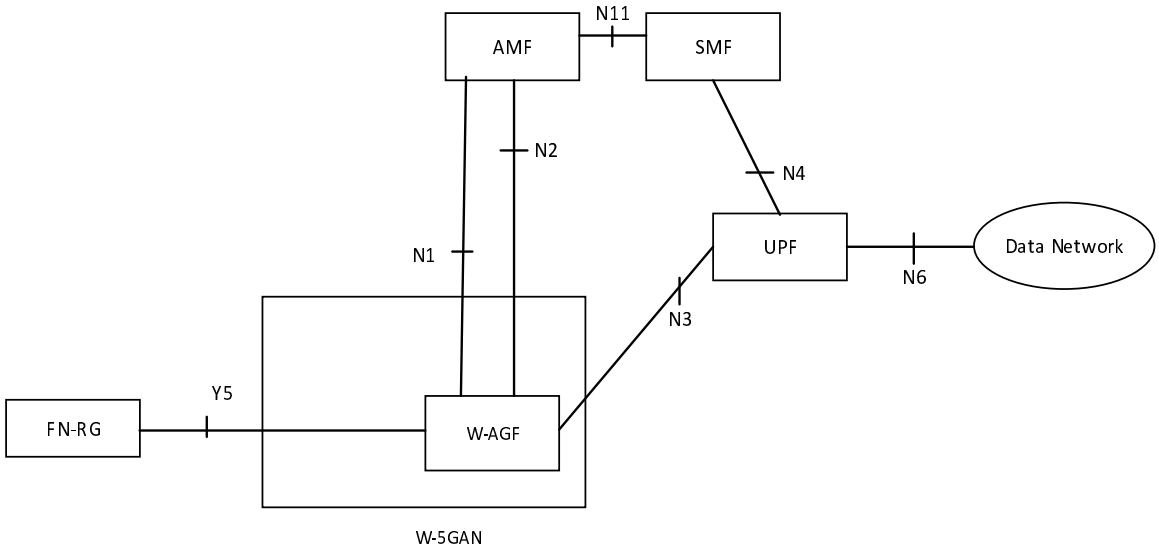


Figure 4.2.8.4-2: Non- roaming architecture for 5G Core Network for FN-RG with Wireline 5G Access network and NG RAN

The N1 for the FN-RG, which is not 5G capable, is terminated on W-AGF which acts on behalf of the FN-RG.

The FN-RG can only be connected to 5GC via W-5GAN.

NOTE 5: The reference architecture in figure 4.2.8.4-2 only shows the architecture and the network functions directly connected to Wireline 5G Access Network, and other parts of the architecture are the same as defined in clause 4.2.

NOTE 6: The reference architecture in figure 4.2.8.4-1 supports service based interfaces for AMF, SMF and other NFs not represented in the figure.

4.2.8.5 Access to 5GC from devices that do not support 5GC NAS over WLAN access

4.2.8.5.1 General

The devices that do not support 5GC NAS signalling over WLAN access are referred to as "Non-5G-Capable over WLAN" devices, or N5CW devices for short. A N5CW device is not capable to operate as a 5G UE that supports 5GC NAS signalling over a WLAN access network, however, it may be capable to operate as a 5G UE over NG-RAN.

Clause 4.2.8.5 specifies the 5GC architectural enhancements that enable N5CW devices to access 5GC via trusted WLAN access networks. A trusted WLAN access network is a particular type of a Trusted Non-3GPP Access Network (TNAN) that supports a WLAN access technology, e.g. IEEE 802.11. Not all trusted WLAN access networks support 5GC access from N5CW devices. To support 5GC access from N5CW devices, a trusted WLAN access network must support the special functionality specified below (e.g. it must support a TWIF function).

When a N5CW device performs an EAP-based access authentication procedure to connect to a trusted WLAN access network, the N5CW device may simultaneously be registered to a 5GC of a PLMN. The 5GC registration is performed by the TWIF function (see next clause) in the trusted WLAN access network, on behalf of the N5CW device. The type of EAP authentication procedure, which is used during the 5GC registration to authenticate the N5CW device, is specified in TS 33.501 [29].

4.2.8.5.2 Reference Architecture

The architecture diagram below is based on the general 5GS architecture diagrams in clause 4.2 and shows the main network functions required to support 5GC access from N5CW devices. Other network functions are not shown for simplicity.

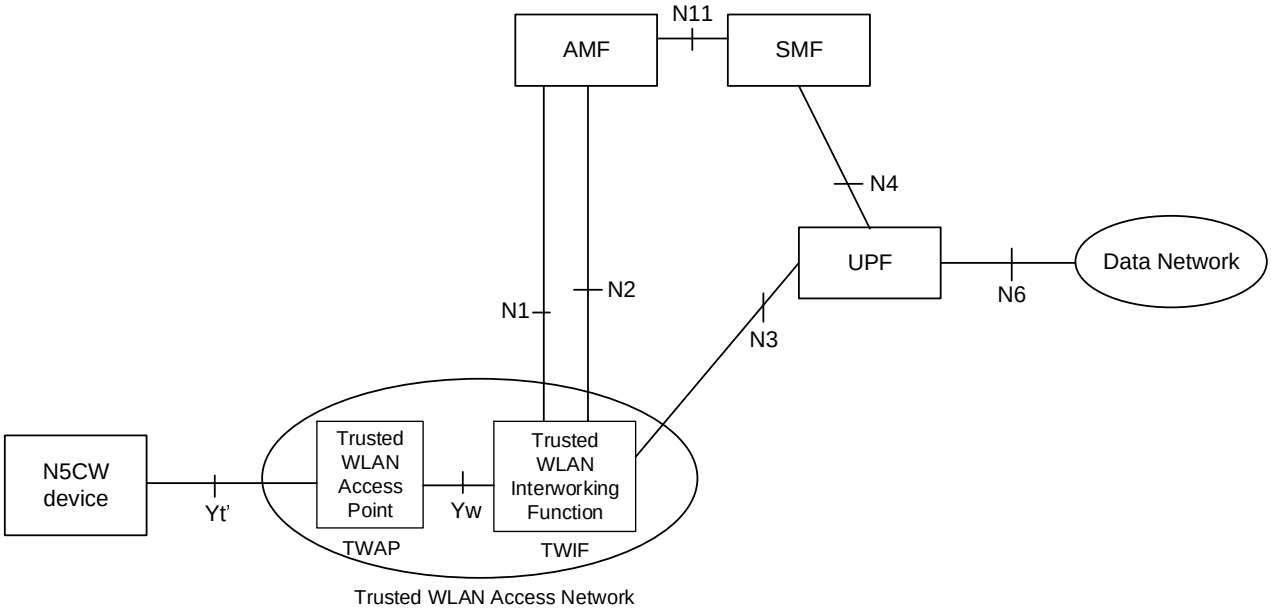


Figure 4.2.8.5.2-1: Non-roaming and LBO Roaming Architecture for supporting 5GC access from N5CW devices

4.2.8.5.3 Network Functions

Trusted WLAN Access Point (TWAP): It is a particular type of a Trusted Non-3GPP Access Point (TNAP) specified in clause 4.2.8.2, that supports a WLAN access technology, e.g. IEEE 802.11. This function is outside the scope of the 3GPP specifications.

Trusted WLAN Interworking Function (TWIF): It provides interworking functionality that enables N5CW devices to access 5GC. The TWIF supports the following functions:

- Terminates the N1, N2 and N3 interfaces.
- Implements the AMF selection procedure.
- Implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device.
- On the user plane, it relays protocol data units (PDUs) between the Yw interface and the N3 interface.
- May implement a local mobility anchor within the trusted WLAN access network.

4.2.8.5.4 Reference Points

The Yt' and Yw reference points are both outside the scope of the 3GPP specifications. The Yt' reference point transports WLAN messages (e.g. IEEE 802.11 messages), while the Yw reference point:

- Shall be able to transport authentication messages between the TNAP and the TWIF for enabling authentication of a N5CW device;
- Shall allow the N5CW device to request and receive IP configuration from the TWIF, including an IP address, e.g. with DHCP.
- Shall support the transport of user-plane traffic for the N5CW device.

The N1, N2 and N3 reference points are the same reference points defined in clause 4.2.7.

4.2.9 Network Analytics architecture

The Network Analytics architecture is defined in TS 23.288 [86].

4.2.10 Architecture Reference Model for ATSSS Support

In order to support the ATSSS feature, the 5G System Architecture is extended as shown in Figure 4.2.10-1, Figure 4.2.10-2 and Figure 4.2.10-3. The additional functionality that is supported by the UE and the network functions shown in these figures is specified in clause 5.32 below. In summary:

- The UE supports one or more of the steering functionalities specified in clause 5.32.6, e.g. MPTCP functionality and/or ATSSS-LL functionality. Each steering functionality in the UE enables traffic steering, switching and splitting across 3GPP access and non-3GPP access, in accordance with the ATSSS rules provided by the network. The ATSSS-LL functionality is mandatory in the UE for MA PDU Session of type Ethernet.

- The UPF may support MPTCP Proxy functionality, which communicates with the MPTCP functionality in the UE by using the MPTCP protocol (IETF RFC 8684 [81]).

- The UPF may support ATSSS-LL functionality, which is similar to the ATSSS-LL functionality defined for the UE. There is no user plane protocol defined between the ATSSS-LL functionality in the UE and the ATSSS-LL functionality in the UPF. The ATSSS-LL functionality in the UPF is not shown in the following three figures.

NOTE 1: ATSSS-LL functionality is needed in the 5GC for MA PDU Session of type Ethernet.

- In addition, the UPF supports Performance Measurement Functionality (PMF), which may be used by the UE to obtain access performance measurements (see clause 5.32.5) over the user-plane of 3GPP access and/or over the user-plane of non-3GPP access.

- The AMF, SMF and PCF are extended with new functionality that is further discussed in clause 5.32.

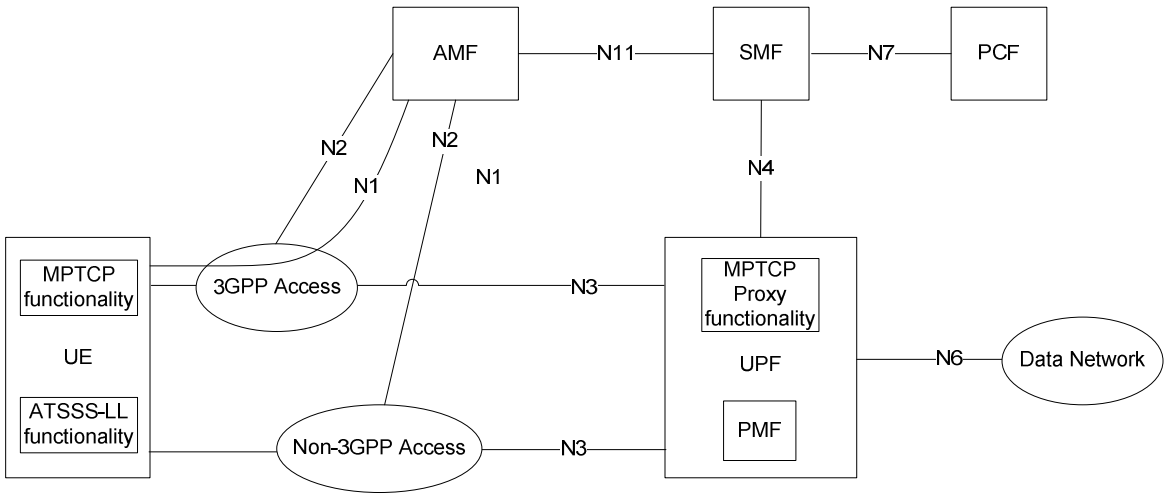


Figure 4.2.10-1: Non-roaming and Roaming with Local Breakout architecture for ATSSS support

NOTE 2: The interactions between the UE and PCF that may be required for ATSSS control are specified in TS 23.503 [45].

NOTE 3: A UPF that supports the MPTCP Proxy functionality and the PMF can be connected via an N9 reference point, instead of the N3 reference point.

Figure 4.2.10-2 shows the 5G System Architecture for ATSSS support in a roaming case with home-routed traffic and when the UE is registered to the same VPLMN over 3GPP and non-3GPP accesses. In this case, the MPTCP Proxy functionality and the PMF are located in the H-UPF.

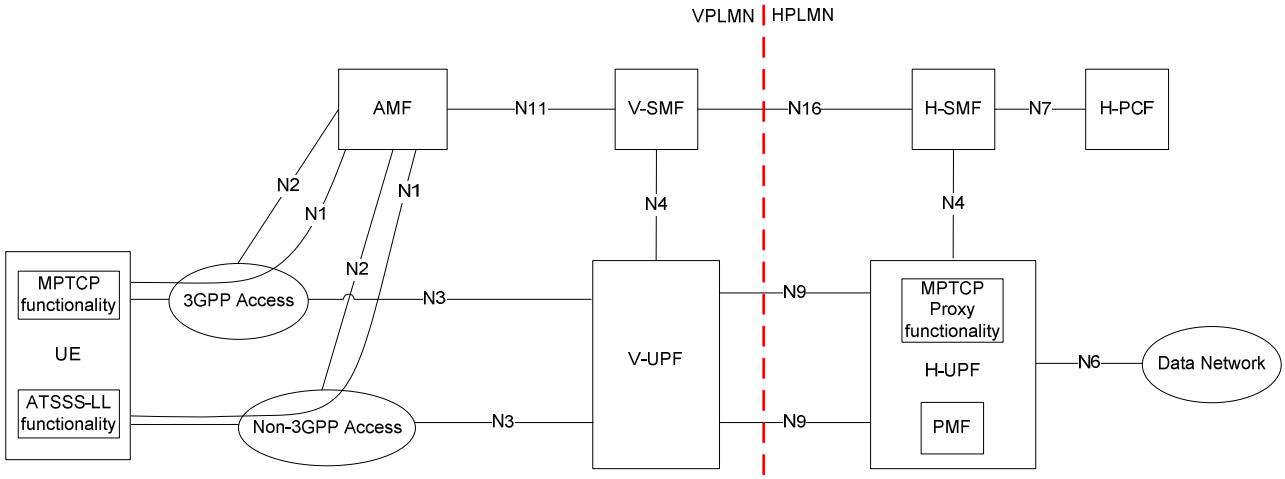


Figure 4.2.10-2: Roaming with Home-routed architecture for ATSSS support (UE registered to the same VPLMN)

Figure 4.2.10-3 shows the 5G System Architecture for ATSSS support in a roaming case with home-routed traffic and when the UE is registered to a VPLMN over 3GPP access and to HPLMN over non-3GPP access (i.e. the UE is registered to different PLMNs). In this case, the MPTCP Proxy functionality and the PMF are located in the H-UPF.

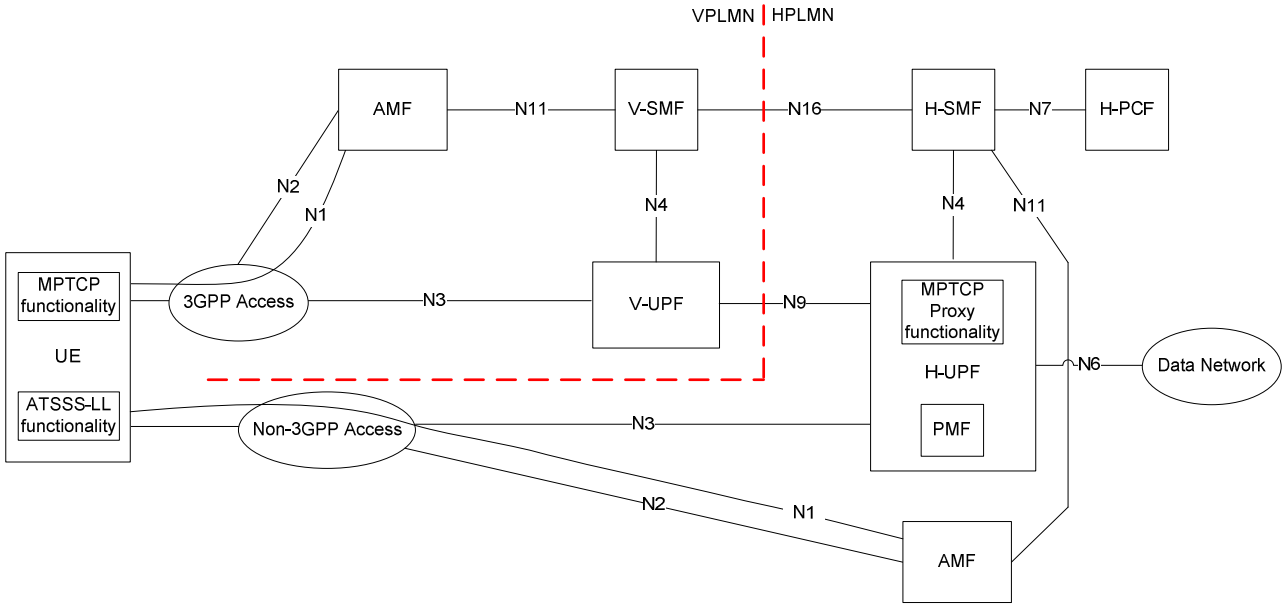


Figure 4.2.10-3: Roaming with Home-routed architecture for ATSSS support (UE registered to different PLMNs)

4.3 Interworking with EPC

4.3.1 Non-roaming architecture

Figure 4.3.1-1 represents the non-roaming architecture for interworking between 5GS and EPC/E-UTRAN.

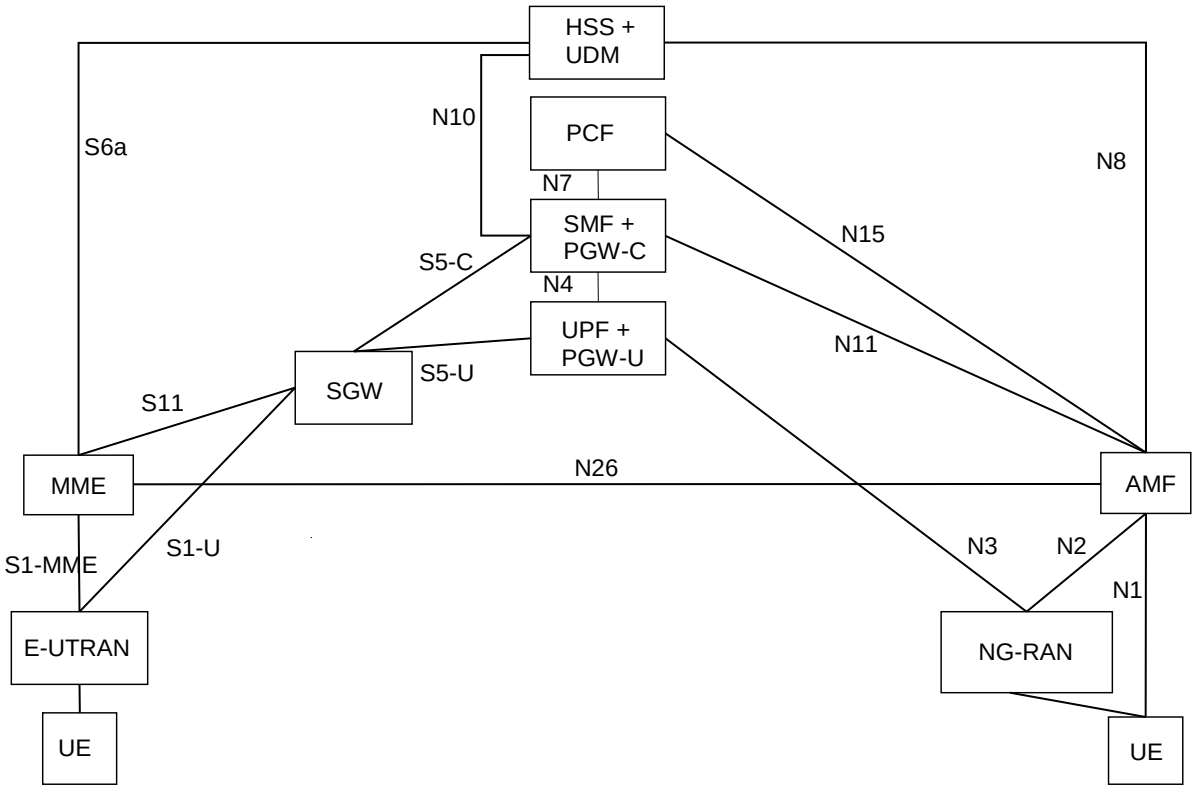


Figure 4.3.1-1: Non-roaming architecture for interworking between 5GS and EPC/E-UTRAN

NOTE 1: N26 interface is an inter-CN interface between the MME and 5GS AMF in order to enable interworking between EPC and the NG core. Support of N26 interface in the network is optional for interworking. N26 supports subset of the functionalities (essential for interworking) that are supported over S10.

NOTE 2: PGW-C + SMF and UPF + PGW-U are dedicated for interworking between 5GS and EPC, which are optional and are based on UE MM Core Network Capability and UE subscription. UEs that are not subject to 5GS and EPC interworking may be served by entities not dedicated for interworking, i.e. by either by PGW or SMF/UPF.

NOTE 3: There can be another UPF (not shown in the figure above) between the NG-RAN and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards an additional UPF, if needed.

NOTE 4: Figures and procedures in this specification that depict an SGW make no assumption whether the SGW is deployed as a monolithic SGW or as an SGW split into its control-plane and user-plane functionality as described in TS 23.214 [32].

4.3.2 Roaming architecture

Figure 4.3.2-1 represents the Roaming architecture with local breakout and Figure 4.3.2-2 represents the Roaming architecture with home-routed traffic for interworking between 5GS and EPC/E-UTRAN.

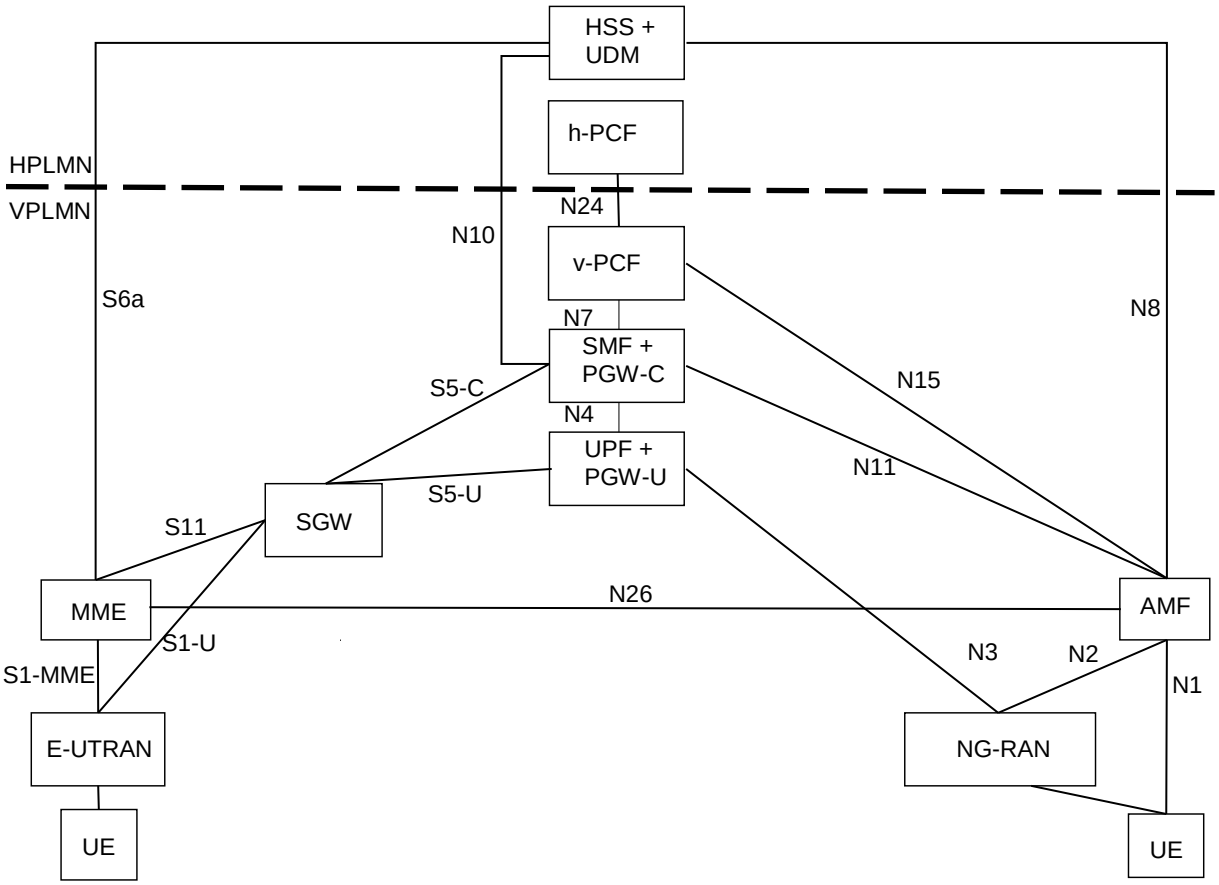


Figure 4.3.2-1: Local breakout roaming architecture for interworking between 5GS and EPC/E-UTRAN

NOTE 1: There can be another UPF (not shown in the figure above) between the NG-RAN and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards the additional UPF, if needed.

NOTE 2: S9 interface from EPC is not required since no known deployment exists.

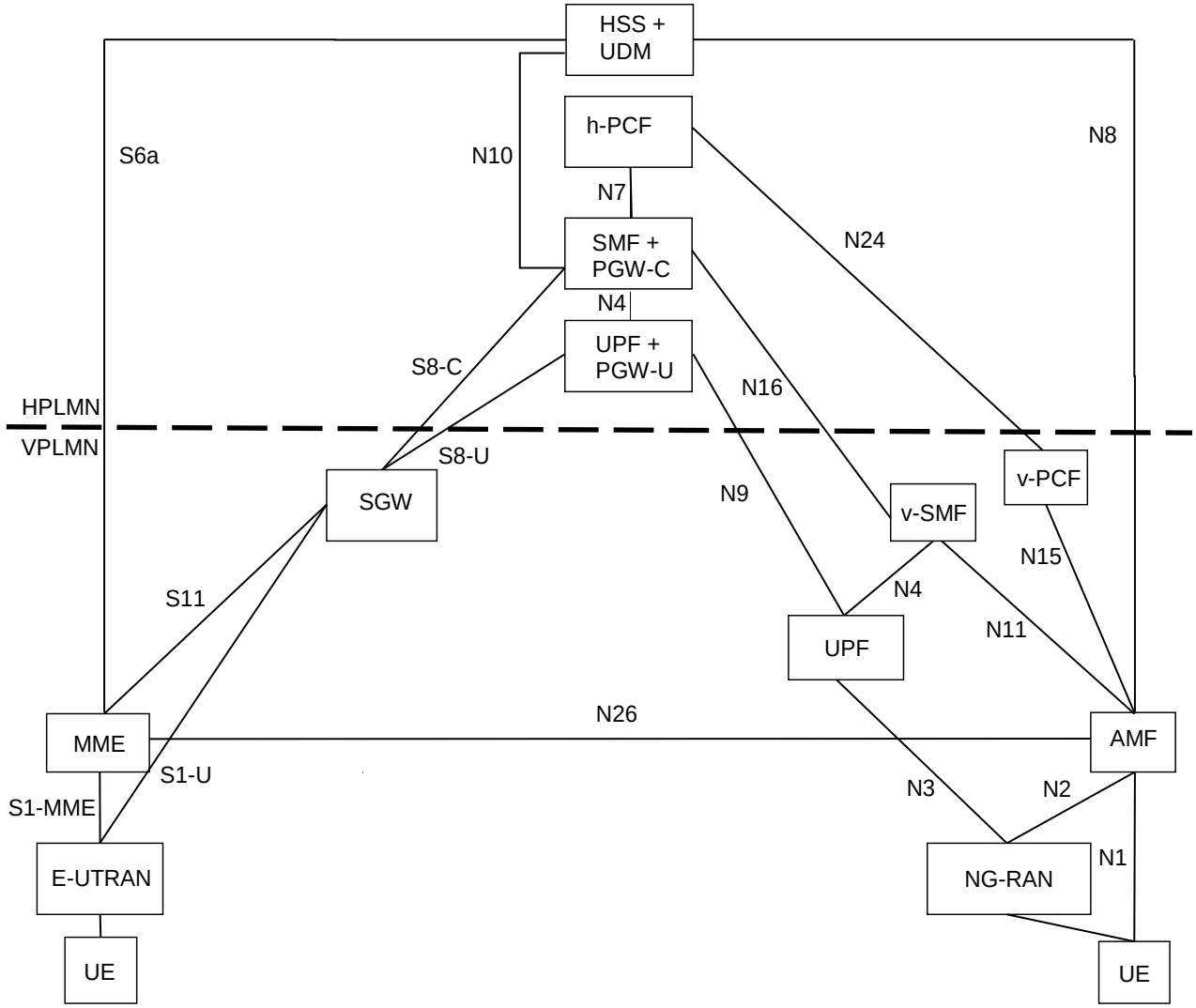


Figure 4.3.2-2: Home-routed roaming architecture for interworking between 5GS and EPC/E-UTRAN

4.3.3 Interworking between 5GC via non-3GPP access and E-UTRAN connected to EPC

4.3.3.1 Non-roaming architecture

Figure 4.3.3-1 represents the non-roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

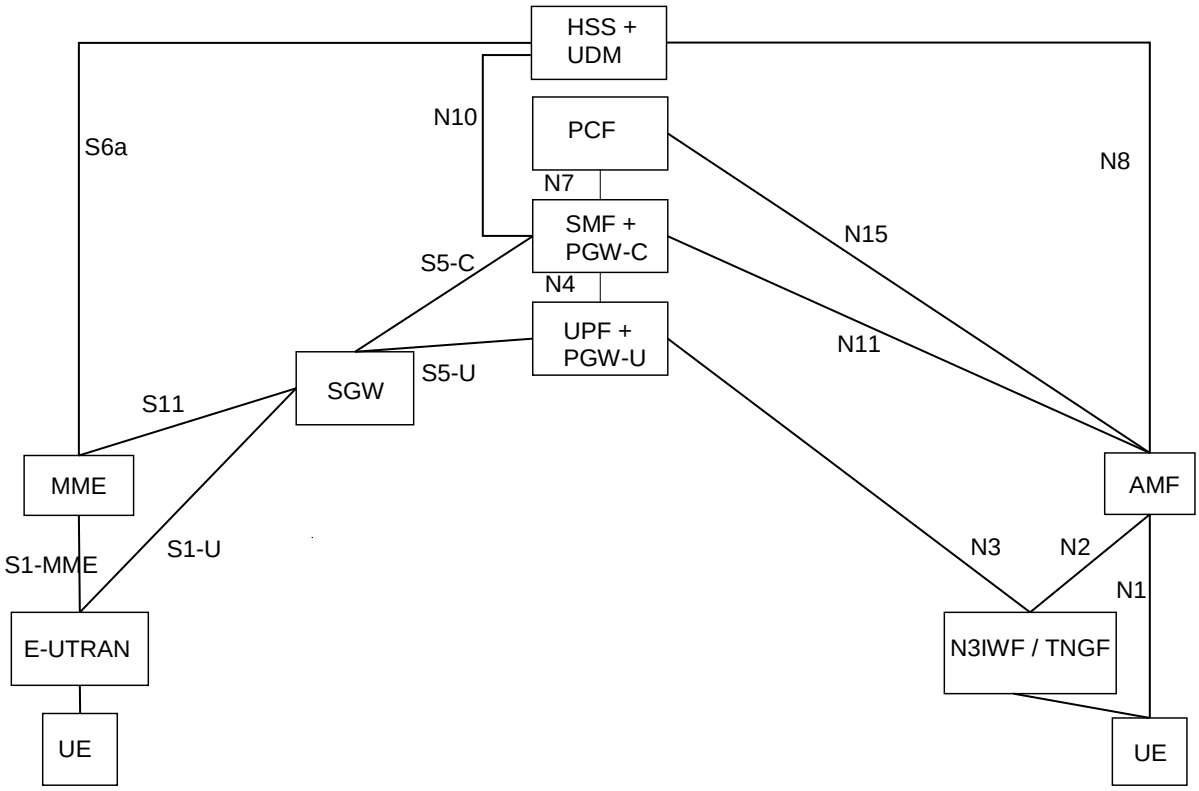


Figure 4.3.3.1-1: Non-roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN

NOTE 1: There can be another UPF (not shown in the figure above) between the N3IWF/TNGF and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards an additional UPF, if needed.

NOTE 2: N26 interface is not precluded, but it is not shown in the figure because it is not required for the interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

4.3.3.2 Roaming architecture

Figure 4.3.3.2-1 represents the Roaming architecture with local breakout and Figure 4.3.3.2-2 represents the Roaming architecture with home-routed traffic for interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

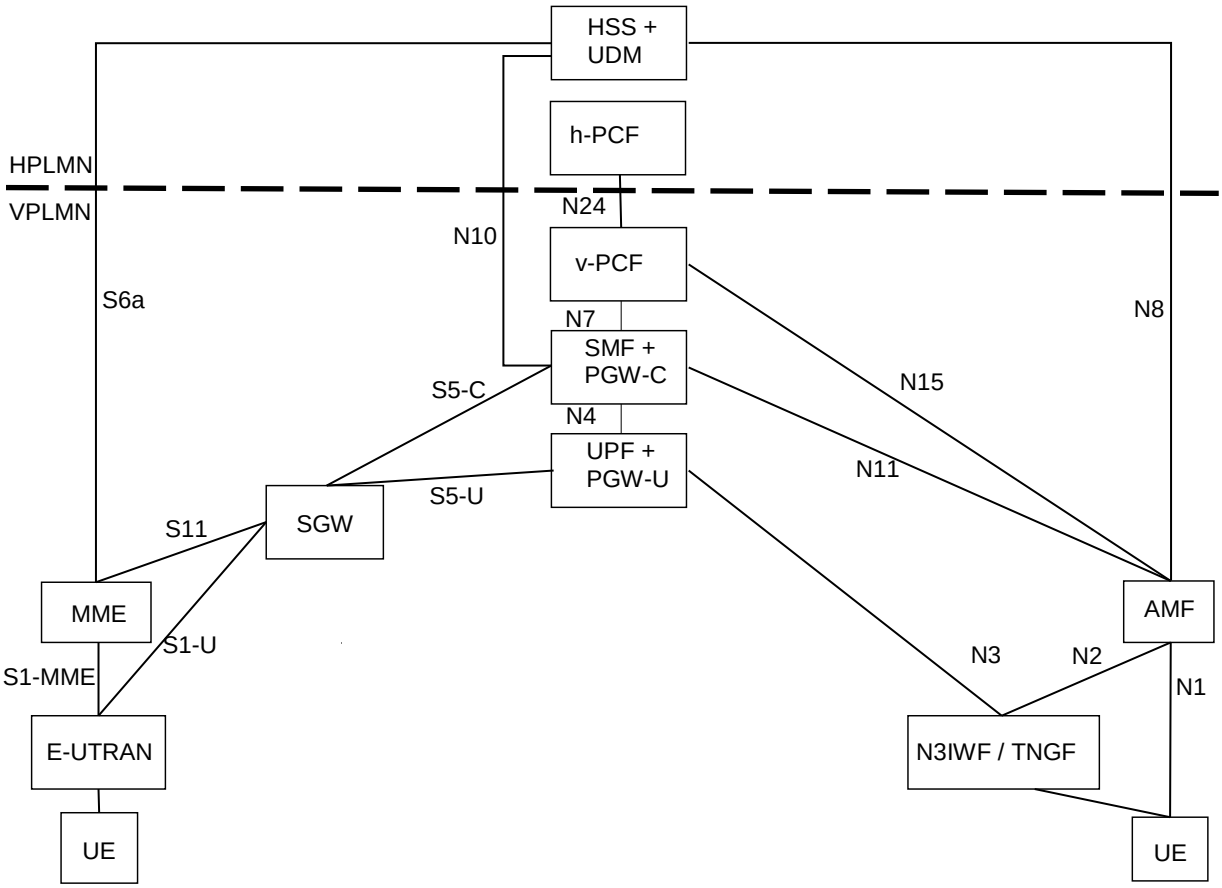


Figure 4.3.3.2-1: Local breakout roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN

NOTE 1: There can be another UPF (not shown in the figure above) between the N3IWF/TNGF and the UPF + PGW-U, i.e. the UPF + PGW-U can support N9 towards the additional UPF, if needed.

NOTE 2: S9 interface from EPC is not required since no known deployment exists.

NOTE 3: N26 interface is not precluded, but it not shown in the figure because it is not required for the interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

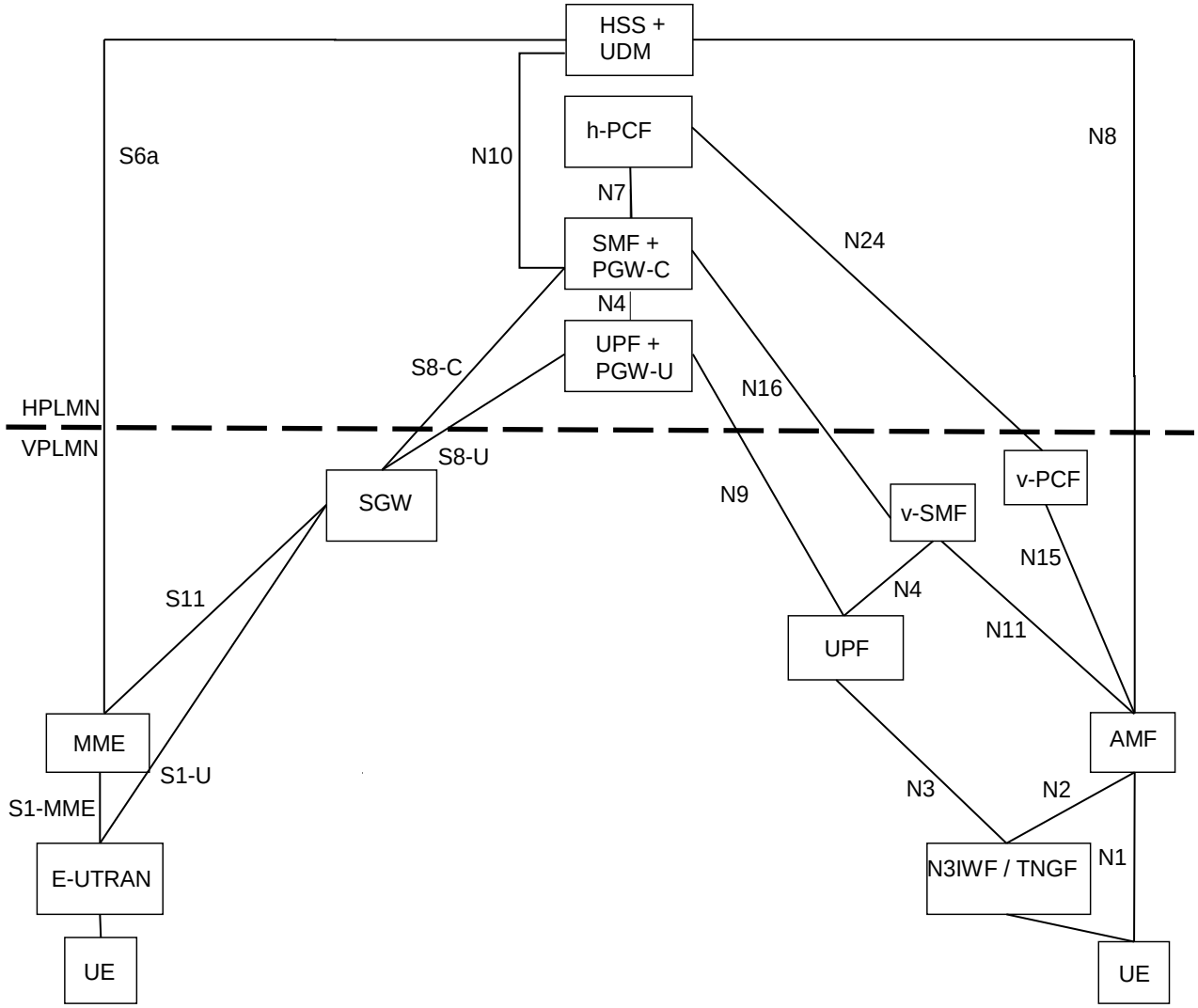


Figure 4.3.3.2-2: Home-routed roaming architecture for interworking between 5GC via non-3GPP access and EPC/E-UTRAN

NOTE 4: N26 interface is not precluded, but it not shown in the figure because it is not required for the interworking between 5GC via non-3GPP access and EPC/E-UTRAN.

4.3.4 Interworking between ePDG connected to EPC and 5GS

4.3.4.1 Non-roaming architecture

Figure 4.3.4.1-1 represents the non-roaming architecture for interworking between ePDG/EPC and 5GS.

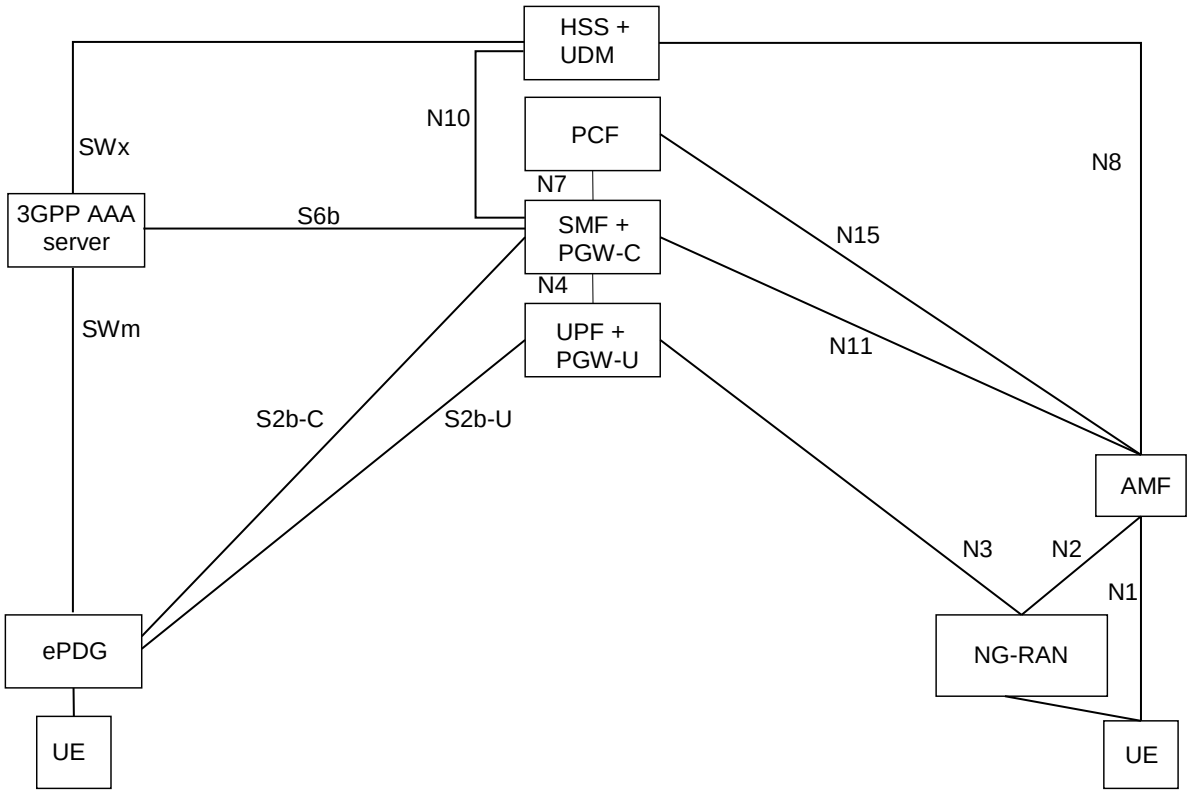


Figure 4.3.4.1-1: Non-roaming architecture for interworking between ePDG/EPC and 5GS

NOTE 1: The details of the interfaces between the UE and the ePDG, and between EPC nodes (i.e. SWm, SWx, S2b and S6b), are documented in TS 23.402 [43].

NOTE 2: Interworking with ePDG is only supported with GTP based S2b. S6b interface is optional (see TS 23.502 [3] clause 4.11.4.3.6).

4.3.4.2 Roaming architectures

Figure 4.3.4.2-1 represents the Roaming architecture with local breakout and Figure 4.3.4.2-2 represents the Roaming architecture with home-routed traffic for interworking between ePDG/EPC and 5GS.

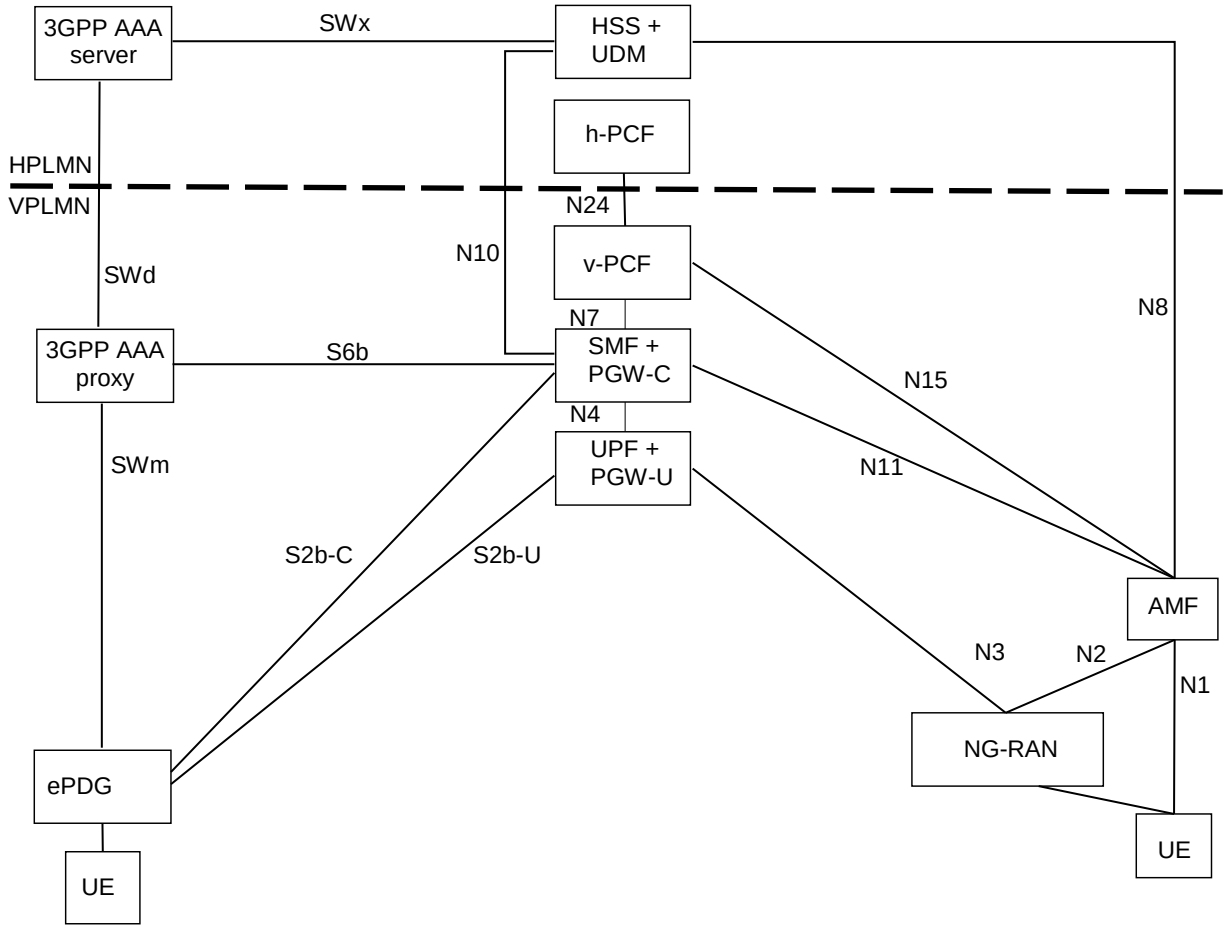


Figure 4.3.4.2-1: Local breakout roaming architecture for interworking between ePDG/EPC and 5GS

NOTE 1: The details of the interfaces between the UE and the ePDG, and between EPC nodes (i.e. SWm, SWd, SWx, S2b and S6b), are documented in TS 23.402 [43].

NOTE 2: Interworking with ePDG is only supported with GTP based S2b. S6b interface is optional (see TS 23.502 [3] clause 4.11.4.3.6).

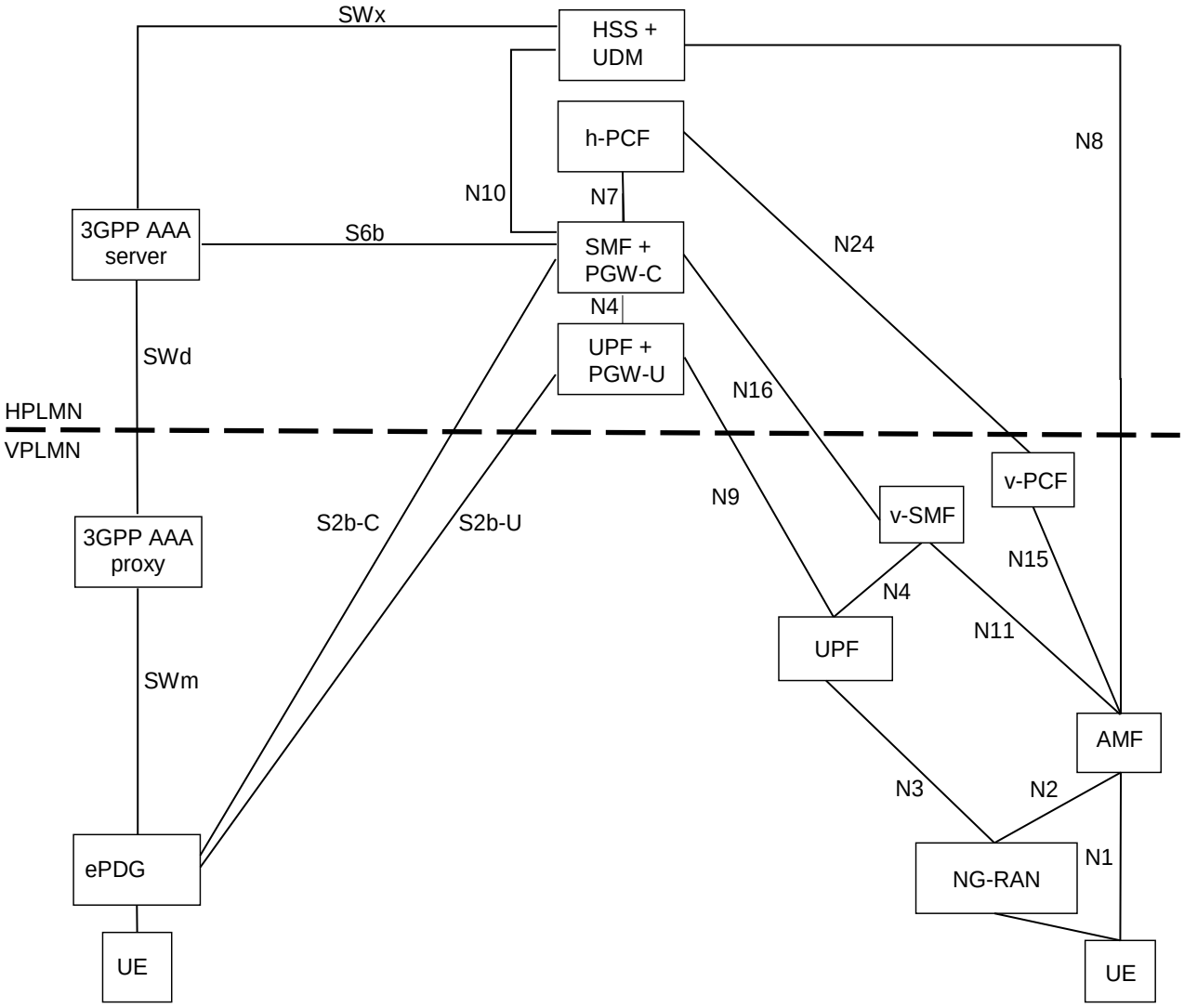


Figure 4.3.4.2-2: Home-routed roaming architecture for interworking between ePDG/EPC and 5GS

NOTE 1: The details of the interfaces between the UE and the ePDG, and between EPC nodes (i.e. SWm, SWd, SWx, S2b and S6b), are documented in TS 23.402 [43].

NOTE 2: Interworking with ePDG is only supported with GTP based S2b. S6b interface is optional (see TS 23.502 [3] clause 4.11.4.3.6).

4.3.5 Service Exposure in Interworking Scenarios

4.3.5.1 Non-roaming architecture

Figure 4.3.5.1-1 shows the non-roaming architecture for Service Exposure for EPC-5GC Interworking. If the UE is capable of mobility between EPS and 5GS, the network is expected to associate the UE with an SCEF+NEF node for Service Capability Exposure.

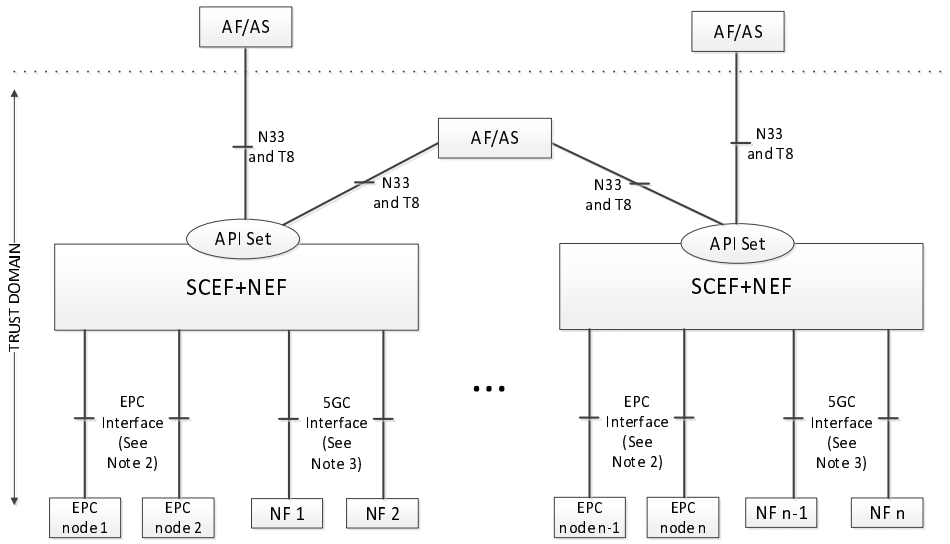


Figure 4.3.5.1 1: Non-roaming Service Exposure Architecture for EPC-5GC Interworking

NOTE 1: In Figure 4.3.5.1-1, Trust domain for SCEF+NEF is same as Trust domain for SCEF as defined in TS 23.682 [36].

NOTE 2: In Figure 4.3.5.1-1, EPC Interface represents southbound interfaces between SCEF and EPC nodes e.g. the S6t interface between SCEF and HSS, the T6a interface between SCEF and MME, etc. All southbound interfaces from SCEF are defined in TS 23.682 [36] and are not shown for the sake of simplicity.

NOTE 3: In Figure 4.3.5.1-1, 5GC Interface represents southbound interfaces between NEF and 5GC Network Functions e.g. N29 interface between NEF and SMF, N30 interface between NEF and PCF, etc. All southbound interfaces from NEF are not shown for the sake of simplicity.

NOTE 4: Interaction between the SCEF and NEF within the combined SCEF+NEF is required. For example, when the SCEF+NEF supports monitoring APIs, the SCEF and NEF need to share context and state information on a UE's configured monitoring events if the UE moves between from EPC and 5GC.

NOTE 5: The north-bound APIs which can be supported by an EPC or 5GC network are discovered by the SCEF+NEF node via the CAPIF function and/or via local configuration of the SCEF+NEF node. Different sets of APIs can be supported by the two network types.

4.3.5.2 Roaming architectures

Figure 4.3.5.2-1 represents the roaming architecture for Service Exposure for EPC-5GC Interworking. This architecture is applicable to both the home routed roaming and local breakout roaming.

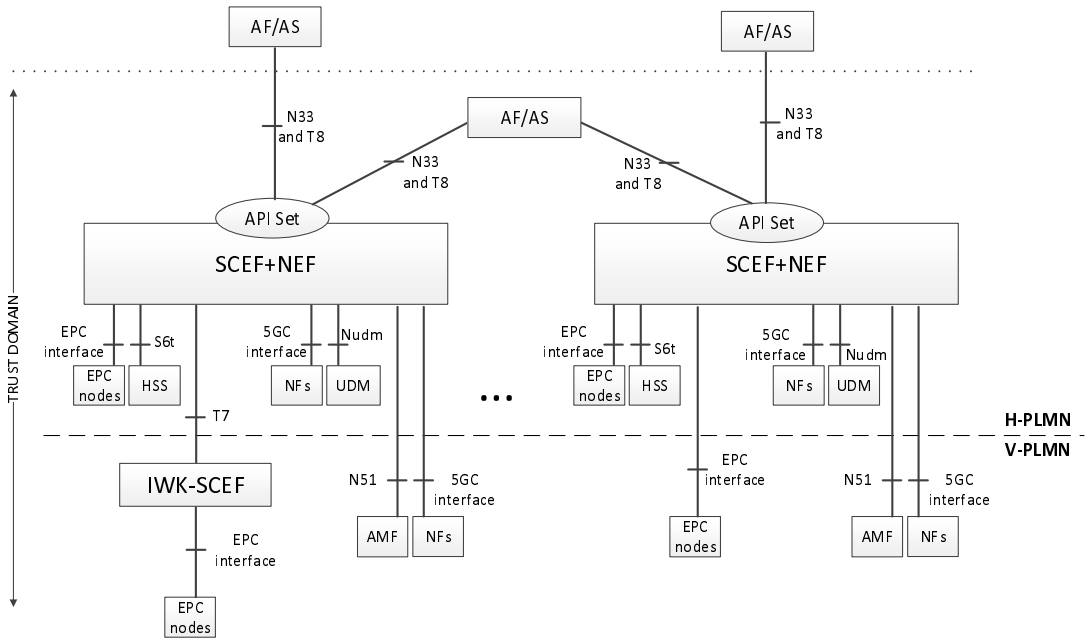


Figure 4.3.5.2-1: Roaming Service Exposure Architecture for EPC-5GC Interworking

NOTE: Figure 4.3.5.2-1 does not include all the interfaces, and network elements or network functions that may be connected to SCEF+NEF.

4.4 Specific services

4.4.1 Public Warning System

The Public Warning System architecture for 5G System is specified in TS 23.041 [46].

4.4.2 SMS over NAS

4.4.2.1 Architecture to support SMS over NAS

Figure 4.4.2.1-1 shows the non-roaming architecture to support SMS over NAS using the Service-based interfaces within the Control Plane.

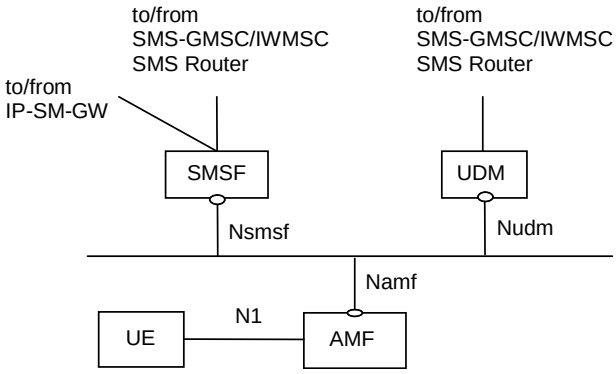


Figure 4.4.2.1-1: Non-roaming System Architecture for SMS over NAS

Figure 4.4.2.1-2 shows the non-roaming architecture to support SMS over NAS using the reference point representation.

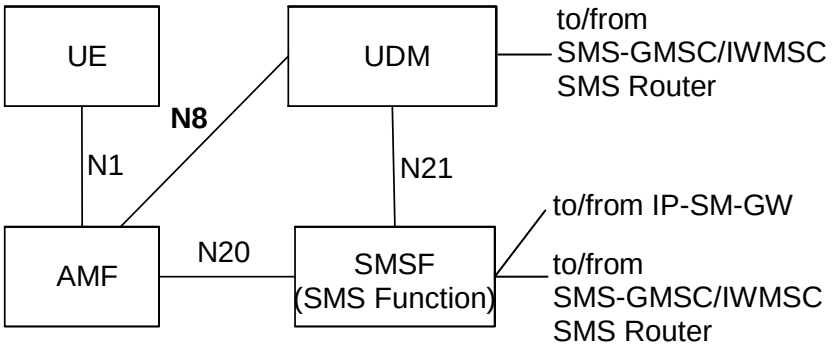


Figure 4.4.2.1-2: Non-roaming System Architecture for SMS over NAS in reference point representation

NOTE 1: SMS Function (SMSF) may be connected to the SMS-GMSC/IWMSC/SMS Router via one of the standardized interfaces as shown in TS 23.040 [5].

NOTE 2: UDM may be connected to the SMS-GMSC/IWMSC/SMS Router via one of the standardized interfaces as shown in TS 23.040 [5].

NOTE 3: Each UE is associated with only one SMS Function in the registered PLMN.

NOTE 4: SMSF re-allocation while the UE is in RM-REGISTERED state in the serving PLMN is not supported in this Release of the specification. When serving AMF is re-allocated for a given UE, the source AMF includes SMSF identifier as part of UE context transfer to target AMF. If the target AMF, e.g. in the case of inter-PLMN mobility, detects that no SMSF has been selected in the serving PLMN, then the AMF performs SMSF selection as specified in clause 6.3.10.

NOTE 5: To support MT SMS domain selection by IP-SM-GW/SMS Router, IP-SM-GW/SMS Router may connect to SGs MSC, MME and SMSF via one of the standardized interfaces as shown in TS 23.040 [5].

Figure 4.4.2.1-3 shows the roaming architecture to support SMS over NAS using the Service-based interfaces within the Control Plane.

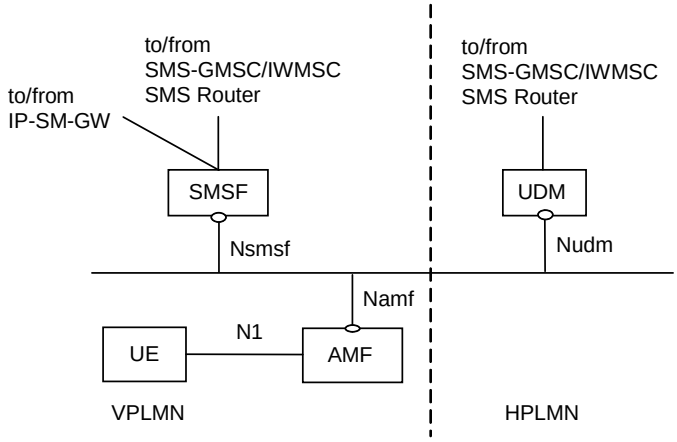


Figure 4.4.2.1-3: Roaming architecture for SMS over NAS

Figure 4.4.2.1-4 shows the roaming architecture to support SMS over NAS using the reference point representation.

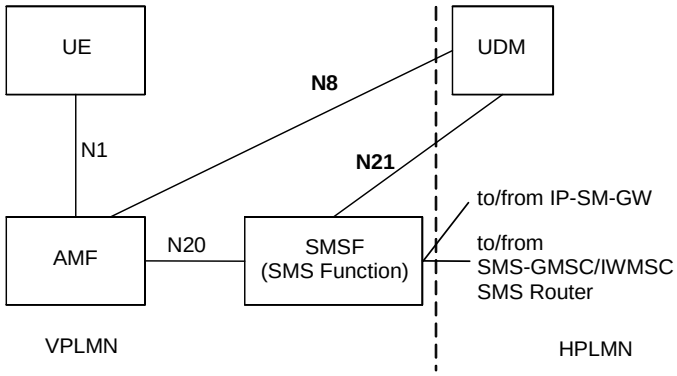


Figure 4.4.2.1-4: Roaming architecture for SMS over NAS in reference point representation

4.4.2.2 Reference point to support SMS over NAS

N1: Reference point for SMS transfer between UE and AMF via NAS.

Following reference points are realized by service based interfaces:

N8: Reference point for SMS Subscription data retrieval between AMF and UDM.

N20: Reference point for SMS transfer between AMF and SMS Function.

N21: Reference point for SMS Function address registration management and SMS Management Subscription data retrieval between SMS Function and UDM.

4.4.2.3 Service based interface to support SMS over NAS

Nsmsf: Service-based interface exhibited by SMSF.

4.4.3 IMS support

IMS support for 5GC is defined in TS 23.228 [15].

The 5G System architecture supports N5 interface between PCF and P-CSCF and supports Rx interface between PCF and P-CSCF, to enable IMS service. See TS 23.228 [15], TS 23.503 [45] and TS 23.203 [4].

NOTE 1: Rx support between PCF and P-CSCF is for backwards compatibility for early deployments using Diameter between IMS and 5GC functions.

NOTE 2: When service based interfaces are used between the PCF and P-CSCF in the same PLMN, the P-CSCF performs the functions of a trusted AF in the 5GC.

4.4.4 Location services

4.4.4.1 Architecture to support Location Services

Location Service feature is optional and applicable to both regulatory services and commercial services in this Release of the specification. The non-roaming and roaming architecture to support Location Services are defined in clause 4.2 of TS 23.273 [87].

4.4.4.2 Reference point to support Location Services

The reference points to support Location Services are defined in clause 4.4 of TS 23.273 [87].

4.4.4.3 Service Based Interfaces to support Location Services

The Service Based Interfaces to support Location Services are defined in clause 4.5 of TS 23.273 [87].

4.4.5 Application Triggering Services

See TS 23.502 [3] clause 5.2.6.1.

Application trigger message contains information that allows the network to route the message to the appropriate UE and the UE to route the message to the appropriate application. The information destined to the application, excluding the information to route it, is referred to as the Trigger payload. The Trigger payload is implementation specific.

NOTE: The application in the UE may perform actions indicated by the Trigger payload when the Triggered payload is received at the UE. For example initiation of immediate or later communication with the application server based on the information contained in the Trigger payload, which includes the PDU Session Establishment procedure if the related PDU Session is not already established.

4.4.6 5G LAN-type Services

4.4.6.1 User plane architecture to support 5G LAN-type service

The general User Plane architectures described in clause 4.2.3 and clause 4.2.4 apply to 5G LAN-type services, with the additional options described in this clause.

Figure 4.4.6.1-1 depicts the non-roaming user plane architecture to support 5G LAN-type service using local switch.

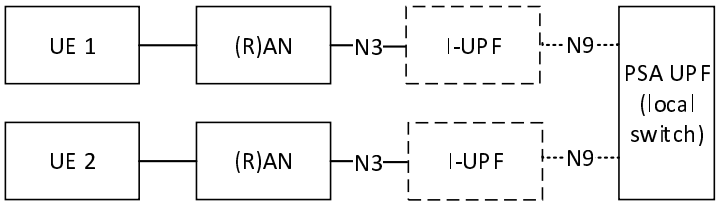


Figure 4.4.6.1-1: Local-switch based user plane architecture in non-roaming scenario

Figure 4.4.6.1-2 depicts the non-roaming user plane architecture to support 5G LAN-type service using N19 tunnel.

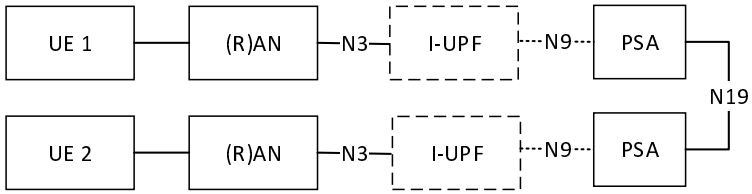


Figure 4.4.6.1-2: N19-based user plane architecture in non-roaming scenario

4.4.6.2 Reference points to support 5G LAN-type service

N19: Reference point between two UPFs for direct routing of traffic between different PDU Sessions without using N6. It has a per 5G VN group granularity.

4.4.7 MSISDN-less MO SMS Service

MSISDN-less MO SMS via T4 is subscription based. The subscription provides the information whether a UE is allowed to originate MSISDN-less MO SMS.

The UE is pre-configured with the Service Centre address that points to SMS-SC that performs this MO SMS delivery via NEF delivery procedure. The recipient of this short message is set to the pre-configured address of the AF (i.e. Address of the destination SME). If UE has multiple GPSIs associated to the same IMSI, the GPSI that is associated with an SMS may be determined from the UE's IMSI and the Application Port ID value in the TP-User-Data field (see TS 23.040 [5]). The NEF may obtain the GPSI by querying the UDM with the IMSI and application port ID.

UE is aware whether the MO SMS delivery status (success or fail) based on the SMS delivery report from SMS-SC. The network does not perform any storing and forwarding functionality for MO SMS.

See TS 23.502 [3] clause 5.2.6 for a description of NEF Services and Service Operations.

4.4.8 Time Sensitive Communication

4.4.8.1 General

The 5G System is extended to support Time sensitive communication as defined in IEEE P802.1Qcc [95].

In this Release of the specification, integration of 5G System with TSN networks that are based on IEEE TSN (IEEE P802.1Qcc [95]) is supported. IEEE TSN is a set of standards to define mechanisms for the time-sensitive (i.e. deterministic) transmission of data over Ethernet networks.

4.4.8.2 Architecture to support Time Sensitive Communication

The 5G System is integrated with the external network as a TSN bridge. This "logical" TSN bridge (see Figure 4.4.8.2-1) includes TSN Translator functionality for interoperation between TSN System and 5G System both for user plane and control plane. 5GS TSN translator functionality consists of Device-side TSN translator (DS-TT) and Network-side TSN translator (NW-TT). 5G System specific procedures in 5GC and RAN, wireless communication links, etc. remain hidden from the TSN network. To achieve such transparency to the TSN network and the 5GS to appear as any other TSN Bridge, the 5GS provides TSN ingress and egress ports via DS-TT and NW-TT. DS-TT and NW-TT optionally support:

- hold and forward functionality for the purpose of de-jittering;
- per-stream filtering and policing as defined in IEEE 802.1Q [98] clause 8.6.5.1.

DS-TT optionally supports link layer connectivity discovery and reporting as defined in IEEE 802.1AB [97] for discovery of Ethernet devices attached to DS-TT. NW-TT supports link layer connectivity discovery and reporting as defined in IEEE 802.1AB [97] for discovery of Ethernet devices attached to NW-TT. If a DS-TT does not support link layer connectivity discovery and reporting, then NW-TT performs link layer connectivity discovery and reporting as defined in IEEE 802.1AB [97] for discovery of Ethernet devices attached to DS-TT on behalf of DS-TT.

NOTE 1: If NW-TT performs link layer connectivity discovery and reporting on behalf of DS-TT, it is assumed that LLDP frames are transmitted between NW-TT and UE on the default QoS Flow. Alternatively, SMF can establish a dedicated QoS Flow matching on the Ethertype defined for LLDP (IEEE 802.1AB [97]).

There are three TSN configuration models defined in IEEE P802.1Qcc [95]. Amongst the three models:

- fully centralized model is supported in this release of the specification;
- fully distributed model is not supported in this release of the specification;
- hybrid model is not supported in this Release of the specification.

NOTE 2: This release only supports interworking with TSN using IEEE 802.1Q [98] clause 8.6.8.4 based scheduled traffic and IEEE 802.1Q [98] clause 8.6.5.1 based per-stream filtering and policy.

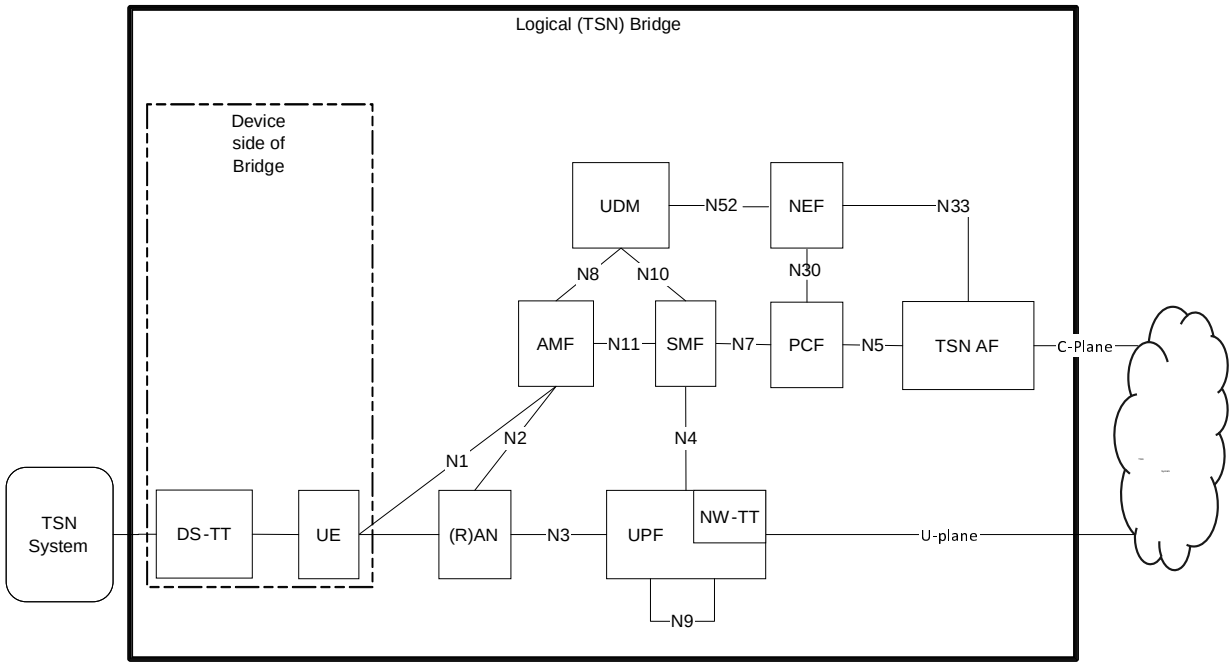


Figure 4.4.8.2-1: System architecture view with 5GS appearing as TSN bridge

NOTE 3: Whether DS-TT and UE are combined or are separate is up to implementation.

5 High level features

5.1 General

Clause 5 specifies the high level functionality and features of the 5G System for both 3GPP and Non-3GPP access and for the interoperability with the EPC defined in TS 23.401 [26].

5.2 Network Access Control

5.2.1 General

Network access is the means for the user to connect to 5G CN. Network access control comprises the following functionality:

- Network selection,
- Identification and authentication,
- Authorisation,
- Access control and barring,
- Policy control,
- Lawful Interception.

5.2.2 Network selection

In order to determine to which PLMN to attempt registration, the UE performs network selection. The network selection procedure comprises two main parts, PLMN selection and access network selection. The requirements for the PLMN

selection are specified in TS 22.011 [25] and the procedures are in TS 23.122 [17]. The access network selection part for the 3GPP access networks is specified in TS 36.300 [30] for E-UTRAN and in TS 38.300 [27] for the NR.

5.2.3 Identification and authentication

The network may authenticate the UE during any procedure establishing a NAS signalling connection with the UE. The security architecture is specified in TS 33.501 [29]. The network may optionally perform an PEI check with 5G-EIR.

5.2.4 Authorisation

The authorisation for connectivity of the subscriber to the 5GC and the authorization for the services that the user is allowed to access based on subscription (e.g. Operator Determined Barring, Roaming restrictions, Access Type and RAT Type currently in use) is evaluated once the user is successfully identified and authenticated. This authorization is executed during UE Registration procedure.

5.2.5 Access control and barring

When the UE needs to transmit an initial NAS message, the UE shall request to establish an RRC Connection first and the NAS shall provide the RRC establishment related information to the lower layer. The RAN handles the RRC Connection with priority during and after RRC Connection Establishment procedure, when UE indicates priority in Establishment related information

Under high network load conditions, the network may protect itself against overload by using the Unified Access Control functionality for 3GPP access specified in TS 22.261 [2], TS 24.501 [47] and TS 38.300 [27] to limit access attempts from UEs. Depending on network configuration, the network may determine whether certain access attempt should be allowed or blocked based on categorized criteria, as specified in TS 22.261 [2] and TS 24.501 [47]. The NG-RAN may broadcast barring control information associated with Access Categories and Access Identities as specified in TS 38.300 [27].

The NG-RAN node may initiate such Unified Access Control when:

- AMFs request to restrict the load for UEs that access the network by sending OVERLOAD START message containing conditions defined in clause 5.19.5.2, or
- requested by OAM, or
- triggered by NG-RAN itself.

If the NG-RAN node takes a decision to initiate UAC because of the reception of the N2 interface OVERLOAD START messages, the NG-RAN should only initiate such procedure if all the AMFs relevant to the request contained in the OVERLOAD START message and connected to this NG-RAN node request to restrict the load for UEs that access the network.

If the UE supports both N1 and S1 modes NAS and, as defined in TS 23.401 [26], the UE is configured for Extended Access Barring (EAB) but is not configured with a permission for overriding Extended Access Barring (EAB), when the UE wants to access the 5GS it shall perform Unified Access Control checks for Access Category 1 on receiving an indication from the upper layers as defined in TS 24.501 [47], TS 38.331 [28], TS 36.331 [51].

If the UE supports both N1 and S1 modes NAS and, as defined in TS 23.401 [26], the UE is configured with a permission for overriding Extended Access Barring (EAB), when the UE wants to access the 5GS it shall ignore Unified Access Control checks for Access Category 1 on receiving an indication from the upper layers, as defined in TS 24.501 [47].

NOTE: UE signalling of Low Access Priority indication over N1 in 5GS is not supported in this release of the specification.

Operator may provide one or more PLMN-specific Operator-defined access category definitions to the UE using NAS signalling, and the UE handles the Operator-defined access category definitions stored for the Registered PLMN, as specified in TS 24.501 [47].

5.2.6 Policy control

Network access control including service authorization may be influenced by Policy control, as specified in clause 5.14.

5.2.7 Lawful Interception

For definition and functionality of Lawful Interception, please see TS 33.126 [35].

5.3 Registration and Connection Management

5.3.1 General

The Registration Management is used to register or deregister a UE/user with the network, and establish the user context in the network. The Connection Management is used to establish and release the signalling connection between the UE and the AMF.

5.3.2 Registration Management

5.3.2.1 General

A UE/user needs to register with the network to receive services that requires registration. Once registered and if applicable the UE updates its registration with the network (see TS 23.502 [3]):

- periodically, in order to remain reachable (Periodic Registration Update); or
- upon mobility (Mobility Registration Update); or
- to update its capabilities or re-negotiate protocol parameters (Mobility Registration Update).

The Initial Registration procedure involves execution of Network Access Control functions as defined in clause 5.2 (i.e. user authentication and access authorization based on subscription profiles in UDM). As result of the Registration procedure, the identifier of the serving AMF serving the UE in the access through which the UE has registered will be registered in UDM.

The registration management procedures are applicable over both 3GPP access and Non-3GPP access. The 3GPP and Non-3GPP RM states are independent of each other, see clause 5.3.2.4.

5.3.2.2 5GS Registration Management states

5.3.2.2.1 General

Two RM states are used in the UE and the AMF that reflect the registration status of the UE in the selected PLMN:

- RM-DEREGISTERED.
- RM-REGISTERED.

5.3.2.2.2 RM-DEREGISTERED state

In the RM-DEREGISTERED state, the UE is not registered with the network. The UE context in AMF holds no valid location or routing information for the UE so the UE is not reachable by the AMF. However, some parts of UE context may still be stored in the UE and the AMF e.g. to avoid running an authentication procedure during every Registration procedure.

In the RM-DEREGISTERED state, the UE shall:

- attempt to register with the selected PLMN using the Initial Registration procedure if it needs to receive service that requires registration (see TS 23.502 [3] clause 4.2.2.2).

- remain in RM-DEREGISTERED state if receiving a Registration Reject upon Initial Registration (see TS 23.502 [3] clause 4.2.2.2).

- enter RM-REGISTERED state upon receiving a Registration Accept (see TS 23.502 [3] clause 4.2.2.2).

When the UE RM state in the AMF is RM-DEREGISTERED, the AMF shall:

- when applicable, accept the Initial Registration of a UE by sending a Registration Accept to this UE and enter RM-REGISTERED state for the UE (see TS 23.502 [3] clause 4.2.2.2); or

- when applicable, reject the Initial Registration of a UE by sending a Registration Reject to this UE (see TS 23.502 [3] clause 4.2.2.2).

5.3.2.2.3 RM-REGISTERED state

In the RM-REGISTERED state, the UE is registered with the network. In the RM-REGISTERED state, the UE can receive services that require registration with the network.

In the RM-REGISTERED state, the UE shall:

- perform Mobility Registration Update procedure if the current TAI of the serving cell (see TS 37.340 [31]) is not in the list of TAIs that the UE has received from the network in order to maintain the registration and enable the AMF to page the UE;

- perform Periodic Registration Update procedure triggered by expiration of the periodic update timer to notify the network that the UE is still active.

- perform a Mobility Registration Update procedure to update its capability information or to re-negotiate protocol parameters with the network;

- perform Deregistration procedure (see TS 23.502 [3] clause 4.2.2.3.1), and enter RM-DEREGISTERED state, when the UE needs to be no longer registered with the PLMN. The UE may decide to deregister from the network at any time.

- enter RM-DEREGISTERED state when receiving a Registration Reject message or a Deregistration message. The actions of the UE depend upon the 'cause value' in the Registration Reject or Deregistration message. See TS 23.502 [3] clause 4.2.2.

When the UE RM state in the AMF is RM-REGISTERED, the AMF shall:

- perform Deregistration procedure (see TS 23.502 [3] clauses 4.2.2.3.2, 4.2.2.3.3), and enter RM-DEREGISTERED state for the UE, when the UE needs to be no longer registered with the PLMN. The network may decide to deregister the UE at any time;

- perform Implicit Deregistration at any time after the Implicit Deregistration timer expires. The AMF shall enter RM-DEREGISTERED state for the UE after Implicit Deregistration;

- when applicable, accept or reject Registration Requests or Service Requests from the UE.

5.3.2.2.4 5GS Registration Management State models

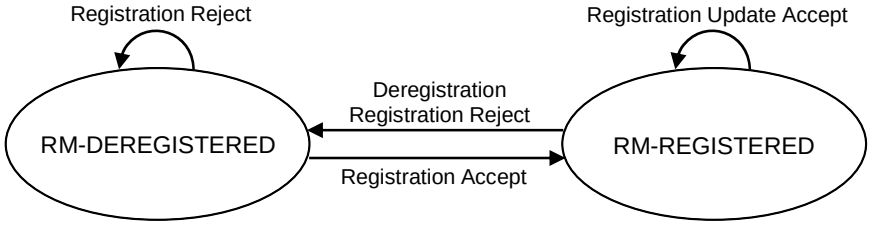


Figure 5.3.2.2.4-1: RM state model in UE

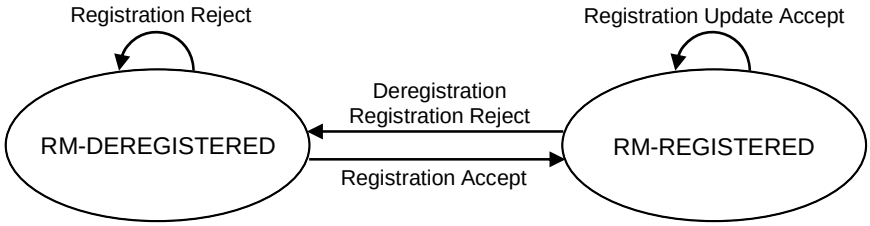


Figure 5.3.2.2.4-2: RM state model in AMF

5.3.2.3 Registration Area management

Registration Area management comprises the functions to allocate and reallocate a Registration area to a UE. Registration area is managed per access type i.e., 3GPP access or Non-3GPP access.

When a UE registers with the network over the 3GPP access, the AMF allocates a set of tracking areas in TAI List to the UE. When the AMF allocates registration area, i.e. the set of tracking areas in TAI List, to the UE it may take into account various information (e.g. Mobility Pattern and Allowed/Non-Allowed Area (refer to clause 5.3.4.1)). An AMF which has the whole PLMN as serving area may alternatively allocate the whole PLMN ("all PLMN") as registration area to a UE in MICO mode (refer to clause 5.4.1.3).

The 5G System shall support allocating a Registration Area using a single TAI List which includes tracking areas of any NG-RAN nodes in the Registration Area for a UE.

A single TAI dedicated to Non-3GPP access, the N3GPP TAI, is defined in a PLMN and applies within the PLMN.

When a UE registers with the network over the Non-3GPP access, the AMF allocates a registration area that only includes the N3GPP TAI to the UE.

When generating the TAI list, the AMF shall include only TAIs that are applicable on the access type (i.e. 3GPP access or Non-3GPP access) where the TAI list is sent.

NOTE 1: To prevent extra signalling load resulting from Mobility Registration Update occurring at every RAT change, it is preferable to avoid generating a RAT-specific TAI list for a UE supporting more than one RAT.

For all 3GPP Access RATs in NG-RAN and for Non-3GPP Access, the 5G System supports the TAI format as specified in TS 23.003 [19] consisting of MCC, MNC and a 3-byte TAC only.

The additional aspects for registration management when a UE is registered over one access type while the UE is already registered over the other access type is further described in clause 5.3.2.4.

To ensure a UE initiates a Mobility Registration procedure when performing inter-RAT mobility to or from NB-IoT, a Tracking Area shall not contain both NB-IoT and other RATs cells (e.g. WB-E-UTRA, NR), and the AMF shall not allocate a TAI list that contains both NB-IoT and other RATs Tracking Areas.

For 3GPP access the AMF determines the RAT type the UE is camping on based on the Global RAN Node IDs associated with the N2 interface and additionally the Tracking Area indicated by NG-RAN. When the UE is accessing NR using unlicensed bands, as defined in clause 5.4.8, an indication is provided in N2 interface as defined in TS 38.413 [34].

The AMF may also determine more precise RAT Type information based on further information received from NG-RAN:

- The AMF may determine the RAT Type to be LTE-M as defined in clause 5.31.20; or
- The AMF may determine the RAT Type to be NR using unlicensed bands, as defined in clause 5.4.8.

For Non-3GPP accesses the AMF determines the RAT type the UE is camping based on the 5G-AN node associated with N2 interface as follows:

- The RAT type is Untrusted Non-3GPP if the 5G-AN node has a Global N3IWF Node ID;

- The RAT type is Trusted Non-3GPP if the 5G-AN node has a Global TNGF Node ID or a Global TWIF Node ID; and

- The RAT type is Wireline -BBF if the 5G-AN node has a Global W-AGF Node ID corresponding to a W-AGF supporting the Wireline BBF Access Network. The RAT type is Wireline-Cable if the 5G-AN node has a Global W-AGF Node ID corresponding to a W-AGF supporting the Wireline Cable Access Network. If not possible to distinguish between the two, the RAT type is Wireline.

NOTE 2: How to differentiate between W-AGF supporting either Wireline BBF Access Network or the Wireline (e.g. different Global W-AGF Node ID IE or the Global W-AGF Node ID including a field to distinguish between them) is left to Stage 3 definition.

NOTE 3: If an operator supports only one kind of Wireline Access Network (either Wireline BBF Access Network or a Wireline Cable Access Network) the AMF may be configured to use RAT type Wireline or the specific one.

For Non-3GPP access the AMF may also use the User Location Information provided at N2 connection setup to determine a more precise RAT Type, e.g. identifying IEEE 802.11 access, Wireline-Cable access, Wireline-BBF access.

When the 5G-AN node has either a Global N3IWF Node ID, or a Global TNGF Node ID, or a Global TWIF Node ID, or a Global W-AGF Node ID, the Access Type is Non-3GPP Access.

5.3.2.4 Support of a UE registered over both 3GPP and Non-3GPP access

This clause applies to Non-3GPP access network corresponding to the Untrusted Non-3GPP access network, to the Trusted Non-3GPP and to the W-5GAN. In the case of W-5GAN the UE mentioned in this clause corresponds to the 5G-RG.

For a given serving PLMN there is one RM context for a UE for each access, e.g. when the UE is consecutively or simultaneously served by a 3GPP access and by a non-3GPP access (i.e. via an N3IWF, TNGF and W-AGF) of the same PLMN. UDM manages separate/independent UE Registration procedures for each access.

When served by the same PLMN for 3GPP and non-3GPP accesses, an UE is served by the same AMF except in the temporary situation described in clause 5.17 i.e. after a mobility from EPS while the UE has PDU Sessions associated with non-3GPP access.

An AMF associates multiple access-specific RM contexts for an UE with:

- a 5G-GUTI that is common to both 3GPP and Non-3GPP accesses. This 5G-GUTI is globally unique.

- a Registration state per access type (3GPP / Non-3GPP)

- a Registration Area per access type: one Registration Area for 3GPP access and another Registration Area for non 3GPP access. Registration Areas for the 3GPP access and the Non-3GPP access are independent.

- timers for 3GPP access:

  - a Periodic Registration timer; and

  - a Mobile Reachable timer and an Implicit Deregistration timer.

- timers for non-3GPP access:

  - a UE Non-3GPP Deregistration timer; and

  - a Network Non-3GPP Implicit Deregistration timer.

The AMF shall not provide a Periodic Registration Timer for the UE over a Non-3GPP access. Consequently, the UE need not perform Periodic Registration Update procedure over Non-3GPP access. Instead, during the Initial Registration procedure and Re-registration, the UE is provided by the network with a UE Non-3GPP Deregistration timer that starts when the UE enters non-3GPP CM-IDLE state.

When the 3GPP access and the non-3GPP access for the same UE are served by the same PLMN, the AMF assigns the same 5G-GUTI for use over both accesses. Such a 5G-GUTI may be assigned or re-assigned over any of the 3GPP and Non-3GPP accesses. The 5G-GUTI is assigned upon a successful registration of the UE, and is valid over both 3GPP

and Non-3GPP access to the same PLMN for the UE. Upon performing an initial access over the Non-3GPP access or over the 3GPP access while the UE is already registered with the 5G System over another access of the same PLMN, the UE provides the native 5G-GUTI for the other access. This enables the AN to select an AMF that maintains the UE context created at the previous Registration procedure via the GUAMI derived from the 5G-GUTI, and enables the AMF to correlate the UE request to the existing UE context via the 5G-GUTI.

If the UE is performing registration over one access and intends to perform registration over the other access in the same PLMN (e.g. the 3GPP access and the selected N3IWF, TNGF or W-AGF are located in the same PLMN), the UE shall not initiate the registration over the other access until the Registration procedure over first access is completed.

NOTE: To which access the UE performs registration first is up to UE implementation.

When the UE is successfully registered to an access (3GPP access or Non-3GPP access respectively) and the UE registers via the other access:

- if the second access is located in the same PLMN (e.g. the UE is registered via a 3GPP access and selects a N3IWF, TNGF or W-AGF located in the same PLMN), the UE shall use for the registration to the PLMN associated with the new access the 5G-GUTI that the UE has been provided with at the previous registration or UE configuration update procedure for the first access in the same PLMN. Upon successful completion of the registration to the second access, if the network included a 5G-GUTI in the Registration Accept, the UE shall use the 5G-GUTI received in the Registration Accept for both registrations. If no 5G-GUTI is included in the Registration Accept, then the UE uses the 5G-GUTI assigned for the existing registration also for the new registration.

- if the second access is located in a PLMN different from the registered PLMN of the first access (i.e. not the registered PLMN), (e.g. the UE is registered to a 3GPP access and selects a N3IWF, TNGF or W-AGF located in a PLMN different from the PLMN of the 3GPP access, or the UE is registered over Non-3GPP and registers to a 3GPP access in a PLMN different from the PLMN of the N3IWF, TNGF or W-AGF), the UE shall use for the registration to the PLMN associated with the new access a 5G-GUTI only if it has got one previously received from a PLMN that is not the same as the PLMN the UE is already registered with. If the UE does not include a 5G-GUTI, the SUCI shall be used for the new registration. Upon successful completion of the registration to the second access, the UE has the two 5G-GUTIs (one per PLMN).

A UE supporting registration over both 3GPP and Non-3GPP access to two PLMNs shall be able to handle two separate registrations, including two 5G-GUTIs, one per PLMN, and two associated equivalent PLMN lists.

When a UE 5G-GUTI assigned during a Registration procedure over 3GPP (e.g. the UE registers first over a 3GPP access) is location-dependent, the same UE 5G-GUTI can be re-used over the Non-3GPP access when the selected N3IWF, TNGF or W-AGF function is in the same PLMN as the 3GPP access. When an UE 5G-GUTI is assigned during a Registration procedure performed over a Non 3GPP access (e.g. the UE registers first over a non-3GPP access), the UE 5G-GUTI may not be location-dependent, so that the UE 5G-GUTI may not be valid for NAS procedures over the 3GPP access and, in this case, a new AMF is allocated during the Registration procedure over the 3GPP access.

When the UE is registered first via 3GPP access, if the UE registers to the same PLMN via Non-3GPP access, the UE shall send the GUAMI obtained via 3GPP access to the N3IWF, TNGF or W-AGF, which uses the received GUAMI to select the same AMF as the 3GPP access.

The Deregistration Request message indicates whether it applies to the 3GPP access the Non-3GPP access, or both.

If the UE is registered on both 3GPP and Non-3GPP accesses and it is in CM-IDLE over Non-3GPP access, then the UE or AMF may initiate a Deregistration procedure over the 3GPP access to deregister the UE only on the Non-3GPP access, in which case all the PDU Sessions which are associated with the Non-3GPP access shall be released.

If the UE is registered on both 3GPP and non-3GPP accesses and it is in CM-IDLE over 3GPP access and in CM-CONNECTED over non-3GPP access, then the UE may initiate a Deregistration procedure over the non-3GPP access to deregister the UE only on the 3GPP access, in which case all the PDU Sessions which are associated with the 3GPP access shall be released.

Registration Management over Non-3GPP access is further defined in clause 5.5.1.

5.3.3 Connection Management

5.3.3.1 General

Connection management comprises the functions of establishing and releasing a NAS signalling connection between a UE and the AMF over N1. This NAS signalling connection is used to enable NAS signalling exchange between the UE and the core network. It comprises both the AN signalling connection between the UE and the AN (RRC Connection over 3GPP access or UE-N3IWF connection over untrusted N3GPP access or UE-TNGF connection over trusted N3GPP access) and the N2 connection for this UE between the AN and the AMF.

5.3.3.2 5GS Connection Management states

5.3.3.2.1 General

Two CM states are used to reflect the NAS signalling Connection of the UE with the AMF:

- CM-IDLE
- CM-CONNECTED

The CM state for 3GPP access and Non-3GPP access are independent of each other, i.e. one can be in CM-IDLE state at the same time when the other is in CM-CONNECTED state.

5.3.3.2.2 CM-IDLE state

A UE in CM-IDLE state has no NAS signalling connection established with the AMF over N1. The UE performs cell selection/cell reselection according to TS 38.304 [50] and PLMN selection according to TS 23.122 [17].

There are no AN signalling connection, N2 connection and N3 connections for the UE in the CM-IDLE state.

If the UE is both in CM-IDLE state and in RM-REGISTERED state, the UE shall, unless otherwise specified in clause 5.3.4.1:

- Respond to paging by performing a Service Request procedure (see TS 23.502 [3] clause 4.2.3.2), unless the UE is in MICO mode (see clause 5.4.1.3);
- perform a Service Request procedure when the UE has uplink signalling or user data to be sent (see TS 23.502 [3] clause 4.2.3.2). Specific conditions apply for LADN, see clause 5.6.5.

When the UE state in the AMF is RM-REGISTERED, UE information required for initiating communication with the UE shall be stored. The AMF shall be able to retrieve stored information required for initiating communication with the UE using the 5G-GUTI.

NOTE: In 5GS there is no need for paging using the SUPI/SUCI of the UE.

The UE provides 5G-S-TMSI as part of AN parameters during AN signalling connection establishment as specified in TS 38.331 [28] and TS 36.331 [51]. The UE shall enter CM-CONNECTED state whenever an AN signalling connection is established between the UE and the AN (entering RRC Connected state over 3GPP access, or at the establishment of the UE-N3IWF connectivity over untrusted non-3GPP access or the UE-TNGF connectivity over trusted non-3GPP access). The transmission of an Initial NAS message (Registration Request, Service Request or Deregistration Request) initiates the transition from CM-IDLE to CM-CONNECTED state.

When the UE states in the AMF are CM-IDLE and RM-REGISTERED, the AMF shall:

- perform a network triggered Service Request procedure when it has signalling or mobile-terminated data to be sent to this UE, by sending a Paging Request to this UE (see TS 23.502 [3] clause 4.2.3.3), if a UE is not prevented from responding e.g. due to MICO mode or Mobility Restrictions.

The AMF shall enter CM-CONNECTED state for the UE whenever an N2 connection is established for this UE between the AN and the AMF. The reception of initial N2 message (e.g., N2 INITIAL UE MESSAGE) initiates the transition of AMF from CM-IDLE to CM-CONNECTED state.

The UE and the AMF may optimize the power efficiency and signalling efficiency of the UE when in CM-IDLE state e.g. by activating MICO mode (see clause 5.4.1.3).

5.3.3.2.3 CM-CONNECTED state

A UE in CM-CONNECTED state has a NAS signalling connection with the AMF over N1. A NAS signalling connection uses an RRC Connection between the UE and the NG-RAN and an NGAP UE association between the AN and the AMF for 3GPP access. A UE can be in CM-CONNECTED state with an NGAP UE association that is not bound to any TNLA between the AN and the AMF. See clause 5.21.1.2 for details on the state of NGAP UE association for an UE in CM-CONNECTED state. Upon completion of a NAS signalling procedure, the AMF may decide to release the NAS signalling connection with the UE.

In the CM-CONNECTED state, the UE shall:

- enter CM-IDLE state whenever the AN signalling connection is released (entering RRC Idle state over 3GPP access or when the release of the UE-N3IWF connectivity over untrusted non-3GPP access or the UE-TNGF connectivity over trusted non-3GPP access is detected by the UE), see TS 38.331 [28] for 3GPP access.

When the UE CM state in the AMF is CM-CONNECTED, the AMF shall:

- enter CM-IDLE state for the UE whenever the logical NGAP signalling connection and the N3 user plane connection for this UE are released upon completion of the AN Release procedure as specified in TS 23.502 [3].

The AMF may keep a UE CM state in the AMF in CM-CONNECTED state until the UE de-registers from the core network.

A UE in CM-CONNECTED state can be in RRC Inactive state, see TS 38.300 [27]. When the UE is in RRC Inactive state the following applies:

- UE reachability is managed by the RAN, with assistance information from core network;
- UE paging is managed by the RAN.
- UE monitors for paging with UE's CN (5G S-TMSI) and RAN identifier.

5.3.3.2.4 5GS Connection Management State models

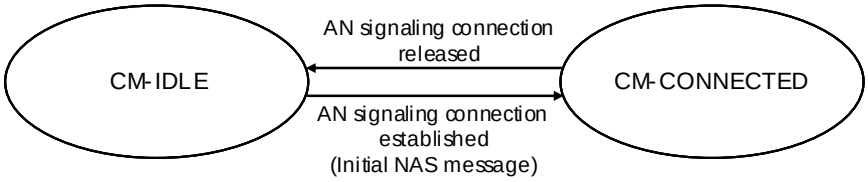


Figure 5.3.3.2.4-1: CM state transition in UE

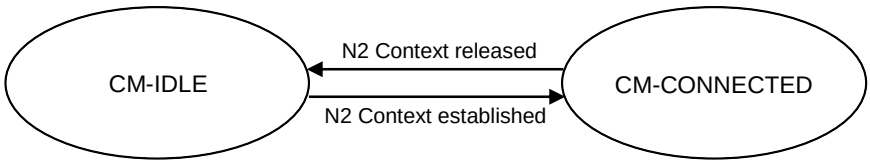


Figure 5.3.3.2.4-2: CM state transition in AMF

When a UE enters CM-IDLE state, the UP connection of the PDU Sessions that were active on this access are deactivated.

NOTE: The activation of UP connection of PDU Sessions is documented in clause 5.6.8.

5.3.3.2.5 CM-CONNECTED with RRC Inactive state

RRC Inactive state applies to NG-RAN. UE support for RRC Inactive state is defined in TS 38.306 [69] for NR and TS 36.306 [70] for E-UTRA connected to 5GC. RRC Inactive is not supported by NB-IoT connected to 5GC.

The AMF shall provide assistance information to the NG-RAN, to assist the NG-RAN's decision whether the UE can be sent to RRC Inactive state except due to some exceptional cases such as:

- PLMN (or AMF set) does not support RRC Inactive;
- The UE needs to be kept in CM-CONNECTED State (e.g. for tracking).

The "RRC Inactive Assistance Information" includes:

- UE specific DRX values;
- UE specific extended idle mode DRX values (cycle length and Paging Time Window length);
- The Registration Area provided to the UE;
- Periodic Registration Update timer;
- If the AMF has enabled MICO mode for the UE, an indication that the UE is in MICO mode;
- Information from the UE identifier, as defined in TS 38.304 [50] for NR and TS 36.304 [52] for E-UTRA connected to 5GC, that allows the RAN to calculate the UE's RAN paging occasions.

The RRC Inactive Assistance Information mentioned above is provided by the AMF during N2 activation with the (new) serving NG-RAN node (i.e. during Registration, Service Request, Handover) to assist the NG RAN's decision whether the UE can be sent to RRC Inactive state. If the AMF allocates a new Registration Area to the UE, the AMF should update the NG-RAN with the new Registration Area by sending the RRC Inactive Assistance Information accordingly.

RRC Inactive state is part of RRC state machine, and it is up to the RAN to determine the conditions to enter RRC Inactive state. If any of the parameters included in the RRC Inactive Assistance Information changes as the result of NAS procedure, the AMF shall update the RRC Inactive Assistance Information to the NG-RAN node.

When the UE is in CM-CONNECTED state, if the AMF has provided RRC Inactive assistance information, the RAN node may decide to move a UE to CM-CONNECTED with RRC Inactive state.

The state and "endpoints" (in the case of Dual Connectivity configuration) of the N2 and N3 reference points are not changed by the UE entering CM-CONNECTED with RRC Inactive state. A UE in RRC inactive state is aware of the RAN Notification area and periodic RAN Notification Area Update timer.

The 5GC network is not aware of the UE transitions between CM-CONNECTED with RRC Connected and CM-CONNECTED with RRC Inactive state, unless the 5GC network is notified via N2 notification procedure in TS 23.502 [3] clause 4.8.3.

At transition into CM-CONNECTED with RRC Inactive state, the NG-RAN configures the UE with a periodic RAN Notification Area Update timer taking into account the value of the Periodic Registration Update timer value indicated in the RRC Inactive Assistance Information, and uses a guard timer with a value longer than the RAN Notification Area Update timer value provided to the UE.

If the periodic RAN Notification Area Update guard timer expires in NG-RAN, the NG-RAN shall initiate AN Release procedure as specified in TS 23.502 [3], clause 4.2.6.

When the UE is in CM-CONNECTED with RRC Inactive state, the UE performs PLMN selection procedures as defined in TS 23.122 [17] and TS 24.501 [47].

When the UE is CM-CONNECTED with RRC Inactive state, the UE may resume the RRC Connection due to:

- Uplink data pending;
- Mobile initiated NAS signalling procedure;
- As a response to RAN paging;

- Notifying the network that it has left the RAN Notification Area;
- Upon periodic RAN Notification Area Update timer expiration.

If the UE resumes the connection in a different NG-RAN node within the same PLMN or equivalent PLMN, the UE AS context is retrieved from the old NG-RAN node and a procedure is triggered towards the CN (see TS 23.502 [3], clause 4.8.2).

NOTE 1: With Dual Connectivity configuration if the UE resumes the RRC connection in the Master RAN node, the Secondary RAN node configuration is defined in TS 38.300 [27].

If the RAN paging procedure, as defined in TS 38.300 [27], is not successful in establishing contact with the UE the procedure shall be handled by the network as follows:

- If NG-RAN has at least one pending NAS PDU for transmission, the RAN node shall initiate the AN Release procedure (see TS 23.502 [3], clause 4.2.6,) to move the UE CM state in the AMF to CM-IDLE state and indicate to the AMF the NAS non-delivery.
- If NG RAN has only pending user plane data for transmission, the NG-RAN node may keep the N2 connection active or initiate the AN Release procedure (see TS 23.502 [3], clause 4.2.6) based on local configuration in NG-RAN.

NOTE 2: The user plane data which triggers the RAN paging can be lost, e.g. in the case of RAN paging failure.

If a UE in CM-CONNECTED with RRC Inactive state performs cell selection to GERAN/UTRAN/E-UTRAN, it shall follow idle mode procedures of the selected RAT as specified in clause 5.17.

In addition, a UE in CM-CONNECTED state with RRC Inactive state shall enter CM-IDLE state and initiates the NAS signalling recovery (see TS 24.501 [47]) in the following cases:

- If RRC resume procedure fails,

  If the UE receives Core Network paging,
- If the periodic RAN Notification Area Update timer expires and the UE cannot successfully resume the RRC Connection,
- In any other failure scenario that cannot be resolved in RRC Inactive state and requires the UE to move to CM-IDLE state.

When a UE is in CM-CONNECTED with RRC Inactive state, and a trigger to change the UE's NG-RAN UE Radio Capability information happens, the UE shall move to CM-IDLE state and initiate the procedure for updating UE Radio Capability defined in clause 5.4.4.1.

When UE is in CM-CONNECTED with RRC Inactive state, if RAN has received Location Reporting Control message from AMF with the Reporting Type indicating single stand-alone report, the RAN shall perform RAN paging before reporting the location to AMF.

When UE is in CM-CONNECTED with RRC Inactive state, if RAN has received Location Reporting Control message from AMF with the Reporting Type indicating continuously reporting whenever the UE changes cell, the RAN shall send a Location Report message to AMF including UE's last known location with time stamp.

When the UE is CM-CONNECTED with RRC Inactive state. If the AMF receives Nudm_UEContextManagement_DeregistrationNotification from UDM, the AMF shall initiate AN Release procedure as specified in TS 23.502 [3], clause 4.2.6.

When UE is in CM-CONNECTED with RRC Inactive state, if RAN has received Location Reporting Control message from AMF with the Reporting Type of the Area Of Interest based reporting, the RAN shall send a Location Report message to AMF including UE presence in the Area Of Interest (i.e., IN, OUT, or UNKNOWN) and the UE's last known location with time stamp.

When the UE is in CM-CONNECTED with RRC Inactive state, if the old NG-RAN node that sents the UE into RRC Inactive state receives the downlink N2 signalling, it initiates the RAN paging as defined in TS 38.300 [27]. If the UE resumes the RRC Connection towards a different NG-RAN node, the old NG-RAN node includes the "UE Context Transfer" indication into a response container to the NF (e.g. AMF or SMF) that generates such N2 downlink

signalling. Then the NF shall reattempt the same procedure when the path switch from the old NG-RAN node to the new NG-RAN node is complete.

5.3.3.3 NAS signalling connection management

5.3.3.3.1 General

NAS signalling connection management includes the functions of establishing and releasing a NAS signalling connection.

5.3.3.3.2 NAS signalling connection establishment

NAS signalling connection establishment function is provided by the UE and the AMF to establish a NAS signalling connection for a UE in CM-IDLE state. The AMF shall provide the list of recommended cells/ TAs / NG-RAN node identifiers for paging, if the NG-RAN had provided that information in an earlier AN Release Procedure in the AN (see clause 4.2.6 of TS 23.502 [3]).

When the UE in CM-IDLE state needs to transmit an NAS message, the UE shall initiate a Service Request, a Registration or a Deregistration procedure to establish a NAS signalling connection to the AMF as specified in TS 23.502 [3], clauses 4.2.2 and 4.2.3. If the NAS signalling connection is to be established via an NG-RAN node, but the AMF detects that this UE has already established a NAS signalling connection via old NG-RAN node, the AMF shall release the old established NAS signalling connection by triggering AN Release Procedure.

Based on UE preferences, UE subscription, Mobility Pattern and network configuration, the AMF may keep the NAS signalling connection until the UE de-registers from the network.

5.3.3.3.3 NAS signalling connection Release

The procedure of releasing a NAS signalling connection is initiated by the AN node (either 5G (R)AN node or N3IWF) or the AMF. The NG-RAN node may include the list of recommended cells/ TAs / NG-RAN node identifiers for paging, during the AN Release Procedure in the AN (see clause 4.2.6 of TS 23.502 [3]). The AMF stores this information, if provided by the NG-RAN.

The UE considers the NAS signalling connection is released if it detects the AN signalling connection is released. The AMF considers the NAS signalling connection is released if it detects the N2 context is released.

5.3.3.4 Support of a UE connected over both 3GPP and Non-3GPP access

The AMF manages two CM states for an UE: a CM state for 3GPP access and a CM state for Non-3GPP access. An N2 interface can serve the UE for either 3GPP access or for Non 3GPP access. UE connected over both 3GPP and Non-3GPP has got two N2 interfaces, one for each access. A UE may be in any combination of the CM states between 3GPP and Non-3GPP access, e.g. a UE may be CM-IDLE for one access and CM-CONNECTED for the other access, CM-IDLE for both accesses or CM-CONNECTED for both accesses.

When the UE CM state in the AMF is CM-IDLE for 3GPP access and CM-CONNECTED for Non-3GPP access, the AMF shall perform a network triggered Service Request procedure, when it has downlink data to be sent to this UE for 3GPP access, by sending either the Paging Request via 3GPP access or the NAS notification via Non-3GPP access to this UE (see TS 23.502 [3] clause 4.2.3.3).

Connection Management over Non-3GPP access is further defined in clause 5.5.2.

5.3.4 UE Mobility

5.3.4.1 Mobility Restrictions

5.3.4.1.1 General

Mobility Restrictions restrict mobility handling or service access of a UE. The Mobility Restriction functionality is provided by the UE (only for mobility restriction categories provided to the UE), the radio access network and the core network.

Unless otherwise stated, Mobility Restrictions only apply to 3GPP access and wireline access, they do not apply to other non-3GPP accesses.

The UE and the network shall override any Forbidden Area, Non-Allowed area restrictions and Core Network type restriction whenever accessing the network for regulatory prioritized services like Emergency services and MPS.

Service Area restrictions and handling of Forbidden Areas for CM-IDLE state and, for CM-CONNECTED state when in RRC Inactive state are executed by the UE based on information received from the core network. Mobility Restrictions for CM-CONNECTED state when in RRC-Connected state are executed by the radio access network and the core network.

In CM-CONNECTED state, the core network provides Mobility Restrictions to the radio access network within Mobility Restriction List.

Mobility Restrictions consists of RAT restriction, Forbidden Area, Service Area Restrictions, Core Network type restriction and Closed Access Group information as follows:

- RAT restriction:

  Defines the 3GPP Radio Access Technology(ies), a UE is not allowed to access in a PLMN. In a restricted RAT a UE based on subscription is not permitted access to the network for this PLMN. For CM-CONNECTED state, when radio access network determines target RAT and target PLMN during Handover procedure, it should take per PLMN RAT restriction into consideration. The RAT restriction is enforced in the network, and not provided to the UE.

- Forbidden Area:

  In a Forbidden Area, the UE, based on subscription, is not permitted to initiate any communication with the network for this PLMN. The UE behaviour in terms of cell selection, RAT selection and PLMN selection depends on the network response that informs the UE of Forbidden Area. A Forbidden Area applies either to 3GPP access or to non-3GPP access.

  Further description on Forbidden Area when using wireline access is available in TS 23.316 [84].

NOTE 1: If the N3GPP TAI (see clause 5.3.2.3) is forbidden in a PLMN, non-3GPP Access is forbidden altogether in this PLMN.

NOTE 2: The UE reactions to specific network responses are described in TS 24.501 [47].

- Service Area Restriction:

  Defines areas in which the UE may or may not initiate communication with the network as follows:

  - Allowed Area:

    In an Allowed Area, the UE is permitted to initiate communication with the network as allowed by the subscription.

  - Non-Allowed Area:

    In a Non-Allowed Area a UE is service area restricted based on subscription. The UE and the network are not allowed to initiate Service Request, or any connection requests for user plane data, control plane data, or SM signalling (except for PS Data Off status change reporting) to obtain user services that are not related to mobility (both in CM-IDLE and in CM-CONNECTED states).

    The UE shall not use the entering of a Non-Allowed Area as a criterion for Cell Reselection, a trigger for PLMN Selection or Domain selection for UE originating sessions or calls. The RRC procedures while the UE is in CM-CONNECTED with RRC Inactive state are unchanged compared to when the UE is in an Allowed Area. The RM procedures are unchanged compared to when the UE is in an Allowed Area. The UE in a Non-Allowed Area shall respond to core network paging or NAS Notification message from non-3GPP access with Service Request and RAN paging. The UE in a Non-Allowed Area may initiate MA PDU Session establishment or activation over a non-3GPP access other than wireline access, but the User Plane resources on the 3GPP access for the MA-PDU shall not be established or activated. The handling of Non-Allowed Area when using wireline access is described in TS 23.316 [84].

NOTE 3: When the services are restricted in 5GS due to Service Area Restriction, then it is assumed that the services will be also restricted in all RATs/Systems at the same location(s) using appropriate mechanisms available in the other RATs/Systems.

NOTE 4: Delivery of SOR transparent container, UE policy container, UE parameters update transparent container as defined in TS 24.501 [47], is part of the mobility related service and is allowed in an area with service restriction.

NOTE 5: For a UE in CM-CONNECTED state then neither control plane data transmission nor, if user plane resources are already established, user plane data transmission are restricted by a non-allowed area.

- Core Network type restriction:

  Defines whether UE is allowed to connect to 5GC only, EPC only, both 5GC and EPC for this PLMN. The Core Network type restriction when received applies in the PLMN either to both 3GPP and non-3GPP Access Types or to non-3GPP Access Type only.

NOTE 6: The Core Network type restriction can be used e.g. in network deployments where the E-UTRAN connects to both EPC and 5GC as described in clause 5.17.

- Closed Access Group information:

  As defined in clause 5.30.3.

For a given UE, the core network determines the Mobility Restrictions based on UE subscription information, UE location and/or local policy (e.g. if the HPLMN has not deployed 5GC, HPLMN ID of the UE and the operator's policy are used in the VPLMN for determining the Core Network type restriction). The Mobility Restriction may change due to e.g. UE's subscription, location change and local policy. Optionally the Service Area Restrictions or the Non-Allowed Area may in addition be fine-tuned by the PCF e.g. based on UE location, PEI and network policies. Service Area Restrictions may be updated during a Registration procedure or UE Configuration Update procedure.

NOTE 7: The subscription management ensure that for MPS service subscriber the Mobility Restrictions is not included.

If the network sends Service Area Restrictions to the UE, the network sends only either an Allowed Area, or a Non-Allowed Area, but not both at the same time, to the UE. If the UE has received an Allowed Area from the network, any TA not part of the Allowed Area is considered by the UE as non-allowed. If the UE has received a Non-Allowed Area from the network, any TA not part of the Non-Allowed Area is considered by the UE as allowed. If the UE has not received any Service Area Restrictions, any TA in the PLMN is considered as allowed.

If the UE has overlapping areas between Forbidden Areas, Service Area Restrictions, or any combination of them, the UE shall proceed in the following precedence order:

- The evaluation of Forbidden Areas shall take precedence over the evaluation of Service Area Restrictions.

The UDM shall provide to the AMF the information defined in TS 23.008 [119] about the subscriber's NR or E-UTRA access restriction set by the operator determined e.g. by subscription scenario and roaming scenario:

- For NR:
  - NR not allowed as primary access.
  - NR not allowed as secondary access.
  - NR in unlicensed bands not allowed as primary access.
  - NR in unlicensed bands not allowed as secondary access.
- For E-UTRA:
  - E-UTRA not allowed as primary access.
  - E-UTRA not allowed as secondary access.
  - E-UTRA in unlicensed bands not allowed as secondary access.
  - NB-IoT not allowed as primary access.

- LTE-M not allowed as primary access.

In order to enforce all primary access restrictions, the related access has to be deployed in different Tracking Area Codes and the subscriber shall not be allowed to access the network in TAs using the particular access.

With all secondary access restrictions, the subscriber shall not be allowed to use this access as secondary access.

5.3.4.1.2 Management of Service Area Restrictions

This clause describes Service Area Restrictions for 3GPP access. For Service Area Restrictions when using wireline access, see TS 23.316 [84].

A Service Area Restriction may contain one or more (e.g. up to 16) entire Tracking Areas each or the Service Area Restriction may be set as unlimited (i.e. contain all Tracking Areas of the PLMN). The UE's subscription data in the UDM includes a Service Area Restriction which may contain either Allowed or Non-Allowed Areas–specified by using explicit Tracking Area identities and/or other geographical information (e.g., longitude/latitude, zip code, etc). The geographical information used to specify Allowed or Non-Allowed Area is only managed in the network, and the network will map it to a list of TAs before sending Service Area Restriction information to the PCF, NG-RAN and UE.

When the AMF assigns a limited allowed area to the UE, the AMF shall provide the UE with Service Area Restrictions which consist of either Allowed Areas or Non-Allowed Areas. The Allowed Areas included in the Service Area Restrictions can be pre-configured and/or dynamically assigned by the AMF.

The Allowed Area may alternatively be configured as unlimited i.e. it may contain all Tracking Areas of the PLMN. The Registration Area of a UE in the Non-Allowed Area should consist of a set of TAs which belongs to a Non-Allowed Area of the UE. The Registration Area of a UE in the Allowed Area should consist of a set of TAs which belongs to an Allowed Area of the UE. The AMF provides the Service Area Restriction in the form of TA(s), which may be a subset of full list stored in UE's subscription data or provided by the PCF, to the UE during the Registration procedure.

NOTE: As the finest granularity for Service Area Restrictions are at TA level, subscriptions with limited geographical extent, like subscriptions for Fixed Wireless Access, will be allocated one or a few TAs and will consequently be allowed to access services in a larger area than in e.g. a FWA system.

The limited allowed area may also be limited by the AMF by a maximum allowed number of Tracking Areas, even though this limitation is not sent to the UE. If maximum allowed number of Tracking Areas is used in combination with Allowed Area, the maximum allowed number of Tracking Areas indicates (to the AMF) the maximum number of TAs allowed in limited allowed area inside the Allowed Area. If maximum allowed number of Tracking Areas is used in combination with Non-Allowed Area, the maximum allowed number of Tracking Areas indicates (to the AMF) the maximum number of TAs allowed in limited allowed area outside of the Non-Allowed Area.

The UDM stores the Service Area Restrictions of a UE as part of the UE's subscription data. The PCF in the serving network may (e.g. due to varying conditions such as UE's location, application in use, time and date) further adjust Service Area Restrictions of a UE, either by expanding an Allowed Area or by reducing a Non-Allowed Area or by increasing the maximum allowed number of Tracking Areas. If NWDAF is deployed, the PCF may use analytics (i.e. statistics or predictions) on UE mobility from NWDAF (see TS 23.288 [86]) to adjust Service Area Restrictions. The UDM and the PCF may update the Service Area Restrictions of a UE at any time. For the UE in CM-CONNECTED state the AMF updates the UE and RAN immediately. For UE in CM-IDLE state the AMF may page the UE immediately or store the updated service area restriction and update the UE upon next signalling interaction with the UE, as defined in TS 24.501 [47].

During registration, if the Service Area Restrictions of the UE is not present in the AMF, the AMF fetches from the UDM the Service Area Restrictions of the UE that may be further adjusted by the PCF. The serving AMF shall enforce the Service Area Restrictions of a UE. A limited allowed area given by a maximum allowed number of Tracking Areas, may be dynamically assigned by the AMF adding any not yet visited (by the UE) Tracking Areas to the limited allowed area until the maximum allowed number of Tracking Areas is reached (i.e. the AMF adds new TAs to the limited allowed area until the number of TAs is equal to the maximum allowed number of Tracking Areas). The AMF deletes the list of TAs that have been used up under the maximum allowed number of Tracking Areas quota at every Initial Registration.

For a UE in CM-CONNECTED state the AMF shall indicate the Service Area Restrictions of this UE to the RAN, using a Mobility Restriction List.

The UE shall store the received Service Area Restrictions and, if there is previously stored Service Area Restrictions, replace them with the newly received information. If the Service Area Restrictions include a limited allowed area, the Service Area Restrictions are applicable for the Tracking areas indicated in Service Area Restrictions. If the Service Area Restrictions included an unlimited allowed area, the received Service Area Restrictions are applicable for the registered PLMN and its equivalent PLMN(s) that are available in the Registration Area. The RAN uses the Service Area Restrictions for target cell selection in Xn and N2 based handover.

Upon change of serving AMF due to mobility, the old AMF may provide the new AMF with the Service Area Restrictions of the UE that may be further adjusted by the PCF.

The network may perform paging for a UE to update Service Area Restrictions with Generic UE Configuration Update procedure (see in TS 23.502 [3] clause 4.2.4).

In the case of roaming, the Service Area Restrictions are transferred from the UDM via the serving AMF to the serving PCF in the visited network. The serving PCF in the visited network may further adjust the Service Area Restrictions.

5.3.4.2 Mobility Pattern

The Mobility Pattern is a concept that may be used by the AMF to characterise and optimise the UE mobility. The AMF determines and updates Mobility Pattern of the UE based on subscription of the UE, statistics of the UE mobility, network local policy, and the UE assisted information, or any combination of them. The statistics of the UE mobility can be historical or expected UE moving trajectory. If NWDAF is deployed, the statistics of the UE mobility can also be analytics (i.e. statistics or predictions) provided by the NWDAF (see TS 23.288 [86]).

The Mobility Pattern can be used by the AMF to optimize mobility support provided to the UE, for example, Registration area allocation.

5.3.4.3 Radio Resource Management functions

To support radio resource management in RAN the AMF provides the parameter 'Index to RAT/Frequency Selection Priority' (RFSP Index) to RAN across N2. The RFSP Index is mapped by the RAN to locally defined configuration in order to apply specific RRM strategies, taking into account any available information in RAN. The RFSP Index is UE specific and applies to all the Radio Bearers. Examples of how this parameter may be used by the RAN:

- to derive UE specific cell reselection priorities to control idle mode camping.
- to decide on redirecting active mode UEs to different frequency layers or RATs.

The HPLMN may set the RFSP Index taking into account the Subscribed S-NSSAIs. The AMF receives the subscribed RFSP Index from the UDM (e.g., during the Registration procedure). For non-roaming subscribers, the AMF chooses the RFSP Index in use according to one of the following procedures, depending on operator's configuration:

- the RFSP Index in use is identical to the subscribed RFSP Index, or
- the AMF chooses the RFSP Index in use based on the subscribed RFSP Index, the locally configured operator's policies, the Allowed NSSAI and the UE related context information available at the AMF, including UE's usage setting, if received during Registration procedures (see clause TS 23.502 [3]).

NOTE: One example of how the AMF can use the "UE's usage setting," is to select an RFSP value that enforces idle mode camping on E-UTRA for a UE acting in a "Voice centric" way, in the case voice over NR is not supported in the specific Registration Area and it contains NR cells.

The AMF may report to the PCF the subscribed RFSP Index received from the UDM for further evaluation as described in clause 6.1.2.1 in TS 23.503 [45]. When receiving the authorized RFSP Index from the PCF, the AMF shall replace the subscribed RFSP Index with the authorized RFSP Index.

For roaming subscribers the AMF may choose the RFSP Index in use based on the visited network policy, but can take input from the HPLMN into account (e.g., an RFSP Index value pre-configured per HPLMN, or a single RFSP Index value to be used for all roamers independent of the HPLMN).

The RFSP Index in use is also forwarded from source to target RAN node when Xn or N2 is used for intra-NG-RAN handover.

The AMF stores the subscribed RFSP Index value received and the RFSP Index value in use. During the Registration procedure, the AMF may update the RFSP Index value in use (e.g. the AMF may need to update the RFSP Index value in use if the UE related context information in the AMF has changed). When the RFSP Index value in use is changed, the AMF immediately provides the updated RFSP Index value in use to NG-RAN node by modifying an existing UE context or by establishing a new UE context in RAN or by being configured to include the updated RFSP Index value in use in the NGAP DOWNLINK NAS TRANSPORT message if the user plane establishment is not needed. During inter-AMF mobility procedures, the source AMF forwards both RFSP Index values to the target AMF. The target AMF may replace the received RFSP Index value in use with a new RFSP Index value in use that is based on the operator's policies and the UE related context information available at the target AMF.

In order to enable UE idle mode mobility control and priority-based reselection mechanism considering availability of Network Slices at the network and the Network Slices allowed for a UE, an RFSP is derived as described in clause 5.3.4.3, considering also the Allowed NSSAI for the UE.

5.3.4.4 UE mobility event notification

5G System supports the functionality of tracking and reporting UE mobility events.

The AMF provides the UE mobility related event reporting to NF that has been authorized to subscribe to the UE mobility event reporting service. Any NF service consumer such as SMF, NEF or NWDAF that wants to be reported on the UE location is able to subscribe to the UE mobility event notification service to the AMF with the following parameters:

- Event reporting type that specifies what to be reported on UE mobility (e.g. UE location, UE mobility on Area of Interest).
- Event filters indicating the:
  - Area Of Interest that specifies a geographical area within 3GPP system. The Area Of Interest is represented by a list of Tracking Areas, list of cells or list of (R)AN node identifiers. In the case of LADN, the event consumer (e.g. SMF) provides the LADN DNN to refer the LADN service area as the Area Of Interest. In the case of PRA, the event consumer (e.g. SMF or PCF) may provide an identifier for Area Of Interest to refer predefined area as the Area Of Interest.
  - S-NSSAI and optionally the NSI ID(s).
- Event Reporting Information: event reporting mode, number of reports, maximum duration of reporting, event reporting condition (e.g. when the target UE moved into a specified Area Of Interest, immediate reporting flag).
- Notification Endpoint of NF service consumer to be notified.
- The target of event reporting that indicates a specific UE, a group of UE(s) or any UE (i.e. all UEs). Further details on the information provided by the NF service consumer are provided in clause 4.15 of TS 23.502 [3].

If an NF service consumer subscribes to the UE mobility event notification service provided by AMF for reporting of UE presence in Area Of Interest, the AMF tracks UE's location considering UE's CM state and using NG-RAN procedures (if RRC Inactive state applies to NG-RAN) in order to determine the UE presence in the Area Of Interest, as described in clause 4.15.4.2 of TS 23.502 [3]. Upon detecting the change of the UE presence in the Area Of Interest, the AMF notifies the UE presence in the Area Of Interest and the new UE location to the subscribed NF consumer.

When the AMF is changed, the subscription of mobility event is transferred from the old AMF. The new AMF may decide not to notify the SMF with the current status related to the subscription of mobility event if the new AMF determines that, based on MM Context of the UE, the event is reported by the old AMF.

In the network deployment where a UE may leave or enter the Area Of Interest without any notification to the 5GC in CM-CONNECTED state (i.e. in the case that RRC Inactive state applies to the NG-RAN), the AMF may initiate the NG-RAN location reporting as described in clause 5.4.7 or N2 Notification as described in TS 23.502 [3] clause 4.8.3 to track the UE presence in the Area Of Interest.

The AMF may provide UE mobility event reporting to PCF, using Policy Control Report Triggers defined in TS 23.503 [45].

5.4 3GPP access specific aspects

5.4.1 UE reachability in CM-IDLE

5.4.1.1 General

Reachability management is responsible for detecting whether the UE is reachable and providing UE location (i.e. access node) for the network to reach the UE. This is done by paging UE and UE location tracking. The UE location tracking includes both UE registration area tracking (i.e. UE registration area update) and UE reachability tracking ((i.e. UE periodic registration area update)). Such functionalities can be either located at 5GC (in the case of CM-IDLE state) or NG-RAN (in the case of CM-CONNECTED state).

The UE and the AMF negotiate UE reachability characteristics for CM-IDLE state during Registration procedures.

Two UE reachability categories are negotiated between UE and AMF for CM-IDLE state:

1. UE reachability allowing Mobile Terminated data while the UE is CM-IDLE state.
   - The UE location is known by the network on a Tracking Area List granularity
   - Paging procedures apply to this category.
   - Mobile originating and mobile terminated data apply in this category for both CM-CONNECTED and CM-IDLE state.
2. Mobile Initiated Connection Only (MICO) mode:
   - Mobile originated data applies in this category for both CM-CONNECTED and CM-IDLE state.
   - Mobile terminated data is only supported when the UE is in CM-CONNECTED state.

Whenever a UE in RM-REGISTERED state enters CM-IDLE state, it starts a periodic registration timer according to the periodic registration timer value received from the AMF during a Registration procedure.

The AMF allocates a periodic registration timer value to the UE based on local policies, subscription information and information provided by the UE. After the expiry of the periodic registration timer, the UE shall perform a periodic registration. If the UE moves out of network coverage when its periodic registration timer expires, the UE shall perform a Registration procedure when it next returns to the coverage.

The AMF runs a Mobile Reachable timer for the UE. The timer is started with a value longer than the UE's periodic registration timer whenever the CM state for the UE in RM-REGISTERED state changes to CM-IDLE. If the AMF receives an elapsed time from RAN when RAN initiate UE context release indicating UE unreachable, the AMF should deduce a Mobile Reachable timer value based on the elapsed time received from RAN and the normal Mobile Reachable timer value. The AMF stops the Mobile Reachable timer, if the UE CM state in the AMF moves to CM-CONNECTED state. If the Mobile Reachable timer expires, the AMF determines that the UE is not reachable.

However, the AMF does not know for how long the UE remains not reachable, thus the AMF shall not immediately de-register the UE. Instead, after the expiry of the Mobile Reachable timer, the AMF should clear the PPF and shall start an Implicit De-registration timer, with a relatively large value. The AMF shall stop the Implicit De-registration timer and set the PPF if the AMF moves the UE CM state in the AMF to CM-CONNECTED state.

NOTE: If the UE CM state in the AMF is CM-IDLE, then AMF considers the UE always unreachable if the UE is in MICO mode (refer to clause 5.4.1.3).

If the PPF is not set, the AMF does not page the UE and shall reject any request for delivering DL signalling or data to this UE.

If the Implicit De-registration timer expires before the UE contacts the network, the AMF implicitly de-register the UE.

As part of deregistration for a particular access (3GPP or non-3GPP), the AMF shall request the UE's related SMF to release the PDU Sessions established on that access.

5.4.1.2 UE reachability allowing mobile terminated data while the UE is CM-IDLE

The AMF considers a UE in RM-REGISTERED state to be reachable by CN paging if the UE CM state in the AMF is CM-IDLE state unless the UE applies MICO mode.

5.4.1.3 Mobile Initiated Connection Only (MICO) mode

A UE may indicate preference for MICO mode during Initial Registration or Mobility Registration Update procedure. The AMF, based on local configuration, Expected UE Behaviour and/or Network Configuration parameters if available from the UDM, UE indicated preferences, UE subscription information and network policies, or any combination of them, determines whether MICO mode is allowed for the UE and indicates it to the UE during Registration procedure. If NWDAF is deployed, the AMF may also use analytics on UE mobility and/or UE communication generated by NWDAF (see TS 23.288 [86]) to decide MICO mode parameters. If the UE does not indicate preference for MICO mode during Registration procedure, the AMF shall not activate MICO mode for this UE.

The UE and the AMF re- negotiate the MICO mode at every subsequent Registration procedure. When the UE is in CM-CONNECTED, the AMF may deactivate MICO mode by triggering Mobility Registration Update procedure through UE Configuration Update procedure as described in clause 4.2.4 in TS 23.502 [3].

The AMF assigns a registration area to the UE during the Registration procedure. When the AMF indicates MICO mode to a UE, the registration area is not constrained by paging area size. If the AMF serving area is the whole PLMN, based on local policy, and subscription information, may decide to provide an "all PLMN" registration area to the UE. In that case, re-registration to the same PLMN due to mobility does not apply.

If Mobility Restrictions are applied to a UE in MICO mode, the AMF needs to allocate an Allowed Area/Non-Allowed Area to the UE as specified in clause 5.3.4.1.

When the AMF indicates MICO mode to a UE, the AMF considers the UE always unreachable while the UE CM state in the AMF is CM-IDLE. The AMF rejects any request for downlink data delivery for UE in MICO mode and whose UE CM state in the AMF is CM-IDLE with an appropriate cause. For MT-SMS over NAS, the AMF notifies the SMSF that UE is not reachable, then the procedure of the unsuccessful Mobile terminating SMS delivery described in clause 4.13.3.9 in TS 23.502 [3] is performed. The AMF also defers location services, etc. The UE in MICO mode is only reachable for mobile terminated data or signalling when the UE is in CM-CONNECTED.

A UE in MICO mode need not listen to paging while in CM-IDLE. A UE in MICO mode may stop any access stratum procedures in CM-IDLE, until the UE initiates transition from CM-IDLE to CM-CONNECTED due to one of the following triggers:

- A change in the UE (e.g. change in configuration) requires an update of its registration with the network.
- Periodic registration timer expires.
- MO data pending.
- MO signalling pending (e.g. SM procedure initiated).

If a registration area that is not the "all PLMN" registration area is allocated to a UE in MICO mode, then the UE determines if it is within the registration area or not when it has MO data or MO signalling, and the UE performs Mobility Registration Update before the UE initiates the MO data or MO signalling if it is not within the registration area.

A UE initiating emergency service shall not indicate MICO preference during Registration procedure. When the MICO mode is already activated in the UE, the UE and AMF shall locally disable MICO mode after PDU Session Establishment procedure for Emergency Services is completed successfully. The UE and the AMF shall not enable MICO mode until the AMF accepts the use of MICO mode in the next registration procedure. To enable an emergency call back, the UE should wait for a UE implementation-specific duration of time before requesting the use of MICO mode after the release of the emergency PDU session.

In order to enable power saving for MT reachability e.g. for Cellular IoT, enhancements to MICO mode are specified in clause 5.31.7:

- MICO mode with Extended Connected Time.
- MICO mode with Active Time.

- MICO mode and Periodic Registration Timer Control.

5.4.2 UE reachability in CM-CONNECTED

For a UE in CM-CONNECTED state:

- the AMF knows the UE location on a serving (R)AN node granularity.
- the NG-RAN notifies the AMF when UE becomes unreachable from RAN point of view.

UE RAN reachability management is used by RAN for UEs in RRC Inactive state, see TS 38.300 [27]. The location of a UE in RRC Inactive state is known by the RAN on a RAN Notification area granularity. A UE in RRC Inactive state is paged in cells of the RAN Notification area that is assigned to the UEs. The RAN Notification area can be a subset of cells configured in UE's Registration Area or all cells configured in the UE's Registration Area. UE in RRC Inactive state performs RAN Notification Area Update when entering a cell that is not part of the RAN Notification area that is assigned to the UE.

At transition into RRC Inactive state RAN configures the UE with a periodic RAN Notification Area Update timer value and the timer is restarted in the UE with this initial timer value. After the expiry of the periodic RAN Notification Area Update timer in the UE, the UE in RRC Inactive state performs periodic RAN Notification Area Update, as specified in TS 38.300 [27].

To aid the UE reachability management in the AMF, RAN uses a guard timer with a value longer than the RAN Notification Area Update timer value provided to the UE. Upon the expiry of the periodic RAN Notification Area Update guard timer in RAN, the RAN shall initiate the AN Release procedure as specified in TS 23.502 [3]. The RAN may provide the elapsed time since RAN's last contact with the UE to AMF.

5.4.3 Paging strategy handling

5.4.3.1 General

Based on operator configuration, the 5GS supports the AMF and NG-RAN to apply different paging strategies for different types of traffic.

In the case of UE in CM-IDLE state, the AMF performs paging and determines the paging strategy based on e.g. local configuration, what NF triggered the paging and information available in the request that triggered the paging. If NWDAF is deployed, the AMF may also use analytics (i.e. statistics or predictions) on the UE's mobility as provided by NWDAF (see TS 23.288 [86]).

In the case of UE in CM-CONNECTED with RRC Inactive state, the NG-RAN performs paging and determines the paging strategy based on e.g. local configuration, and information received from AMF as described in clause 5.4.6.3 and SMF as described in clause 5.4.3.2.

In the case of Network Triggered Service Request from SMF, the SMF determines the 5QI and ARP based on the downlink data or the notification of downlink data received from UPF. The SMF includes the 5QI and ARP corresponding to the received downlink PDU in the request sent to the AMF. If the UE is in CM IDLE, the AMF uses e.g. the 5QI and ARP to derive different paging strategies as described in TS 23.502 [3], clause 4.2.3.3.

NOTE: The 5QI is used by AMF to determine suitable paging strategies.

5.4.3.2 Paging Policy Differentiation

Paging policy differentiation is an optional feature that allows the AMF, based on operator configuration, to apply different paging strategies for different traffic or service types provided within the same PDU Session. In this Release of the specification this feature applies only to PDU Session of IP type.

When the 5GS supports the Paging Policy Differentiation (PPD) feature, the DSCP value (TOS in IPv4 / TC in IPv6) is set by the application to indicate to the 5GS which Paging Policy should be applied for a certain IP packet. For example, as defined in TS 23.228 [15], the P-CSCF may support Paging Policy Differentiation by marking packet(s) to be sent towards the UE that relate to a specific IMS services (e.g. conversational voice as defined in IMS multimedia telephony service).

It shall be possible for the operator to configure the SMF in such a way that the Paging Policy Differentiation feature only applies to certain HPLMNs, DNNs and 5QIs. In the case of HR roaming, this configuration is done in the SMF in the VPLMN.

NOTE 1: Support of Paging Policy Differentiation in the case of HR roaming requires inter operator agreements including on the DSCP value associated with this feature.

In the case of Network Triggered Service Request and UPF buffering downlink data packet, the UPF shall include the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the downlink data packet and an indication of the corresponding QoS Flow in the data notification message sent to the SMF. When PPD applies, the SMF determines the Paging Policy Indicator (PPI) based on the DSCP received from the UPF.

In the case of Network Triggered Service Request and SMF buffering downlink data packet, when PPD applies, the SMF determines the PPI based on the DSCP in TOS (IPv4) / TC (IPv6) value from the IP header of the received downlink data packet and identifies the corresponding QoS Flow from the QFI of the received downlink data packet.

The SMF includes the PPI, the ARP and the 5QI of the corresponding QoS Flow in the N11 message sent to the AMF. If the UE is in CM IDLE, the AMF uses this information to derive a paging strategy, and sends paging messages to NG-RAN over N2.

NOTE 2: Network configuration needs to ensure that the information used as a trigger for Paging Policy Indication is not changed within the 5GS.

NOTE 3: Network configuration needs to ensure that the specific DSCP in TOS (IPv4) / TC (IPv6) value, used as a trigger for Paging Policy Indication, is managed correctly in order to avoid the accidental use of certain paging policies.

For a UE in RRC Inactive state the NG-RAN may enforce specific paging policies in the case of NG-RAN paging, based on 5QI, ARP and PPI associated with an incoming DL PDU. To enable this, the SMF instructs the UPF to detect the DSCP in the TOS (IPv4) / TC (IPv6) value in the IP header of the DL PDU (by using a DL PDR with the DSCP for this traffic) and to transfer the corresponding PPI in the CN tunnel header (by using a QER with the PPI value). The NG-RAN can then utilize the PPI received in the CN tunnel header of an incoming DL PDU in order to apply the corresponding paging policy for the case the UE needs to be paged when in RRC Inactive state. In the case of Home-Routed roaming, the V-SMF is responsible of controlling UPF setting of the PPI. In the case of PDU Session with I-SMF, the I-SMF is responsible of controlling UPF setting of the PPI.

5.4.3.3 Paging Priority

Paging Priority is a feature that allows the AMF to include an indication in the Paging Message sent to NG-RAN that the UE be paged with priority. The decision by the AMF whether to include Paging Priority in the Paging Message is based on the ARP value in the message received from the SMF for an IP packet waiting to be delivered in the UPF. If the ARP value is associated with select priority services (e.g., MPS, MCS), the AMF includes Paging Priority in the Paging Message. When the NG-RAN receives a Paging Message with Paging Priority, it handles the page with priority.

The AMF while waiting for the UE to respond to a page sent without priority receives another message from the SMF with an ARP associated with select priority services (e.g., MPS, MCS), the AMF sends another Paging message to the (R)AN including the Paging Priority. For subsequent messages, the AMF may determine whether to send the Paging message with higher Paging Priority based on local policy.

For a UE in RRC Inactive state, the NG-RAN determines Paging Priority based on the ARP associated with the QoS Flow as provisioned by the operator policy, and the Core Network Assisted RAN paging information from AMF as described in clause 5.4.6.3.

5.4.4 UE Radio Capability handling

5.4.4.1 UE radio capability information storage in the AMF

This clause applies when no radio capability signalling optimisation is used between a UE and the network.

The UE Radio Capability information contains information on RATs that the UE supports (e.g. power class, frequency bands, etc). Consequently, this information can be sufficiently large that it is undesirable to send it across the radio interface at every transition of UE CM state in the AMF from CM-IDLE to CM-CONNECTED. To avoid this radio overhead, the AMF shall store the UE Capability information during CM-IDLE state for the UE and RM-

REGISTERED state for the UE and the AMF shall if it is available, send its most up to date UE Radio Capability information to the RAN in the N2 REQUEST message, i.e. INITIAL CONTEXT SETUP REQUEST or UE RADIO CAPABILITY CHECK REQUEST.

The AMF deletes the UE radio capability when the UE RM state in the AMF transitions to RM-DEREGISTERED.

The UE Radio Capability is maintained in the core network, even during AMF reselection.

NOTE: The UE Radio Capability is not transferred to EPC during the inter-system mobility.

If the UE's NG-RAN UE Radio Capability information changes while in CM-IDLE state, the UE shall perform the Registration procedure with the Registration type set to Mobility Registration Update and it also includes "UE Radio Capability Update". When the AMF receives Mobility Registration Update Request with "UE Radio Capability Update" requested by the UE, it shall delete any UE Radio Capability information that it has stored for the UE.

If the trigger to change the UE's NG-RAN UE Radio Capability information happens when the UE is in CM-CONNECTED state, the UE shall first enter CM-IDLE state and then perform the Registration procedure with the Registration type set to Mobility Registration Update and it also includes "UE Radio Capability Update".

The RAN stores the UE Radio Capability information, received in the N2 message or obtained from the UE, for the duration of the UE staying in RRC connected or RRC Inactive state.

If the AMF sends N2 REQUEST (i.e. INITIAL CONTEXT SETUP REQUEST or UE RADIO CAPABILITY CHECK REQUEST) message to NG-RAN without UE Radio Capability information in that message and there is no UE Radio Capability information available in RAN, this triggers the RAN to request the UE Radio Capability from the UE and to upload it to the AMF in the N2 UE RADIO CAPABILITY INFO INDICATION message.

If a UE supports both NB-IoT and other RATs the UE handles the UE Radio capability information as follows:

- When the UE is camping on NB-IoT the UE provides only NB-IoT UE radio capabilities to the network.
- When the UE is not camping on NB-IoT, the UE provides UE radio capabilities for the RAT but not NB-IoT UE radio capabilities to the network.

In order to handle the distinct UE radio capabilities, the AMF stores a separate NB-IoT specific UE Radio Capability information when the UE provides the UE Radio Capability information while camping on NB-IoT.

When the UE is camping on NB-IoT, the AMF sends, if available, the NB-IoT RAT specific UE Radio Capability information to the E-UTRAN.

When the UE is not camping on NB-IoT, the AMF sends, if available, UE radio capabilities for the RAT but not NB-IoT radio capabilities.

5.4.4.1a UE radio capability signalling optimisation (RACS)

With the increase of the size of UE radio capabilities driven e.g. by additional frequency bands and combinations thereof for E-UTRA and NR, an efficient approach to signal UE Radio Capability Information over the radio interface and other network interfaces is defined with RACS.

In this Release of the specification, RACS does not apply to NB-IOT.

RACS works by assigning an identifier to represent a set of UE radio capabilities. This identifier is called UE Radio Capability ID. A UE Radio Capability ID can be either UE manufacturer-assigned or PLMN-assigned, as specified in clause 5.9.10. The UE Radio Capability ID is an alternative to the signalling of the UE Radio Capability information over the radio interface, within NG-RAN, from NG-RAN to E-UTRAN, from AMF to NG-RAN and between CN nodes supporting RACS.

PLMN-assigned UE Radio Capability ID is assigned to the UE using the UE Configuration Update Command, or Registration Accept as defined in TS 23.502 [3]. The UCMF shall be configured with a Version ID for PLMN-assigned UE Radio Capability IDs, defined in clause 5.9.10.

The UCMF (UE radio Capability Management Function) stores all UE Radio Capability ID mappings in a PLMN and is responsible for assigning every PLMN-assigned UE Radio Capability ID in this PLMN, see clause 6.2.21. The UCMF stores the UE Radio Capability IDs alongside the UE Radio Capability information they map to. Each UE Radio Capability ID stored in the UCMF can be associated to one or both UE radio capabilities formats specified in

TS 36.331 [51] and TS 38.331 [28]. The two UE radio capabilities formats shall be identifiable by the AMF and UCMF and the AMF shall store the TS 38.331 [28] format only.

An NG-RAN which supports RACS can be configured to operate with one of two modes of operation when providing the UE radio capabilities to the AMF when the NG-RAN executes a UE Radio Capability Enquiry procedure (see TS 38.331 [28]) to retrieve UE radio capabilities from the UE:

- Mode of operation A): The NG-RAN provides to the AMF both formats (i.e the TS 38.331 [28] format and TS 36.331 [51] format). The NG-RAN derives one of the formats using local transcoding of the other format it receives from the UE.

- Mode of operation B): The NG-RAN provides to the AMF the TS 38.331 [28] format only.

In a PLMN supporting RACS only in 5GS, Mode of Operation B shall be configured.

If the PLMN supports RACS in both EPS and 5GS:

- If RAN nodes in the EPS and 5GS are configured in Mode of operation B, then the UCMF shall be capable to transcode between TS 36.331 [51] and TS 38.331 [28] formats.

- If the NG-RAN is configured to operate according to Mode A, then also the E-UTRAN shall be configured to operate according to mode A and the UMCF is not required to transcode between TS 36.331 [51] and TS 38.331 [28] formats.

When the NG-RAN updates the AMF with new UE radio capabilities information, the AMF provides the information obtained from the NG-RAN to the UCMF even if the AMF already has a UE Radio Capability ID for that UE. The UCMF then returns a value of UE Radio Capability ID. If the value is different from the one stored in the AMF, the AMF updates the UE Radio Capability ID it stores and provides this new value to the NG-RAN (if applicable) and to the UE.

In order to be able to interpret the UE Radio Capability ID a Network Function or node may store a local copy of the mapping between the UE Radio Capability ID and its corresponding UE Radio Capability information i.e. a dictionary entry. When no mapping is available between a UE Radio Capability ID and the corresponding UE Radio Capability information in a Network Function or node, this Network Function or node shall be able to retrieve this mapping and store it.

- An AMF which supports RACS shall store such UE Radio Capability ID mapping at least for all the UEs that it serves that have a UE Radio Capability ID assigned.

- The NG-RAN performs local caching of the UE Radio Capability information for the UE Radio Capability IDs for the UEs it is serving, and potentially for other UE Radio Capability IDs according to suitable local policies.

- When the NG-RAN needs to retrieve the mapping of a UE Radio Capability ID to the corresponding UE Radio Capability information, it queries the AMF using N2 signalling defined in TS 38.413 [34].

- When the AMF needs to obtain a PLMN-assigned UE Radio Capability ID for a UE from the UCMF, it provides the UE Radio Capability information it has for the current radio configuration of the UE and the IMEI/TAC for the UE and the UCMF returns a UE Radio Capability ID. The AMF shall provide to the UCMF the UE Radio Capability information obtained from the NG-RAN in one or both the TS 36.331 [51] and TS 38.331 [28] formats depending on how the RAN is configured. The UCMF stores the association of this IMEI/TAC with this UE Radio Capability ID and the UE Radio Capability information in all the formats it receives. The UE Radio Capability information formats the AMF provides shall be identifiable at the UCMF.

- When the AMF needs to obtain the UE Radio Capability information associated to a UE Radio Capability ID it provides the UE Radio Capability ID to the UCMF with an indication that it is requesting the TS 38.331 [28] format and the UCMF returns a mapping of the UE Radio Capability ID to the corresponding UE Radio Capability information in TS 38.331 [28] format to the AMF.

- UEs, AMFs and RAN nodes which support RACS learn the current value of the Version ID when a new PLMN-assigned UE Radio Capability ID is received from the UCMF and the Version ID it contains is different from the ones in their PLMN Assigned UE Radio Capability ID cache. For a PLMN, PLMN-assigned UE Radio Capability IDs related to old values (i.e. not current value) of the Version ID can be removed from cache but, if so, prior to removing any cached PLMN-assigned UE radio Capability IDs with the current value of the Version ID.. The AMF, RAN and UE may continue to use the stored PLMN assigned UE Radio Capability IDs with old values of the Version ID, until these are purged from cache. If an out of date PLMN assigned UE Radio

Capability ID is removed form an AMF cache, the AMF shall proceed to assign a new PLMN assigned UE Radio Capability ID to all the UEs for which the UE context includes the removed PLMN-assigned UE Radio Capability ID using a UE Configuration Update procedure, or when these UEs perform a Registration. If the AMF attempts to resolve a PLMN assigned UE Radio capability ID with an old Version ID, the UCMF shall return an error code indicating that the Version ID in the UE radio capability ID is no longer current and proceed to assign a new UE Radio Capability ID to the UE.

If at any time the AMF has neither a valid UE Radio Capability ID nor any stored UE radio capabilities for the UE, the AMF may trigger the RAN to provide the UE Radio Capability information and subsequently request the UCMF to allocate a UE Radio Capability ID.

- The RAN, in order to support MOCN network sharing scenarios, shall be capable to cache PLMN assigned UE Radio Capability IDs per PLMN ID.

A network may utilise the PLMN-assigned UE Radio Capability ID, without involving the UE, e.g. for use with legacy UEs.

Mutual detection of the support of the RACS feature happens between NG-RAN nodes at Xn setup and between NG-RAN and AMF at N2 setup time. To allow for a mix of RACS-supporting and non-RACS-supporting RAN nodes over the Xn interfaces, the UE Radio Capability ID should be included in the Path Switch signalling during Xn based handover and Handover Request during N2 based handover between AMF and NG-RAN. In addition, RACS-supporting RAN nodes can be discovered across inter-CN node boundaries e.g. using the Configuration Transfer procedure. The support of RACS by peer AMFs or MMEs is based on configuration in a PLMN or across PLMNs.

A UE that supports WB-E-UTRA and/or NR indicates its support for RACS to AMF using UE MM Core Network Capability as defined in clause 5.4.4a.

A UE that supports RACS and stores an applicable UE Radio Capability ID for the current UE Radio Configuration in the PLMN, shall signal the UE Radio Capability ID in the Initial Registration procedure as defined in TS 23.502 [3]. If both PLMN-assigned for the current PLMN and UE manufacturer-assigned UE Radio Capability IDs are stored in the UE and applicable in the PLMN, the UE shall signal the PLMN-assigned UE Radio Capability ID in the Registration Request message.

When a PLMN decides to switch to request a particular type of UE to use UE manufacturer-assigned UE Radio Capability ID(s):

- The UCMF sends a Nucmf_UECapabilityManagement_Notify message to the AMF including either a list of UE Radio Capability IDs (if the UE was previously using any PLMN-assigned IDs) or the IMEI/TAC values corresponding to UE types that are requested to use UE manufacturer-assigned UE Radio Capability ID. These values are stored in a "UE Manufacturer Assigned operation requested list" in the AMF.

- The AMF uses the Registration Accept message or the UE Configuration Update command message to request the UE to delete all the PLMN-assigned UE Radio Capability ID(s) for this PLMN if the UE is, respectively, registering or is registered with PLMN-assigned ID or IMEI/TAC values matching one value in the "UE Manufacturer Assigned operation requested list".

NOTE 1: It is expected that in a given PLMN the UCMF and AMFs will be configured to either use a UE manufacturer-assigned operation requested list based on a list of PLMN-assigned UE Radio Capability IDs or a list of IMEI/TACs, but not both.

NOTE 2: The strategy for triggering of the deletion of PLMN-assigned UE Radio Capability ID(s) in the UE by the AMF is implementation-specific (e.g. can be used only towards UEs in CM_Connected state).

- a UE that receives indication to delete all the PLMN-assigned UE Radio Capability IDs in the Registration Accept message, or UE Configuration Update command message, shall delete any PLMN-assigned UE Radio Capability IDs for this PLMN. The UE proceeds to register with a UE manufacturer-assigned UE Radio Capability ID that is applicable to the current UE Radio configuration.

- When the "UE Manufacturer Assigned operation requested list" contains PLMN-assigned UE Radio Capability IDs, the UCMF shall avoid re-assigning PLMN-assigned UE Radio Capability IDs that were added to the "UE Manufacturer Assigned operation requested list" in the AMFs to any UE.

- The AMF stores a PLMN-assigned ID in the "UE Manufacturer Assigned operation requested list" for a time duration that is implementation specific, but IMEI/TACs are stored until the UCMF require to remove certain

TACs from the list (i.e. the list of IMEI/TACs which are requested to use UE manufacturer-assigned IDs in the AMF and UCMF is synchronised at all times).

- The UCMF can request at any time the AMF to remove PLMN-assigned ID(s) or IMEI/TAC(s) values from the UE manufacturer-assigned operation requested list.

NOTE 3: The AMF can decide to remove a UE Radio Capability ID from the "UE Manufacturer Assigned operation requested list" list e.g. because no UE with that UE Radio Capability ID has connected to the network for long time. If later a UE with such UE Radio Capability ID connects to the network, the AMF contacts the UCMF to resolve the UE Radio Capability ID, and at this point the UCMF can trigger again the deletion of the UE Radio Capability ID by including this in the "UE Manufacturer Assigned operation requested list" of the AMF.

The serving AMF stores the UE Radio Capability ID for a UE in the UE context and provides this UE Radio Capability ID to NG-RAN as part of the UE context information using N2 signalling. During inter PLMN mobility, the new AMF shall delete the UE Radio Capability ID received from the old AMF, unless the operator policy indicates that all UE Radio Capability IDs used in the old PLMN is also valid in the new PLMN.

The UE stores the PLMN-assigned UE Radio Capability ID in non-volatile memory when in RM-DEREGISTERED state and can use it again when it registers in the same PLMN.

NOTE 4: It is assumed that UE does not need to store the access stratum information (i.e. UE-E-UTRA-Capability and UE-NR-Capability specified in TS 36.331 [51] and TS 38.331 [28], respectively) that was indicated by the UE to the network when the PLMN-assigned UE Radio Capability ID was assigned by the network. However, it is assumed that the UE does store the related UE configuration (e.g. whether or not GERAN or UTRAN or MBMS is enabled/disabled).

At any given time at most one UE Radio Capability ID is stored in the UE context in CN and RAN.

The number of PLMN-assigned UE Radio Capability IDs that the UE stores in non-volatile memory is left up to UE implementation. However, to minimise the load (e.g. from radio signalling) on the Uu interface and to provide smoother inter-PLMN mobility (e.g. at land borders) the UE shall be able to store at least the latest 16 PLMN-assigned UE Radio Capability IDs (along with the PLMN that assigned them). This number is independent of the UE manufacturer-assigned UE Radio Capability ID(s) the UE may store.

It shall be possible for a UE to change, e.g. upon change in its usage settings, the set of UE radio capabilities in time and signal the associated UE Radio Capability ID, if available. The UE stores the mapping between the UE Radio Capability ID and the corresponding UE Radio Capability Information for every UE Radio Capability ID it stores.

If the UE's Radio Capability Information changes and there is no the associated UE Radio Capability ID for the updated UE Radio Capability information, the UE shall perform capability update procedure as defined in clause 5.4.4.1.

The NG-RAN may apply RRC filtering of UE radio capabilities when it retrieves the UE Radio Capability Information from the UE as defined in TS 38.331 [28].

NOTE 5: In a RACS supporting PLMN, the filter of UE radio capabilities configured in NG-RAN is preferably as wide in scope as possible (e.g. PLMN-wide). In this case, it corresponds e.g. to the super-set of bands, band-combinations and RATs the PLMN deploys and not only to the specific NG-RAN node or region.

NOTE 6: If the filter, included in the UE Radio Capability information, of UE radio capabilities configured in two NG-RAN nodes is different, during handover between these two nodes, it is possible that the target NG-RAN node might need to enquire the UE for its UE Radio Capability Information again and trigger re-allocation of a PLMN-assigned UE Radio Capability ID leading to extra signalling. Additionally, a narrow filter might reduce the list of candidate target nodes.

If a UE supports both NB-IoT and other RATs that do support RACS (e.g. WB-E-UTRA and/or NR) then (since there is no support for RACS in NB-IoT) the UE handles the RACS procedures as follows:

- NB-IoT specific UE Radio Capability Information is handled in UE, NG-RAN and AMF according to clause 5.4.4.1 and in EPS according to TS 23.401 [26].

- when the UE is not camping on NB-IoT, the RAN provides UE radio capabilities for other RATs but not NB-IoT UE radio capabilities, according to TS 38.300 [27] and TS 36.300 [30]. As a result the UE Radio Capability ID that is assigned by the network corresponds only to the UE radio capabilities of the non-NB-IoT RATs. The UE

uses the UE Radio Capability IDs assigned only in Mobility Registration Update procedures performed over non-NB-IoT RATs.

Support for RACS in EPS is defined in TS 23.401 [26].

5.4.4.2 Void

5.4.4.2a UE Radio Capability Match Request

If the AMF requires more information on the UE radio capabilities support to be able to set the IMS voice over PS Session Supported Indication (see clause 5.16.3), then the AMF may send a UE Radio Capability Match Request message to the NG-RAN. This procedure is typically used during the Registration Procedure or when AMF has not received the Voice Support Match Indicator (as part of the 5GMM Context).

NOTE: During the Registration Procedure, if the AMF does not already have the UEs radio capabilities, and if the RAT where the UE is requires the establishement of AN security context prior to retrieval of radio capabilities, the AMF needs to initiate "Initial Context Setup" procedure as defined in TS 38.413 [34] to provide the 5G-AN with security context, before sending a UE Radio Capability Match Request message.

5.4.4.3 Paging assistance information

The paging assistance information contains UE radio related information that assists the RAN for efficient paging. The Paging assistance information contains:

a) UE radio capability for paging information:

- The UE Radio Capability for Paging Information contains information derived by the NG-RAN node (e.g. band support information) from the UE Radio Capability information. The AMF stores this information without needing to understand its contents.

  As the AMF only infrequently -e.g. at Initial Registration) prompts the NG-RAN to retrieve and upload the UE radio capabilities i.e. UE Radio Capability information to the AMF, and the AMF may be connected to more than one NG-RAN RAT, it is the responsibility of the NG-RAN to ensure that UE Radio Capability for Paging Information -which is derived by the NG-RAN node) contains information on all NG-RAN RATs that the UE supports in that PLMN. To assist the NG-RAN in this task, -and as specified in TS 38.413 [34]) the AMF provides its stored UE Radio Capability for Paging Information in every NG-AP INITIAL CONTEXT SETUP REQUEST message sent to the NG-RAN.

- The UE Radio Capability for Paging Information is maintained in the core network, even during AMF reselection.

b) Information On Recommended Cells And RAN nodes For Paging:

- Information sent by the NG-RAN, and used by the AMF when paging the UE to help determining the NG RAN nodes to be paged as well as to provide the information on recommended cells to each of these RAN nodes, in order to optimize the probability of successful paging while minimizing the signalling load on the radio path.

- The RAN provides this information during N2 release.

5.4.4a UE MM Core Network Capability handling

The UE MM Core Network Capability is split into the S1 UE network capability (mostly for E-UTRAN access related core network parameters) and the UE 5GMM Core Network Capability (mostly to include other UE capabilities related to 5GCN or interworking with EPS) as defined in TS 24.501 [47] and contains non radio-related capabilities, e.g. the NAS security algorithms etc. The S1 UE network capability is transferred between all CN nodes at AMF to AMF, AMF to MME, MME to MME, and MME to AMF changes. The UE 5GMM Core Network Capability is transferred only at AMF to AMF changes.

In order to ensure that the UE MM Core Network Capability information stored in the AMF is up to date (e.g. to handle the situation when the USIM is moved into a different device while out of coverage, and the old device did not send the Detach message; and the cases of inter-RAT Registration Area Update), the UE shall send the UE MM Core Network Capability information to the AMF during the Initial Registration and Mobility Registration Update procedure within the NAS message.

The AMF shall store always the latest UE MM Core Network Capability received from the UE. Any UE MM Core Network Capability that an AMF receives from an old AMF/MME is replaced when the UE provides the UE MM Core Network Capability with Registration signalling.

If the UE's UE MM Core Network Capability information changes (in either CM-CONNECTED or in CM-IDLE state), the UE shall perform a Mobility Registration Update procedure when it next returns to NG-RAN coverage. See clause 4.2.2 of TS 23.502 [3].

The UE shall indicate in the UE 5GMM Core Network Capability if the UE supports:

- Attach in EPC with Request type "Handover" in PDN CONNECTIVITY Request message (TS 23.401 [26], clause 5.3.2.1).
- EPC NAS.
- SMS over NAS.
- LCS.
- 5G SRVCC from NG-RAN to UTRAN, as specified in TS 23.216 [88].
- Radio Capabilities Signalling optimisation (RACS).
- Network Slice-Specific Authentication and Authorization.
- Parameters in Supported Network Behaviour for 5G CIoT as described in clause 5.31.2.
- Receiving WUS Assistance Information.
- CAG, see clause 5.30.3.3.

5.4.4b UE 5GSM Core Network Capability handling

The UE 5GSM Core Network Capability is included in PDU Session Establishment/Modification Request.

The UE shall indicate in the UE 5GSM Core Network Capability whether the UE supports:

- "Ethernet" PDU Session Type supported in EPC as PDN Type "Ethernet";
- Reflective QoS;
- Multi-homed IPv6 PDU Session (only if the Requested PDU Type was set to "IPv6" or "IPv4v6");
- ATSSS capability (as referred to clause 5.32.2);
- Transfer of Port Management Information containers.

The 5GSM Core Network Capability is transferred, if needed, from V-SMF to H-SMF during PDU Session Establishment/Modification procedure.

After the first inter-system change from EPS to 5GS for a PDU session established in EPS, the 5GSM Core Network Capability is also included in the PDU Session Modification if the Reflective QoS and/or Multi-homed IPv6 PDU Session is present.

5.4.5 DRX (Discontinuous Reception) framework

The 5G System supports DRX architecture which allows Idle mode DRX cycle is negotiated between UE and the AMF. The Idle mode DRX cycle applies in CM-IDLE state and in CM-CONNECTED with RRC Inactive state.

If the UE wants to use UE specific DRX parameters, the UE shall include its preferred values consistently in every Initial Registration and Mobility Registration procedure separately for NR/WB-EUTRA and NB-IoT. During Initial Registration and Mobility Registration procedures performed on NB-IoT cells, the normal 5GS procedures apply. For NB-IoT, the cell broadcasts an indication of support of UE specific DRX for NB-IoT in that cell, and the UE can request UE specific DRX for NB-IoT in the Registration procedure irrespective of whether the cell broadcasts that support indication.

The AMF shall determine Accepted DRX parameters based on the received UE specific DRX parameters and the AMF should accept the UE requested values, but subject to operator policy the AMF may change the UE requested values.

The AMF shall respond to the UE with the Accepted DRX parameters separately for NR/WB-EUTRA and NB-IoT.

For details of DRX parameters, see TS 38.331 [28] and TS 36.331 [51].

The UE shall apply the DRX cycle broadcast in the cell by the RAN unless it has received Accepted DRX parameters for the RAT from the AMF and for NB-IoT the cell supports UE specific DRX for NB-IoT, in which case the UE shall apply either the DRX cycle broadcast in the cell or the Accepted DRX parameters for the RAT, as defined in TS 38.304 [50] and TS 36.304 [52].

The Periodic Registration procedure does not change the UE's DRX settings.

In CM-CONNECTED with RRC Inactive state, the UE applies either the DRX cycle negotiated with AMF, or the DRX cycle broadcast by RAN or the UE specific DRX cycle configured by RAN, as defined in TS 38.300 [27] and TS 38.304 [50].

5.4.6 Core Network assistance information for RAN optimization

5.4.6.1 General

Core Network assistance information for RAN aids the RAN to optimize the UE state transition steering and the RAN paging strategy formulation in RRC Inactive state. The Core Network assistance information includes the information set, Core Network assisted RAN parameters tuning, which assist RAN optimize the UE RRC state transition and CM state transition decision. It also includes the information set, Core Network assisted RAN paging information, which assist RAN to formulate an optimized paging strategy when RAN paging is triggered.

5.4.6.2 Core Network assisted RAN parameters tuning

Core Network assisted RAN parameters tuning aids the RAN to minimize the UE state transitions and achieve optimum network behaviour. How the RAN uses the CN assistance information is not defined in this specification.

Core Network assisted RAN parameters tuning may be derived by the AMF per UE in the AMF based on collection of UE behaviour statistics, Expected UE Behaviour and/or other available information about the UE (such as subscribed DNN, SUPI ranges, or other information). If the AMF maintains Expected UE Behaviour parameters, Network Configuration parameters (as described in clause 4.15.6.3 or 4.15.6.3a, TS 23.502 [3]) or SMF derived CN assisted RAN parameters tuning, the AMF may use this information for selecting the CN assisted RAN parameter values. If the AMF is able to derive the Mobility Pattern of the UE (as described in clause 5.3.4.2), the AMF may take the Mobility Pattern information into account when selecting the CN assisted RAN parameter values.

The SMF uses the SMF-Associated parameters (e.g. Expected UE Behaviour parameters or Network Configuration parameters of the UE) to derive the SMF derived CN assisted RAN parameters tuning. The SMF sends the SMF derived CN assisted RAN parameters tuning to the AMF during the PDU Session establishment procedure and if the SMF-Associated parameters change the PDU Session modification procedure is applied. The AMF stores the SMF derived CN assisted RAN parameters tuning in the PDU Session level context. The AMF uses the SMF derived CN assisted RAN parameters tuning to determine a PDU Session level "Expected UE activity behaviour" parameters set, which may be associated with a PDU Session ID, as described below in this clause.

The Expected UE Behaviour parameters or the Network Configuration parameters can be provisioned by external party via the NEF to the AMF or SMF, as described in clause 5.20.

The CN assisted RAN parameters tuning provides the RAN with a way to understand the UE behaviour for these aspects:

- "Expected UE activity behaviour", i.e. the expected pattern of the UE's changes between CM-CONNECTED and CM-IDLE states or the duration of CM-CONNECTED state. This may be derived e.g. from the statistical information, or Expected UE Behaviour or from subscription information. The AMF derives one or more sets of the "Expected UE activity behaviour" parameters for the UE as follows:

  - AMF may derive and provide to the RAN a UE level of "Expected UE activity behaviour" parameters set considering the Expected UE Behaviour parameters or Network Configuration parameters received from the UDM (see clauses 4.15.6.3 or 4.15.6.3a of TS 23.502 [3]) and the SMF derived CN assisted RAN parameters tuning associated with a PDU Session using Control Plane CIoT 5GS Optimisation. This set of "Expected UE activity behaviour" parameters is valid for the UE; and

  - AMF may provide to the RAN a PDU Session level "Expected UE activity behaviour" parameters set, e.g. considering the SMF derived CN assisted RAN parameters tuning, per established PDU Session. The PDU Session level "Expected UE activity behaviour" set of parameters is associated with and valid for a PDU Session ID. The RAN may consider the PDU Session level "Expected UE activity behaviour" parameters when the User Plane resources for the PDU Session are activated;

- "Expected HO behaviour", i.e. the expected interval between inter-RAN handovers. This may be derived by the AMF e.g. from the Mobility Pattern information;

- "Expected UE mobility", i.e. whether the UE is expected to be stationary or mobile. This may be derived e.g. from the statistical information or Expected UE Behaviour parameters or from subscription information;

- "Expected UE moving trajectory" which may be derived e.g. from the statistical information or Expected UE Behaviour parameters or from subscription information; or

- "UE Differentiation Information" including the Expected UE Behaviour parameters excluding the Expected UE moving trajectory (see clause 4.15.6.3 of TS 23.502 [3]) to support Uu operation optimisation for NB-IoT UE differentiation if the RAT type is NB-IoT.

The AMF decides when to send this information to the RAN as "Expected UE activity behaviour" carried in N2 request over the N2 interface (see TS 38.413 [34]).

NOTE: The calculation of the CN assistance information, i.e. the algorithms used and related criteria, and the decision when it is considered suitable and stable to send to the RAN are vendor specific.

5.4.6.3 Core Network assisted RAN paging information

Core Network assisted RAN paging information aids the RAN to formulate a RAN paging policy and strategy in RRC Inactive state, besides the PPI and QoS information associated to the QoS Flows as indicated in clause 5.4.3.

CN assisted RAN paging information may be derived by the AMF per UE and/or per PDU Session based on collection of UE behaviour statistics, Expected UE Behaviour and/or other available information about the UE (such as subscribed DNN, SUPI ranges, Multimedia priority service), and/or information received from other network functions when downlink signalling is triggered.

The CN assisted RAN paging information consists of a service priority (values 1 to 256) which provides AN with a way to understand how important the downlink signalling is. The AMF derives this service priority based on available information as described above. The method to derive the service priority is implementation depended and can be controlled by operator.

The Core Network may provide the CN assisted RAN paging information to RAN in different occasions, e.g. during downlink N1 and N2 message delivery, etc.

5.4.7 NG-RAN location reporting

NG-RAN supports the NG-RAN location reporting for the services that require accurate cell identification (e.g. emergency services, lawful intercept, charging) or for the UE mobility event notification service subscribed to the AMF by other NFs. The NG-RAN location reporting may be used by the AMF when the target UE is in CM-CONNECTED state.

The AMF may request the NG-RAN location reporting with event reporting type (e.g. UE location or UE presence in Area of Interest), reporting mode and its related parameters (e.g. number of reporting).

If the AMF requests UE location, the NG-RAN reports the current UE location (or last known UE location with time stamp if the UE is in RRC Inactive state) based on the requested reporting parameter (e.g. one-time reporting or continuous reporting).

If the AMF requests UE presence in the Area Of Interest, the NG-RAN reports the UE location and the indication (i.e. IN, OUT or UNKNOWN) when the NG-RAN determines the change of UE presence in Area Of Interest.

After N2 based Handover, if the NG-RAN location reporting information is required, the AMF shall re-request the NG-RAN location reporting to the target NG-RAN node. For Xn based Handover, the source NG-RAN shall transfer the requested NG-RAN location reporting information to target NG-RAN node.

The AMF requests the location information of the UE either through independent N2 procedure (i.e. NG-RAN location reporting as specified in clause 4.10 of TS 23.502 [3]), or by including the request in some specific N2 messages as specified in TS 38.413 [34].

5.4.8 Support for identification and restriction of using unlicensed spectrum

Support for NG-RAN using unlicensed spectrum is defined in TS 38.300 [27] and TS 36.300 [30].

For NG-RAN, in the case of NR in stand-alone mode, all cells are in unlicensed spectrum and the NR is used as primary RAT. NR or E-UTRA cells in unlicensed spectrum, can be used as secondary cells as specified in the Dual Connectivity architecture defined in clause 5.11 or in addition can be configured to support the Carrier Aggregation Architecture (CA) defined in TS 38.300 [27] and TS 36.300 [30].

For either case the serving PLMN can enforce Access Restriction for Unlicensed Spectrum (either signalled from the UDM, or, locally generated by VPLMN policy in the AMF) with the following:

- To restrict the use of NR in unlicensed spectrum as primary RAT, the AMF rejects the UE Registration procedure with appropriate cause code defined in TS 24.501 [47] if the UE performs initial access from NR using unlicensed spectrum. If the UE is accessing through some other allowed RAT, the AMF signals this access restriction to NG-RAN as part of Mobility Restriction List.

- To restrict the use of use of unlicensed spectrum with NR or E-UTRA as secondary RAT using Dual Connectivity or Carrier Aggregation Architecture (CA) defined in TS 38.300 [27] and TS 36.300 [30], the AMF signals this access restriction to NG-RAN as part of Mobility Restriction List.

An NG-RAN node supporting aggregation with unlicensed spectrum using either NR or E-UTRA checks whether the UE is allowed to use unlicensed spectrum based on received Mobility Restriction List. If the UE is not allowed to use Unlicensed Spectrum, the NG-RAN node shall restrict the using of unlicensed spectrum, either NR or E-UTRA as secondary RATs when using either Dual Connectivity or Carrier Aggregation (CA) as defined in TS 38.300 [27] and TS 36.300 [30].

At inter-RAT handover from E-UTRAN/EPS, the Access Restriction for Unlicensed Spectrum is either already in the AMF's UE context, or is obtained from the UDM during the subsequent Registration Area Update procedure (i.e. not from the source MME or source RAN). In both inter-RAT handover cases, any Access Restriction for use of Unlicensed Spectrum is then signalled to NG-RAN or enforced in AMF.

NOTE: This signalling of the Access Restriction during the Registration Area Update after the inter-RAT handover procedure means that there is a small risk that unlicensed spectrum resources are transiently allocated.

When the UE is accessing 5GS using unlicensed spectrum as primary RAT:

- The NG-RAN node shall provide an indication to the AMF in N2 interface that NR access is using unlicensed spectrum as defined in TS 38.413 [34].

- In order to restrict access to NR in unlicensed spectrum, cells supporting NR in unlicensed spectrum have to be deployed in Tracking Area(s) different to cells supporting licensed spectrum.

- When the AMF receives an indication from NG-RAN over N2 whether NR in unlicensed spectrum is being used as defined in TS 38.413 [34], the AMF provides to the SMF an indication that the RAT type is NR with usage of unlicensed spectrum during PDU Session Establishment or as part of the UP activation and Handover procedures.

- The PCF will also receive the indication whether the UE is using NR in unlicensed spectrum, when applicable, from the SMF during SM Policy Association Establishment or SM Policy Association Modification procedure.

- The NFs generating CDRs shall include the indication that the UE is using NR in unlicensed spectrum in their CDRs.

When the UE is accessing NR or E-UTRA using unlicensed spectrum as secondary RAT, procedures for Usage Data Reporting for Secondary RAT as defined in clause 5.12.2 can apply.

5.4.9 Wake Up Signal Assistance

To support the Wake Up Signal (WUS), the WUS Assistance Information is used by the NG-eNB to help determine the WUS group used when paging the UE (see TS 36.300 [30]).

The content of the WUS Assistance Information consists of the paging probability information. The paging probability information provides a metric on the probability of a UE receiving a paging message based on, e.g., statistical information.

The UE may in the Registration Request message provide its capability to support receiving WUS Assistance Information. If WUS Assistance Information is supported by the UE, then the UE in the Registration Request message may provide the additional UE paging probability information. The AMF may use the UE provided paging probability, local configuration and/or previous statistical information for the UE, when determining the WUS Assistance Information. If the UE supports WUS Assistance Information, the AMF may assign WUS Assistance Information to the UE, even when the UE has not provided the additional UE paging probability information.

If the AMF has determined WUS Assistance Information for the UE, the AMF provides it to the UE in every Registration Accept message. The AMF stores the WUS Assistance Information parameter in the MM context and provides it to the NG-eNB when paging the UE.

UE and AMF shall not signal WUS Assistance Information in Registration Request, Registration Accept messages when the UE has an active emergency PDU session.

5.5 Non-3GPP access specific aspects

5.5.0 General

This clause describe the specific aspects for untrusted non-3GPP access and trusted non-3GPP access.

5.5.1 Registration Management

This clause applies to Non-3GPP access network corresponding to the Untrusted Non-3GPP access network, to the Trusted Non-3GPP and to the W-5GAN. In the case of W-5GAN the UE mentioned in this clause corresponds to 5G-RG or to the W-AGF in the case of FN-RG. In the case of N5CW devices access 5GC via trusted WLAN access networks, the UE mentioned in this clause corresponds to TWIF.

The UE shall enter RM-DEREGISTERED state and the AMF shall enter RM-DEREGISTERED state for the UE on non-3GPP access as follows:

- at the UE and at the AMF, after performing an Explicit Deregistration procedure;

- at the AMF, after the Network non-3GPP Implicit Deregistration timer has expired.

- at the UE, after the UE non-3GPP Deregistration timer has expired.

NOTE: This is assumed to leave sufficient time to allow the UE to re-activate UP connections for the established PDU Sessions over 3GPP or non-3GPP access.

Whenever a UE registered over non-3GPP access enters CM-IDLE state for the non-3GPP access, it starts the UE non-3GPP Deregistration timer according to the value received from the AMF during a Registration procedure.

Over non-3GPP access, the AMF runs the Network non-3GPP Implicit Deregistration timer. The Network non-3GPP Implicit Deregistration timer is started with a value longer than the UE's non-3GPP Deregistration timer, whenever the CM state for the UE registered over non-3GPP access changes to CM-IDLE for the non-3GPP access.

For a UE that is registered over Non-3GPP access, a change of the point of attachment (e.g. change of WLAN AP) shall not lead the UE to perform a Registration procedure.

A UE shall not provide 3GPP-specific parameters (e.g. indicate a preference for MICO mode) during registration over a non-3GPP access.

5.5.2 Connection Management

This clause applies to Non-3GPP access network corresponding to the Untrusted Non-3GPP access network, to the Trusted Non-3GPP and to the W-5GAN. The UE mentioned in this clause corresponds to the 5G-RG in the case of W-5GAN and to the W-AGF in the case of FN-RG. In the case of N5CW devices access 5GC via trusted WLAN access networks, the UE mentioned in this clause corresponds to TWIF.

A UE that successfully establishes a Non-3GPP Access Connection to the 5GC over a Non-3GPP access transitions to CM-CONNECTED state for the Non-3GPP access.

In the case of Untrusted Non-3GPP access to 5GC, the Non-3GPP Access Connection corresponds to an NWu connection.

In the case of Trusted access to 5GC, the Non-3GPP Access Connection corresponds to an NWt connection.

In the case of N5CW devices access 5GC via trusted WLAN access networks, the Non-3GPP Access Connection corresponds to an Yt' connection.

In the case of Wireline access to 5GC, the Non-3GPP Access Connection corresponds to a Y4 connection and to Y5 connection.

A UE does not establish multiple simultaneous Non-3GPP Access Connection to the 5GC.

The Non-3GPP Access Connection is released either as a result of an Explicit Deregistration procedure or an AN Release procedure.

In the case of Untrusted Non-3GPP access, Trusted Non-3GPP access and W-5GAN access to 5GC, the N3IWF, TNGF, TWIF and W-AGF may in addition explicitly release the NWu, NWt, Yt', Y4 and Y5 signalling connection due to NWu, NWt, Yt', Y4 and Y5 connection failure, respectively. In the case of NWu and NWt, the release may be determined by the "dead peer detection" mechanism in IKEv2 defined in RFC 7296 [60]. In the case of Y4 and Y5 the release may be detected for example by lost of synchronisation of physical link, lost of PPPoE session, etc. Further details on how NWu, NWt, Yt', Y4 and Y5 connection failure is detected is out of scope of 3GPP specifications.

For W-5GCAN, the W-AGF explicitly releases the N2 connection due to Y4 or Y5 connection failure, as determined by the "dead peer detection" mechanism in DOCSIS MULPI [89].

The release of the Non-3GPP Access Connection between the UE and the N3IWF, TNGF, TWIF or W-AGF shall be interpreted as follows:

- By the N3IWF, TNGF, TWIF and W-AGF as a criterion to release the N2 connection.
- By the UE as a criterion for the UE to transition to CM-IDLE. A UE registered over non-3GPP access remains in RM-REGISTERED state, unless the Non-3GPP Access Connection release occurs as part of a Deregistration procedure over non-3GPP access in which case the UE enters the RM-DEREGISTERED state. When the UE in RM-REGISTERED transitions to CM-IDLE, the UE non-3GPP Deregistration timer starts running in the UE. The UE non-3GPP Deregistration timer stops when the UE moves to CM-CONNECTED state or to the RM-DEREGISTERED state.

NOTE 1: When moved to CM-IDLE state over one access, the UE can attempt to re-activate UP connections for the PDU Sessions over other access, per UE policies and depending on the availability of these accesses.

NOTE 2: The release of the NWu, NWt, Yt', Y4 or Y5 at the UE can occur as a result of explicit signalling from the N3IWF, TNGF, TWIF or W-AGF respectively, e.g. IKE INFORMATION EXCHANGE in the case of NWu or as a result of the UE detecting NWu, NWt, Yt', Y4 or Y5 connection failure, e.g. as determined by the "dead peer detection" mechanism in IKEv2 as defined in RFC 7296 [60] for NWu, NWt and Yt' or W-5GAN access specific mechanism for Y4 and Y5. Further details on how the UE detects NWu, NWt, Yt', Y4 or Y5 connection failure is out of scope of 3GPP specifications.

In the case of Non-3GPP access, when the AMF releases the N2 interface, the N3IWF, TNGF, TWIF and W-AGF shall release all the resources associated with the UE including the Non-3GPP Access Connection with the UE and its corresponding N3 resources. A release of the N2 connection by the AMF shall set the CM state for the UE in the AMF to CM-IDLE.

NOTE 3: It is assumed that a UE configured to receive services from a 5GC over non-3GPP access that is RM-DEREGISTERED or CM-IDLE over the non-3GPP access will attempt to establish Non-3GPP Access Connection and transition to CM-CONNECTED state whenever the UE successfully connects to a non-3GPP access unless prohibited by the network to make a N3GPP Access Connection (e.g. due to network congestion).

An UE cannot be paged on Non-3GPP access network.

When a UE registered simultaneously over a 3GPP access and a non-3GPP access moves all the PDU Sessions to one of the accesses, whether the UE initiates a Deregistration procedure in the access that has no PDU Sessions is up to the UE implementation.

Release of PDU Sessions over the non-3GPP access does not imply the release of N2 connection.

When the UE has PDU Sessions routed over the non-3GPP access and the UE state becomes CM-IDLE for the non-3GPP access, these PDU Sessions are not released to enable the UE to move the PDU Sessions over the 3GPP access based on UE policies. The core network maintains the PDU Sessions but deactivates the N3 user plane connection for such PDU Sessions.

5.5.3 UE Reachability

5.5.3.1 UE reachability in CM-IDLE

This clause applies to Non-3GPP access network corresponding to the Untrusted Non-3GPP access network, to the Trusted Non-3GPP and to the W-5GAN. The UE mentioned in this clause corresponds to 5G-RG, in the case of W-5GAN or to W-AGF in the case of support of FN-RG. In the case of N5CW devices access 5GC via trusted WLAN access networks, the UE mentioned in this clause corresponds to TWIF.

An UE cannot be paged over Non-3GPP access network.

If the UE states in the AMF are CM-IDLE and RM-REGISTERED for the non-3GPP access, there may be PDU Sessions that were last routed over the non-3GPP access and without user plane resources. If the AMF receives a message with a Non-3GPP Access Type indication from an SMF for a PDU Session corresponding to a UE that is CM-IDLE for non-3GPP access, and the UE is registered over 3GPP access in the same PLMN as the one registered over non-3GPP access, a Network Triggered Service Request may be performed over the 3GPP access independently of whether the UE is CM-IDLE or CM-CONNECTED over the 3GPP access. In this case, the AMF provides an indication that the procedure is related to non-3GPP access, as specified in clause 5.6.8.

NOTE: The UE behaviour upon such network triggered Service Request is specified in clause 5.6.8.

5.5.3.2 UE reachability in CM-CONNECTED

This clause applies to Non-3GPP access network corresponding to the Untrusted Non-3GPP access network, to the Trusted Non-3GPP and to the W-5GAN. In the case of W-5GAN the UE mentioned in this clause corresponds to 5G-RG and to W-AGF in the case of support of FN-RG. In the case of N5CW devices access 5GC via trusted WLAN access networks, the UE mentioned in this clause corresponds to TWIF.

For a UE in CM-CONNECTED state:

- the AMF knows the UE location on a N3IWF, TNGF, TWIF and W-AGF node granularity.

- the N3IWF, TNGF, TWIF and W-AGF releases the N2 connection when UE becomes unreachable from N3IWF, TNGF, TWIF and W-AGF point of view, i.e. upon Non-3GPP Access Connection release.

5.6 Session Management

5.6.1 Overview

The 5GC supports a PDU Connectivity Service i.e. a service that provides exchange of PDUs between a UE and a data network identified by a DNN. The PDU Connectivity Service is supported via PDU Sessions that are established upon request from the UE.

The Subscription Information for each S-NSSAI may contain a Subscribed DNN list and one default DNN. When the UE does not provide a DNN in a NAS Message containing PDU Session Establishment Request for a given S-NSSAI, the serving AMF determines the DNN for the requested PDU Session by selecting the default DNN for this S-NSSAI if a default DNN is present in the UE's Subscription Information; otherwise the serving AMF selects a locally configured DNN for this S-NSSAI.

The expectation is that the URSP in the UE is always up to date using the procedure defined in TS 23.502 [3] clause 4.16.12.2 and therefore the UE requested DNN will be up to date.

In order to cover cases that UE operates using local configuration, but also other cases where operator policies can be used in order to replace an "up to date" UE requested DNN with another DNN used only internally in the network, during UE Registration procedure the PCF may indicate, to the AMF, the operator policies to be used at PDU Session Establishment for DNN replacement of a UE requested DNN. PCF may indicate a policy for DNN replacement of UE requested DNNs not supported by the network, and/or indicate a list of UE requested DNNs per S-NSSAI valid for the serving network, that are subject for replacement (details are described in TS 23.503 [45]).

If the DNN provided by the UE is not supported by the network and AMF cannot select an SMF by querying NRF, the AMF shall reject the NAS Message containing PDU Session Establishment Request from the UE with a cause indicating that the DNN is not supported unless the PCF provided the policy to perform a DNN replacement of unsupported DNNs.

If the DNN requested by the UE is indicated for replacement or the DNN provided by the UE is not supported by the network and the PCF provided the policy to perform DNN replacement of UE requested DNNs not supported by the network, the AMF shall interact with the PCF to perform a DNN replacement. During PDU Session Establishment procedure and as a result of DNN replacement, the PCF provides the selected DNN that is applicable for the S-NSSAI requested by the UE at the PDU Session Establishment. The AMF uses the selected DNN in the query towards the NRF for the SMF selection, as specified in clause 6.3.2, and provides both requested and selected DNN to the selected SMF. For PDU Session with Home-routed Roaming whether to perform DNN replacement is based on operator agreements.

NOTE 1: The selected DNN is determined based on operator preferences and can differ from subscribed DNNs. The matching of selected DNN to S-NSSAI is assumed to be based on network configuration.

Each PDU Session supports a single PDU Session type i.e. supports the exchange of a single type of PDU requested by the UE at the establishment of the PDU Session. The following PDU Session types are defined: IPv4, IPv6, IPv4v6, Ethernet, Unstructured.

PDU Sessions are established (upon UE request), modified (upon UE and 5GC request) and released (upon UE and 5GC request) using NAS SM signalling exchanged over N1 between the UE and the SMF. Upon request from an Application Server, the 5GC is able to trigger a specific application in the UE. When receiving that trigger message, the UE shall pass it to the identified application in the UE. The identified application in the UE may establish a PDU Session to a specific DNN, see clause 4.4.5.

SMF may support PDU Sessions for LADN where the access to a DN is only available in a specific LADN service area. This is further defined in clause 5.6.5.

SMF may support PDU Sessions for a 5G VN group which offers a virtual data network capable of supporting 5G LAN-type service over the 5G system. This is further defined in clause 5.8.2.13.

The SMF is responsible of checking whether the UE requests are compliant with the user subscription. For this purpose, it retrieves and requests to receive update notifications on SMF level subscription data from the UDM. Such data may indicate per DNN and per S-NSSAI of the HPLMN:

- The allowed PDU Session Types and the default PDU Session Type.
- The allowed SSC modes and the default SSC mode.
- QoS Information (refer to clause 5.7): the subscribed Session-AMBR, Default 5QI and Default ARP.
- The static IP address/prefix.
- The subscribed User Plane Security Policy.
- the Charging Characteristics to be associated with the PDU Session. Whether this information is provided by the UDM to a SMF in another PLMN (for PDU Sessions in LBO mode) is defined by operator policies in the UDM/UDR.

NOTE 2: The content of the Charging Characteristics as well as the usage of the Charging Characteristics by the SMF are defined in TS 32.240 [41].

A PDU Session may support:

(a) a single-access PDU Connectivity Service, in which case the PDU Session is associated with a single access type at a given time, i.e. either 3GPP access or non-3GPP access; or

(b) a multi-access PDU Connectivity Service, in which case the PDU Session is simultaneously associated with both 3GPP access and non-3GPP access and simultaneously associated with two independent N3/N9 tunnels between the PSA and RAN/AN.

A PDU Session supporting a single-access PDU Connectivity Service is also referred to as single-access PDU Session, while a PDU Session supporting a multi-access PDU Connectivity Service is referred to as Multi-Access PDU (MA PDU) Session and it is used to support the ATSSS feature (see clause 5.32 for details).

A UE that is registered over multiple accesses chooses over which access to establish a PDU Session. As defined in TS 23.503 [45], the HPLMN may send policies to the UE to guide the UE selection of the access over which to establish a PDU Session.

NOTE 3: In this Release of the specification, at any given time, a PDU Session is routed over only a single access network, unless it is an MA PDU Session in which case it can be routed over one 3GPP access network and one Non 3GPP access network concurrently.

A UE may request to move a single-access PDU Session between 3GPP and Non 3GPP accesses. The decision to move single-access PDU Sessions between 3GPP access and Non 3GPP access is made on a per PDU Session basis, i.e. the UE may, at a given time, have some PDU Sessions using 3GPP access while other PDU Sessions are using Non 3GPP access.

In a PDU Session Establishment Request message sent to the network, the UE shall provide a PDU Session ID. The PDU Session ID is unique per UE and is the identifier used to uniquely identify one of a UE's PDU Sessions. The PDU Session ID shall be stored in the UDM to support handover between 3GPP and non-3GPP access when different PLMNs are used for the two accesses. The UE also provides as described in TS 24.501 [47]:

(a) PDU Session Type.

(b) S-NSSAI of the HPLMN that matches the application (that is triggering the PDU Session Request) within the NSSP in the URSP rules or within the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45].

NOTE 4: If the UE cannot determine any S-NSSAI after performing the association of the application to a PDU Session, then it does not indicate any S-NSSAI in the PDU Session Establishment procedure as defined in clause 5.15.5.3.

(c) S-NSSAI of the Serving PLMN from the Allowed NSSAI, corresponding to the S-NSSAI of the HPLMN (b).

NOTE 5: Generally, in non-roaming scenario the mapping of the Allowed NSSAI to HPLMN S-NSSAIs is not provided to the UE (because the S-NSSAI of the Serving PLMN (c) has the same value of the S-NSSAI of the HPLMN (b)), therefore the UE provides in the PDU Session Request only the S-NSSAI of the Serving PLMN (c). However, if the UE is provided with the mapping of the Allowed NSSAI to HPLMN S-NSSAIs even in non-roaming scenario, then the UE provides in the PDU Session Request both the S-NSSAI of the HPLMN (b) and the S-NSSAI from the Allowed NSSAI (c) that maps to the S-NSSAI of the HPLMN.

NOTE 6: In roaming scenarios the UE provides in the PDU Session Request both the S-NSSAI of the HPLMN (b) and the S-NSSAI of the VPLMN from the Allowed NSSAI (c) that maps to the S-NSSAI of the HPLMN.

(d) DNN (Data Network Name).

(e) SSC mode (Service and Session Continuity mode defined in clause 5.6.9.2).

Additionally, if the UE supports ATSSS and wants to activate a MA PDU Session, the UE shall provide Request Type as "MA PDU Request" and shall indicate the supported ATSSS capabilities (see clause 5.32 for details).

Table 5.6.1-1: Attributes of a PDU Session

PDU Session attribute	May be modified later during the lifetime of the PDU Session	Notes
S-NSSAI of the HPLMN	No	(Note 1) (Note 2)
S-NSSAI of the Serving PLMN	Yes	(Note 1) (Note 2) (Note 4)
DNN (Data Network Name)	No	(Note 1) (Note 2)
PDU Session Type	No	(Note 1)
SSC mode	No	(Note 2) The semantics of Service and Session Continuity mode is defined in clause 5.6.9.2
PDU Session Id	No	
User Plane Security Enforcement information	No	(Note 3)
Multi-access PDU Connectivity Service	No	Indicates if the PDU Session provides multi-access PDU Connectivity Service or not.
NOTE 1: If it is not provided by the UE, the network determines the parameter based on default information received in user subscription. Subscription to different DNN(s) and S-NSSAI(s) may correspond to different default SSC modes and different default PDU Session Types NOTE 2: S-NSSAI(s) and DNN are used by AMF to select the SMF(s) to handle a new session. Refer to clause 6.3.2. NOTE 3: User Plane Security Enforcement information is defined in clause 5.10.3. NOTE 4: The S-NSSAI value of the Serving PLMN associated to a PDU Session can change whenever the UE moves to a different PLMN, while keeping that PDU Session.		

Subscription Information may include a wildcard DNN per subscribed S-NSSAI: when a wildcard DNN is associated with a subscribed S-NSSAI, the subscription allows, for this S-NSSAI, the UE to establish a PDU Session using any DNN value.

NOTE 7: The SMF is made aware whether the DNN of a PDU Session being established corresponds to an explicitly subscribed DNN or corresponds to a wildcard DNN. Thus, the SMF can reject a PDU Session establishment if the DNN of the PDU Session is not part of explicitly subscribed DNN(s) and local policies in the SMF require UE to have a subscription to this DNN.

A UE may establish multiple PDU Sessions, to the same data network or to different data networks, via 3GPP and via and Non-3GPP access networks at the same time.

A UE may establish multiple PDU Sessions to the same Data Network and served by different UPF terminating N6.

A UE with multiple established PDU Sessions may be served by different SMF.

The SMF shall be registered and deregistered on a per PDU Session granularity in the UDM.

The user plane paths of different PDU Sessions (to the same or to different DNN) belonging to the same UE may be completely disjoint between the AN and the UPF interfacing with the DN.

When the SMF cannot control the UPF terminating the N3 interface used by a PDU Session and SSC mode 2/3 procedures are not applied to the PDU Session, an I-SMF is inserted between the SMF and the AMF and handling of PDU Session(s) is described in clause 5.34.

NOTE 8: User Plane resources for PDU Sessions of a UE, except for regulatory prioritized service like Emergency Services and MPS, can be deactivated by the SMF if the UE is only reachable for regulatory prioritized services.

The SMF serving a PDU session (i.e. Anchor) does not change during lifetime of the PDU session.

5.6.2 Interaction between AMF and SMF

The AMF and SMF are separate Network Functions.

N1 related interaction with SMF is as follows:

- The single N1 termination point is located in AMF. The AMF forwards SM related NAS information to the SMF based on the PDU Session ID in the NAS message. Further SM NAS exchanges (e.g. SM NAS message responses) for N1 NAS signalling received by the AMF over an access (e.g. 3GPP access or non-3GPP access) are transported over the same access.

- The serving PLMN ensures that subsequent SM NAS exchanges (e.g. SM NAS message responses) for N1 NAS signalling received by the AMF over an access (e.g. 3GPP access or non-3GPP access) are transported over the same access.

- SMF handles the Session management part of NAS signalling exchanged with the UE.

- The UE shall only initiate PDU Session Establishment in RM-REGISTERED state.

- When a SMF has been selected to serve a specific PDU Session, AMF has to ensure that all NAS signalling related with this PDU Session is handled by the same SMF instance.

- Upon successful PDU Session Establishment, the AMF and SMF stores the Access Type that the PDU Session is associated.

N11 related interaction with SMF is as follows:

- The AMF reports the reachability of the UE based on a subscription from the SMF, including:

  - The UE location information with respect to the area of interest indicated by the SMF.

- The SMF indicates to AMF when a PDU Session has been released.

- Upon successful PDU Session Establishment, AMF stores the identification of serving SMF of UE and SMF stores the identification of serving AMF of UE including the AMF set. When trying to reach the AMF serving the UE, the SMF may need to apply the behaviour described for "the other CP NFs" in clause 5.21.

N2 related interaction with SMF is as follows:

- Some N2 signalling (such as handover related signalling) may require the action of both AMF and SMF. In such case, the AMF is responsible to ensure the coordination between AMF and SMF. The AMF may forward the SM N2 signalling towards the corresponding SMF based on the PDU Session ID in N2 signalling.

- SMF shall provide PDU Session Type together with PDU Session ID to NG-RAN, in order to facilitate NG-RAN to apply suitable header compression mechanism to packet of different PDU type. Details refer to TS 38.413 [34].

N3 related interaction with SMF is as follows:

- Selective activation and deactivation of UP connection of existing PDU Session is defined in clause 5.6.8.

N4 related interaction with SMF is as follows:

- When it is made aware by the UPF that some DL data has arrived for a UE without downlink N3 tunnel information, the SMF interacts with the AMF to initiate Network Triggered Service Request procedure. In this case, if the SMF is aware that the UE is unreachable or if the UE is reachable only for regulatory prioritized service and the PDU Session is not for regulatory prioritized service, then the SMF shall not inform DL data notification to the AMF

The AMF is responsible of selecting the SMF per procedures described in clause 6.3.2. For this purpose, it gets subscription data from the UDM that are defined in that clause. Furthermore, it retrieves the subscribed UE-AMBR from the UDM, and optionally dynamic serving network UE-AMBR from PCF based on operator local policy, and sends to the (R)AN as defined in clause 5.7.2

AMF-SMF interactions to support LADN are defined in clause 5.6.5.

In order to support charging data collection and to fulfil regulatory requirement (in order to provide NPLI - Network Provided Location Information- as defined in TS 23.228 [15]) related with the set-up, modification and release of IMS Voice calls or with SMS transfer the following applies

- At the time of the PDU Session Establishment, the AMF provides the SMF with the PEI of the UE if the PEI is available at the AMF.

- When it forwards UL NAS or N2 signalling to a peer NF (e.g. to SMF or to SMSF) or during the UP connection activation of a PDU Session, the AMF provides any User Location Information it has received from the 5G-AN as well as the Access Type (3GPP - Non 3GPP) of the AN over which it has received the UL NAS or N2 signalling. The AMF also provides the corresponding UE Time Zone. In addition, in order to fulfil regulatory requirement (i.e. providing Network Provided Location Information (NPLI), as defined in TS 23.228 [15]) when the access is non-3GPP, the AMF may also provide the last known 3GPP access User Location Information with its age, if the UE is still attached to the same AMF for 3GPP access (i.e. valid User Location Information).

The User Location Information, the access type and the UE Time Zone may be further provided by SMF to PCF. The PCF may get this information from the SMF in order to provide NPLI to applications (such as IMS) that have requested it.

The User Location Information may correspond to:

- In the case of 3GPP access: Cell-Id. The AMF includes only the Primary Cell-Id even if it had received also the Cell-Id of the Primary cell in the Secondary RAN node from NG-RAN.

- In the case of Untrusted non-3GPP access: a UE local IP address (used to reach the N3IWF) and optionally UDP or TCP source port number (if NAT is detected).

- In the case of Trusted non-3GPP access: TNAP/TWAP Identifier, a UE/N5CW device local IP address (used to reach the TNGF/TWIF) and optionally UDP or TCP source port number (if NAT is detected).

  When the UE uses WLAN based on IEEE 802.11 technology to reach the TNGF, the TNAP Identifier shall include the SSID of the access point to which the UE is attached. The TNAP Identifier shall include at least one of the following elements, unless otherwise determined by the TWAN operator's policies:

  - the BSSID (see IEEE Std 802.11-2012 [106]);

  - civic address information of the TNAP to which the UE is attached.

  The TWAP Identifier shall include the SSID of the access point to which the NC5W is attached. The TWAP Identifier shall also include at least one of the following elements, unless otherwise determined by the TWAN operator's policies:

  - the BSSID (see IEEE Std 802.11-2012 [106]);

  - civic address information of the TWAP to which the UE is attached.

NOTE 1: The SSID can be the same for several TNAPs/TWAPs and SSID only cannot provide a location, but it might be sufficient for charging purposes.

NOTE 2: the BSSID associated with a TNAP/TWAP is assumed to be static.

- In the case of W-5GAN access: The User Location Information for W-5GAN is defined in TS 23.316 [84].

When the SMF receives a request to provide Access Network Information reporting while there is no action to carry out towards the 5G-AN or the UE (e.g. no QoS flow to create / Update / modify), the SMF may request User Location Information from the AMF.

The interaction between AMF and SMF(s) for the case of a I-SMF insertion, relocation or removal for a PDU session is described in clause 5.34.

5.6.3 Roaming

In the case of roaming the 5GC supports following possible deployments scenarios for a PDU Session:

- "Local Break Out" (LBO) where the SMF and all UPF(s) involved by the PDU Session are under control of the VPLMN.
- "Home Routed" (HR) where the PDU Session is supported by a SMF function under control of the HPLMN, by a SMF function under control of the VPLMN, by at least one UPF under control of the HPLMN and by at least one UPF under control of the VPLMN. In this case the SMF in HPLMN selects the UPF(s) in the HPLMN and the SMF in VPLMN selects the UPF(s) in the VPLMN. This is further described in clause 6.3.

NOTE 1: The use of an UPF in the VPLMN e.g. enables VPLMN charging, VPLMN LI and minimizes the impact on the HPLMN of the UE mobility within the VPLMN (e.g. for scenarios where SSC mode 1 applies).

Different simultaneous PDU Sessions of an UE may use different modes: Home Routed and LBO. The HPLMN can control via subscription data per DNN and per S-NSSAI whether a PDU Session is to be set-up in HR or in LBO mode.

In the case of PDU Sessions per Home Routed deployment:

- NAS SM terminates in the SMF in VPLMN.
- The SMF in VPLMN forwards to the SMF in the HPLMN SM related information.
- The SMF in the HPLMN receives the SUPI of the UE from the SMF in the VPLMN during the PDU Session Establishment procedure.
- The SMF in HPLMN is responsible to check the UE request with regard to the user subscription and to possibly reject the UE request in the case of mismatch. The SMF in HPLMN obtains subscription data directly from the UDM.
- The SMF in HPLMN may send QoS requirements associated with a PDU Session to the SMF in VPLMN. This may happen during the PDU Session Establishment procedure and after the PDU Session is established. The interface between SMF in HPLMN and SMF in VPLMN is also able to carry (N9) User Plane forwarding information exchanged between SMF in HPLMN and SMF in VPLMN. The SMF in the VPLMN may check QoS requests from the SMF in HPLMN with respect to roaming agreements.

In home routed roaming case, the AMF selects an SMF in the VPLMN and a SMF in the HPLMN as described in clause 6.3.2 and TS 23.502 [3] clause 4.3.2.2.3.3, and provides the identifier of the selected SMF in the HPLMN to the selected SMF in the VPLMN.

In roaming with LBO, the AMF selects a SMF in the VPLMN as described in clause 6.3.2 and TS 23.502 [3] clause 4.3.2.2.3.2. In this case, when handling a PDU Session Establishment Request message, the SMF in the VPLMN may reject the N11 message (related with the PDU Session Establishment Request message) with a proper N11 cause. This triggers the AMF to select both a new SMF in the VPLMN and a SMF in the HPLMN in order to handle the PDU Session using home routed roaming.

5.6.4 Single PDU Session with multiple PDU Session Anchors

5.6.4.1 General

In order to support selective traffic routing to the DN or to support SSC mode 3 as defined in clause 5.6.9.2.3, the SMF may control the data path of a PDU Session so that the PDU Session may simultaneously correspond to multiple N6 interfaces. The UPF that terminates each of these interfaces is said to support PDU Session Anchor functionality. Each PDU Session Anchor supporting a PDU Session provides a different access to the same DN. Further, the PDU Session Anchor assigned at PDU Session Establishment is associated with the SSC mode of the PDU Session and the additional PDU Session Anchor(s) assigned within the same PDU Session e.g. for selective traffic routing to the DN are independent of the SSC mode of the PDU Session. When a PCC rule including the AF influenced Traffic Steering Enforcement Control information defined in clause 6.3.1 of TS 23.503 [45] is provided to the SMF, the SMF can decide whether to apply traffic routing (by using UL Classifier functionality or IPv6 multi-homing) based on DNAI(s) included in the PCC rule.

NOTE 1: AF influenced Traffic Steering Enforcement Control information can be either determined by the PCF when requested by AF via NEF as described in clause 5.6.7.1 or statically pre-configured in the PCF.

NOTE 2: Selective traffic routing to the DN supports, for example, deployments where some selected traffic is forwarded on an N6 interface to the DN that is "close" to the AN serving the UE.

This may correspond to

- The Usage of UL Classifier functionality for a PDU Session defined in clause 5.6.4.2.
- The Usage of an IPv6 multi-homing for a PDU Session defined in clause 5.6.4.3.

5.6.4.2 Usage of an UL Classifier for a PDU Session

In the case of PDU Sessions of type IPv4 or IPv6 or IPv4v6 or Ethernet, the SMF may decide to insert in the data path of a PDU Session an "UL CL" (Uplink classifier). The UL CL is a functionality supported by an UPF that aims at diverting (locally) some traffic matching traffic filters provided by the SMF. The insertion and removal of an UL CL is decided by the SMF and controlled by the SMF using generic N4 and UPF capabilities. The SMF may decide to insert in the data path of a PDU Session a UPF supporting the UL CL functionality during or after the PDU Session Establishment, or to remove from the data path of a PDU Session a UPF supporting the UL CL functionality after the PDU Session Establishment. The SMF may include more than one UPF supporting the UL CL functionality in the data path of a PDU Session.

The UE is unaware of the traffic diversion by the UL CL, and does not involve in both the insertion and the removal of UL CL. In the case of a PDU Session of IPv4 or IPv6 or IPv4v6 type, the UE associates the PDU Session with either a single IPv4 address or a single IPv6 Prefix or both of them allocated by the network.

When an UL CL functionality has been inserted in the data path of a PDU Session, there are multiple PDU Session Anchors for this PDU Session. These PDU Session Anchors provide different access to the same DN. In the case of a PDU Session of IPv4 or IPv6 or IPv4v6 type, only one IPv4 address and/or IPv6 prefix is provided to the UE. The SMF may be configured with local policies for some (DNN, S-NSSAI) combinations to release the PDU Session when there is a PSA associated with the IPv4 address allocated to the UE and this PSA has been removed.

NOTE 0: The use of only one IPv4 address and/or IPv6 prefix with multiple PDU Session Anchors assumes that when needed, appropriate mechanisms are in place to correctly forward packets on the N6 reference point. The mechanisms for packet forwarding on the N6 reference point between the PDU Session Anchor providing local access and the DN are outside the scope of this specification.

The UL CL provides forwarding of UL traffic towards different PDU Session Anchors and merge of DL traffic to the UE i.e. merging the traffic from the different PDU Session Anchors on the link towards the UE. This is based on traffic detection and traffic forwarding rules provided by the SMF.

The UL CL applies filtering rules (e.g. to examine the destination IP address/Prefix of UL IP packets sent by the UE) and determines how the packet should be routed. The UPF supporting an UL CL may also be controlled by the SMF to support traffic measurement for charging, traffic replication for LI and bit rate enforcement (Session-AMBR per PDU Session).

NOTE 1: When N9 forwarding tunnel exists between source ULCL and target ULCL, the Session-AMBR per PDU Session can be enforced by the source UL CL UPF.

NOTE 2: The UPF supporting an UL CL may also support a PDU Session Anchor for connectivity to the local access to the data network (including e.g. support of tunnelling or NAT on N6). This is controlled by the SMF.

Additional UL CLs (and thus additional PDU Session Anchors) can be inserted in the data path of a PDU Session to create new data paths for the same PDU Session. The way to organize the data path of all UL CLs in a PDU Session is up to operator configuration and SMF logic and there is only one UPF supporting UL CL connecting to the (R)AN via N3 interface, except when session continuity upon UL CL relocation is used.

The insertion of an ULCL in the data path of a PDU Session is depicted in Figure 5.6.4.2-1.

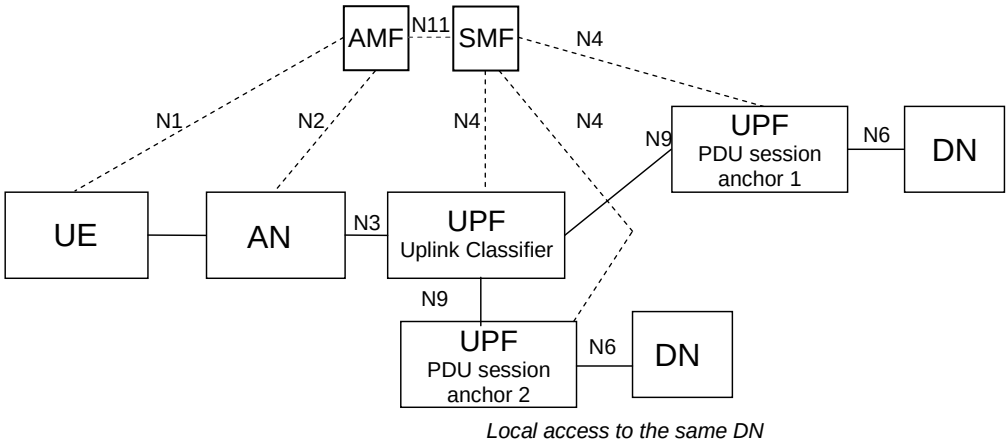


Figure 5.6.4.2-1: User plane Architecture for the Uplink Classifier

NOTE 3: It is possible for a given UPF to support both the UL CL and the PDU Session Anchor functionalities.

Due to UE mobility the network may need to relocate the UPF acting as UL CL and establish a new PSA for access to the local DN. To support session continuity during UL CL relocation the network may establish a temporary N9 forwarding tunnel between the source UL CL and target UL CL.

The N9 forwarding tunnel is maintained until all active traffic flowing on it ceases to exist for a configurable period of time or until the AF informs the SMF that it can release the source PSA providing access to the source local DN.

During the existence of the N9 forwarding tunnel the UPF acting as target UL CL is configured with packet filters that:

- force uplink traffic from existing data sessions between UE and the application in the source local DN into the N9 forwarding tunnel towards the source UL CL.

- force any traffic related to the application in the target local DN to go to the new local DN via the target PSA.

SMF may send a Late Notification to AF to inform it about the DNAI change as described in TS 23.502 [3] clause 4.3.6.3. This notification can be used by the AF e.g. to trigger mechanisms in the source local DN to redirect the ongoing traffic sessions towards an application in the target local DN. SMF can also send late notification to the target AF instance if associated with this target local DN.

The procedure for session continuity upon UL CL relocation is described in TS 23.502 [3] clause 4.3.5.7.

When an I-SMF is inserted for a PDU Session, the details of UL CL insertion which is controlled by an I-SMF is described in clause 5.34.4.

5.6.4.3 Usage of IPv6 multi-homing for a PDU Session

A PDU Session may be associated with multiple IPv6 prefixes. This is referred to as multi-homed PDU Session. The multi-homed PDU Session provides access to the Data Network via more than one PDU Session Anchor. The different user plane paths leading to the different PDU Session Anchors branch out at a "common" UPF referred to as a UPF supporting "Branching Point" functionality. The Branching Point provides forwarding of UL traffic towards the different PDU Session Anchors and merge of DL traffic to the UE i.e. merging the traffic from the different PDU Session Anchors on the link towards the UE.

The UPF supporting a Branching Point functionality may also be controlled by the SMF to support traffic measurement for charging, traffic replication for LI and bit rate enforcement (Session-AMBR per PDU Session). The insertion and removal of a UPF supporting Branching Point is decided by the SMF and controlled by the SMF using generic N4 and UPF capabilities. The SMF may decide to insert in the data path of a PDU Session a UPF supporting the Branching Point functionality during or after the PDU Session Establishment, or to remove from the data path of a PDU Session a UPF supporting the Branching Point functionality after the PDU Session Establishment.

Multi homing of a PDU Session applies only for PDU Sessions of IPv6 type. When the UE requests a PDU Session of type "IPv4v6" or "IPv6" the UE also provides an indication to the network whether it supports a Multi-homed IPv6 PDU Session.

The use of multiple IPv6 prefixes in a PDU Session is characterised by the following:

- The UPF supporting a Branching Point functionality is configured by the SMF to spread UL traffic between the PDU Session Anchors based on the Source Prefix of the PDU (which may be selected by the UE based on routing information and preferences received from the network).

- IETF RFC 4191 [8] is used to configure routing information and preferences into the UE to influence the selection of the source Prefix.

NOTE 1: This corresponds to Scenario 1 defined in IETF RFC 7157 [7] "IPv6 Multi-homing without Network Address Translation". This allows to make the Branching Point unaware of the routing tables in the Data Network and to keep the first hop router function in the PDU Session Anchors.

- The multi-homed PDU Session may be used to support make-before-break service continuity to support SSC mode 3. This is illustrated in Figure 5.6.4.3-1.

- The multi-homed PDU Session may also be used to support cases where UE needs to access both a local service (e.g. local server) and a central service (e.g. the internet), illustrated in Figure 5.6.4.3-2.

- The UE shall use the method specified in TS 23.502 [3], clause 4.3.5.3, to determine if a multi-homed PDU Session is used to support the service continuity case shown in Figure 5.6.4.3-1, or if it is used to support the local access to DN case shown in Figure 5.6.4.3-2.

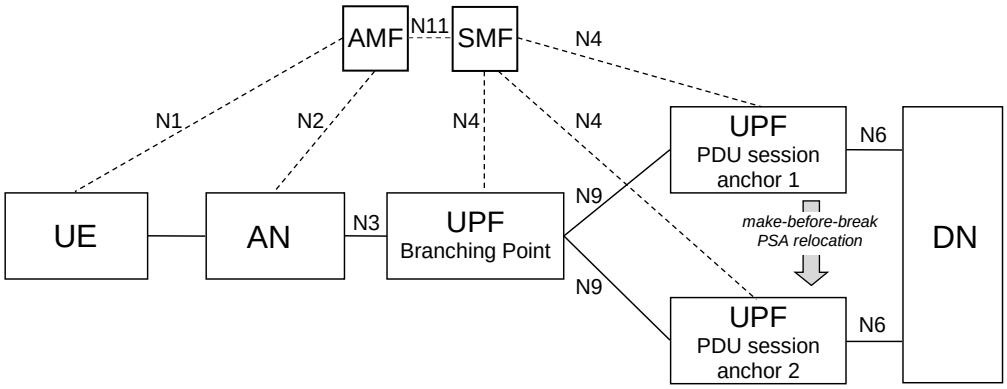


Figure 5.6.4.3-1: Multi-homed PDU Session: service continuity case

NOTE 2: It is possible for a given UPF to support both the Branching Point and the PDU Session Anchor functionalities.

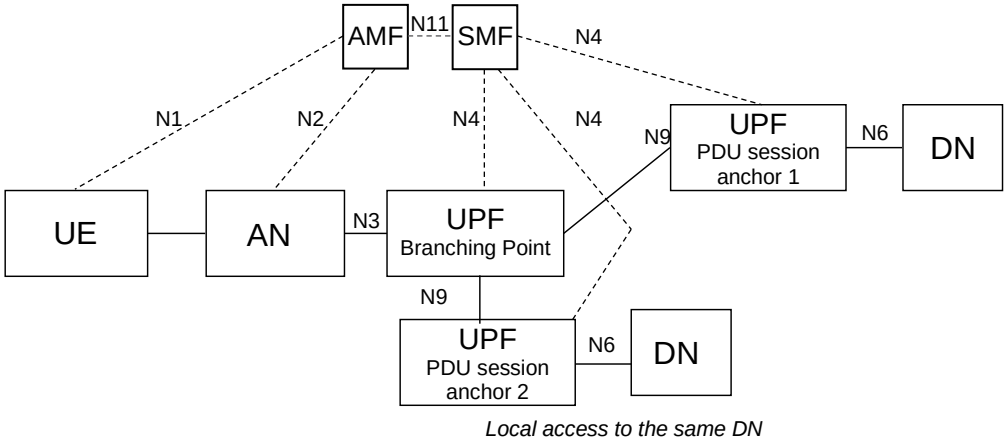


Figure 5.6.4.3-2: Multi-homed PDU Session: local access to same DN

NOTE 3: It is possible for a given UPF to support both the Branching Point and the PDU Session Anchor functionalities.

5.6.5 Support for Local Area Data Network

The access to a DN via a PDU Session for a LADN is only available in a specific LADN service area. A LADN service area is a set of Tracking Areas. LADN is a service provided by the serving PLMN. It includes:

- LADN service applies only to 3GPP accesses and does not apply in Home Routed case.
- The usage of LADN DNN requires an explicit subscription to this DNN or subscription to a wildcard DNN.
- Whether a DNN corresponds to a LADN service is an attribute of a DNN and is per PLMN.

The UE is configured to know whether a DNN is a LADN DNN on a per-PLMN basis, and an association between application and LADN DNN. The configured association is considered to be a UE local configuration defined in TS 23.503 [45]. Alternatively, the UE gets the information whether a DNN is a LADN DNN from LADN Information during (re-)registration procedure as described in this clause.

NOTE 1: No other procedure for configuring the UE to know whether a DNN is a LADN DNN is defined in this release of the specifications.

NOTE 2: The procedure for configuring the UE to know an association between application and LADN DNN is not defined in this release of the specifications.

LADN service area and LADN DNN are configured in the AMF on a per DN basis, i.e. for different UEs accessing the same LADN, the configured LADN service area is the same regardless of other factors (e.g. UE's Registration Area or UE subscription).

NOTE 3: If a LADN is not available in any TA of an AMF's service area, the AMF is not required to be configured with any LADN related information for that DNN.

LADN Information (i.e. LADN Service Area Information and LADN DNN) is provided by AMF to the UE during the Registration procedure or UE Configuration Update procedure. For each LADN DNN configured in the AMF, the corresponding LADN Service Area Information includes a set of Tracking Areas that belong to the Registration Area that the AMF assigns to the UE (i.e. the intersection of the LADN service area and the assigned Registration Area). The AMF shall not create Registration Area based on the availability of LADNs.

NOTE 4: It is thus possible that the LADN Service Area Information sent by the AMF to the UE contains only a sub-set of the full LADN service area as the LADN service area can contain TA(s) outside of the registration area of the UE or outside of the area served by the AMF.

When the UE performs a successful (re-)registration procedure, the AMF may provide to the UE, based on local configuration (e.g. via OAM) about LADN, on UE location, and on UE subscription information received from the UDM about subscribed DNN(s), the LADN Information for the list of LADN available to the UE in that Registration Area in the Registration Accept message.

The UE may provide either the LADN DNN(s) to retrieve the LADN Information for the indicated LADN DNN(s) or an indication of Requesting LADN Information to retrieve the LADN Information for all LADN(s) available in the current Registration Area.

The list of LADN is determined as follows:

- If neither LADN DNN nor an indication of requesting LADN Information is provided in the Registration Request message, the list of LADN is the LADN DNN(s) in subscribed DNN list except for wildcard DNN.
- If the UE provides LADN DNN(s) in the Registration Request message, the list of LADN is LADN DNN(s) the UE requested if the UE subscribed DNN(s) includes the requested LADN DNN or if a wildcard DNN is included in the UE's subscription data.

NOTE 5: It is assumed that an application can use only one LADN DNN at a time.

- If the UE provides an indication of requesting LADN Information in the Registration Request message, the list of LADN is all the LADN DNN(s) configured in the AMF if the wildcard DNN is subscribed, or the LADN DNN(s) which is in subscribed DNN list and no wildcard DNN is subscribed.

The UE considers the retrieved LADN Information valid only for the registered PLMN and the E-PLMN(s) if the LADN Service Area Information includes Tracking Areas that belong to E-PLMN(s). Additionally, an LADN DNN

discovered by the UE via the retrieved LADN Information is considered an LADN DNN also in the E-PLMNs of the Registered PLMN, i.e. the UE can request LADN Information for the discovered LADN DNN in the E-PLMNs.

During the subsequent Registration procedure, if the network does not provide LADN Information for a DNN, the UE deletes any LADN Information for that DNN.

When the LADN Information for the UE in the 5GC is changed, the AMF shall update LADN Information to the UE through UE Configuration Update/Registration procedure as described in clause 4.2.4/4.2.2.2.2 in TS 23.502 [3].

When receiving PDU Session Establishment with LADN DNN or Service Request for the established PDU Session corresponding to LADN, the AMF determines UE presence in LADN service area and forwards it to the SMF if the requested DNN is configured at the AMF as a LADN DNN.

Based on the LADN Service Area Information in the UE, the UE determines whether it is in or out of a LADN service area. If the UE does not have the LADN Service Area Information for a LADN DNN, the UE shall consider it is out of the LADN service area.

The UE takes actions as follows:

a) When the UE is out of a LADN service area, the UE:

   - shall not request to activate UP connection of a PDU Session for this LADN DNN;

   - shall not establish/modify a PDU Session for this LADN DNN (except for PS Data Off status change reporting for an established PDU Session);

   - need not release any existing PDU Session for this LADN DNN unless UE receives explicit SM PDU Session Release Request message from the network.

b) When the UE is in a LADN service area, the UE:

   - may request a PDU Session Establishment/Modification for this LADN DNN;

   - may request to activate UP connection of the existing PDU Session for this LADN DNN.

The SMF supporting a DNN is configured with information about whether this DNN is a LADN DNN or not.

When receiving SM request corresponding an LADN from the AMF, the SMF determines whether the UE is inside LADN service area based on the indication (i.e. UE Presence in LADN service area) received from the AMF. If the SMF does not receive the indication, the SMF considers that the UE is outside of the LADN service area. The SMF shall reject the request if the UE is outside of the LADN service area.

When the SMF receives a request for PDU Session Establishment with the LADN DNN, it shall subscribe to "UE mobility event notification" for reporting UE presence in Area of Interest by providing LADN DNN to the AMF as described in clauses 5.6.11 and 5.3.4.4.

Based on the notification about the UE presence in LADN service area notified by AMF (i.e. IN, OUT, or UNKNOWN), the SMF takes actions as follows based on operator's policy:

a) When SMF is informed that the UE presence in a LADN service area is OUT, the SMF shall:

   - release the PDU Session immediately; or

   - deactivate the user plane connection for the PDU Session with maintaining the PDU Session and ensure the Data Notification is disabled and the SMF may release the PDU Session if the SMF is not informed that the UE moves into the LADN service area after a period.

b) When SMF is informed that the UE presence a LADN service area is IN, the SMF shall:

   - ensure that Data Notification is enabled.

   - trigger the Network triggered Service Request procedure for a LADN PDU Session to active the UP connection when the SMF receives downlink data or Data Notification from UPF.

c) When the SMF is informed that the UE presence in a LADN service area is UNKNOWN, the SMF may:

   - ensure that Data Notification is enabled.

- trigger the Network triggered Service Request procedure for a LADN PDU Session to active the UP connection when the SMF receives downlink data or Data Notification from UPF.

5.6.6 Secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session

At PDU Session Establishment to a DN:

- The DN-specific identity (TS 33.501 [29]) of a UE may be authenticated/authorized by the DN.

NOTE 1: the DN-AAA server may belong to the 5GC or to the DN.

- If the UE provides authentication/authorization information corresponding to a DN-specific identity during the Establishment of the PDU Session, and the SMF determines that Secondary authentication/authorization of the PDU Session Establishment is required based on the SMF policy associated with the DN, the SMF passes the authentication/authorization information of the UE to the DN-AAA server via the UPF if the DN-AAA server is located in the DN. If the SMF determines that Secondary authentication/authorization of the PDU Session Establishment is required but the UE has not provided a DN-specific identity as part of the PDU Session Establishment request, the SMF requests the UE to indicate a DN-specific identity using EAP procedures as described in TS 33.501 [29]. If the Secondary authentication/authorization of the PDU Session Establishment fails, the SMF rejects the PDU Session Establishment.

NOTE 2: If the DN-AAA server is located in the 5GC and reachable directly, then the SMF may communicate with it directly without involving the UPF.

- The DN-AAA server may authenticate/authorize the PDU Session Establishment.

- When DN-AAA server authorizes the PDU Session Establishment, it may send DN Authorization Data for the established PDU Session to the SMF. The DN authorization data for the established PDU Session may include one or more of the following:

  - A DN Authorization Profile Index which is a reference to authorization data for policy and charging control locally configured in the SMF or PCF.

  - a list of allowed MAC addresses for the PDU Session; this shall apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2.

  - a list of allowed VIDs for the PDU Session; this shall apply only for PDU Session of Ethernet PDU type and is further described in clause 5.6.10.2.

  - DN authorized Session AMBR for the PDU Session. The DN Authorized Session AMBR for the PDU Session takes precedence over the subscribed Session-AMBR received from the UDM.

  - Framed Route information (see clause 5.6.14) for the PDU Session.

SMF policies may require DN authorization without Secondary authentication/authorization. In that case, when contacting the DN-AAA server for authorization, the SMF provides the GPSI of the UE if available.

Such Secondary authentication/authorization takes place for the purpose of PDU Session authorization in addition to:

- The 5GC access authentication handled by AMF and described in clause 5.2.

- The PDU Session authorization enforced by SMF with regard to subscription data retrieved from UDM.

Based on local policies the SMF may initiate Secondary authentication/authorization at PDU Session Establishment. The SMF provides the GPSI, if available, in the signalling exchanged with the DN-AAA during Secondary authentication/authorization.

After the successful Secondary authentication/authorization, a session is kept between the SMF and the DN-AAA.

The UE provides the authentication/authorization information required to support Secondary authentication/authorization by the DN over NAS SM.

NOTE 3: The way for the UE to acquire such information is not defined.

SMF policies or subscription information (such as defined in TS 23.502 [3] Table 5.2.3.3.1) may trigger the need for SMF to request the Secondary authentication/authorization and/or UE IP address / Prefix from the DN-AAA server.

When SMF adds a PDU Session Anchor (such as defined in clause 5.6.4) to a PDU Session Secondary authentication/authorization is not carried out, but SMF policies may require SMF to notify the DN when a new prefix or address has been added to or removed from a PDU Session or N6 traffic routing information has been changed for a PDU Session.

When SMF gets notified from UPF with the addition or removal of MAC addresses to/from a PDU Session, the SMF policies may require SMF to notify the DN-AAA server.

Indication of PDU Session Establishment rejection is transferred by SMF to the UE via NAS SM.

If the DN-AAA sends DN Authorization Data for the authorized PDU Session to the SMF and dynamic PCC is deployed, the SMF sends the PCF the DN authorized Session AMBR and/or DN Authorization Profile Index in the DN Authorization Data for the established PDU Session.

If the DN-AAA sends DN Authorization Profile Index in DN Authorization Data to the SMF and dynamic PCC is not deployed, the SMF uses the DN Authorization Profile Index to refer the locally configured information.

NOTE 4: DN Authorization Profile Index is assumed to be pre-negotiated between the operator and the administrator of DN-AAA server.

If the DN-AAA does not send DN Authorization Data for the established PDU Session, the SMF may use locally configured information.

At any time, a DN-AAA server may revoke the authorization for a PDU Session or update DN Authorization Data for a PDU Session. According to the request from DN-AAA server, the SMF may release or update the PDU Session. See clause 5.6.14 when the update involves Framed Route information.

At any time, a DN-AAA server or SMF may trigger Secondary Re-authentication procedure for a PDU Session established with Secondary Authentication as specified in clause 11.1.3 in TS 33.501 [29].

During Secondary Re-authentication/Re-authorization, if the SMF receives from DN-AAA the DN authorized Session AMBR and/or DN Authorization Profile Index, the SMF shall report the received value(s) to the PCF.

The procedure for secondary authentication/authorization by a DN-AAA server during the establishment of a PDU Session is described in TS 23.502 [3] clause 4.3.2.3.

5.6.7 Application Function influence on traffic routing

5.6.7.1 General

The content of this clause applies to non-roaming and to LBO deployments i.e. to cases where the involved entities (AF, PCF, SMF, UPF) belong to the Serving PLMN or AF belongs to a third party with which the Serving PLMN has an agreement. AF influence on traffic routing does not apply in the case of Home Routed deployments. PCF shall not apply AF requests to influence traffic routing to PDU Sessions established in Home Routed mode.

An AF may send requests to influence SMF routeing decisions for traffic of PDU Session. The AF requests may influence UPF (re)selection and allow routeing user traffic to a local access to a Data Network (identified by a DNAI)

The AF may issue requests on behalf of applications not owned by the PLMN serving the UE.

If the operator does not allow an AF to access the network directly, the AF shall use the NEF to interact with the 5GC, as described in clause 6.2.10.

The AF may be in charge of the (re)selection or relocation of the applications within the local DN. Such functionality is not defined. For this purpose, the AF may request to get notified about events related with PDU Sessions.

The AF requests are sent to the PCF via N5 (in the case of requests targeting specific on-going PDU Sessions of individual UE(s), for an AF allowed to interact directly with the 5GC NFs) or via the NEF. The AF requests that target existing or future PDU Sessions of multiple UE(s) or of any UE are sent via the NEF and may target multiple PCF(s), as described in clause 6.3.7.2. The PCF(s) transform(s) the AF requests into policies that apply to PDU Sessions. When the AF has subscribed to UP path management event notifications from SMF(s) (including notifications on how to reach a

GPSI over N6), such notifications are sent either directly to the AF or via an NEF (without involving the PCF). For AF interacting with PCF directly or via NEF, the AF requests may contain the information as described in the Table 5.6.7-1:

Table 5.6.7-1: Information element contained in AF request

Information Name	Applicable for PCF or NEF (NOTE 1)	Applicable for NEF only	Category
Traffic Description	Defines the target traffic to be influenced, represented by the combination of DNN and optionally S-NSSAI, and application identifier or traffic filtering information.	The target traffic can be represented by AF-Service-Identifier, instead of combination of DNN and optionally S-NSSAI.	Mandatory
Potential Locations of Applications	Indicates potential locations of applications, represented by a list of DNAI(s).	The potential locations of applications can be represented by AF-Service-Identifier.	Conditional (NOTE 2)
Target UE Identifier(s)	Indicates the UE(s) that the request is targeting, i.e. an individual UE, a group of UE represented by Internal Group Identifier (NOTE 3), or any UE accessing the combination of DNN, S-NSSAI and DNAI(s).	GPSI can be applied to identify the individual UE, or External Group Identifier can be applied to identify a group of UE.	Mandatory
Spatial Validity Condition	Indicates that the request applies only to the traffic of UE(s) located in the specified location, represented by areas of validity.	The specified location can be represented by a list of geographic zone identifier(s).	Optional
AF transaction identifier	The AF transaction identifier refers to the AF request.	N/A	Mandatory
N6 Traffic Routing requirements	Routing profile ID and/or N6 traffic routing information corresponding to each DNAI and an optional indication of traffic correlation.	N/A	Optional (NOTE 2)
Application Relocation Possibility	Indicates whether an application can be relocated once a location of the application is selected by the 5GC.	N/A	Optional
UE IP address preservation indication	Indicates UE IP address should be preserved.	N/A	Optional
Temporal Validity Condition	Time interval(s) or duration(s).	N/A	Optional
Information on AF subscription to corresponding SMF events	Indicates whether the AF subscribes to change of UP path of the PDU Session and the parameters of this subscription.	N/A	Optional
NOTE 1: When the AF request targets existing or future PDU Sessions of multiple UE(s) or of any UE and is sent via the NEF, as described in clause 6.3.7.2, the information is stored in the UDR by the NEF and notified to the PCF by the UDR. NOTE 2: The potential locations of applications and N6 traffic routing requirements may be absent only if the request is for subscription to notifications about UP path management events only. NOTE 3: Internal Group ID can only be used by an AF controlled by the operator.			

For each information element mentioned above in the AF request, the detailed description is as follows:

1) Information to identify the traffic. The traffic can be identified in the AF request by

   - Either a DNN and possibly slicing information (S-NSSAI) or an AF-Service-Identifier

     - When the AF provides an AF-Service-Identifier i.e. an identifier of the service on behalf of which the AF is issuing the request, the 5G Core maps this identifier into a target DNN and slicing information (S-NSSAI)

- When the NEF processes the AF request the AF-Service-Identifier may be used to authorize the AF request.

- An application identifier or traffic filtering information (e.g. 5 Tuple). The application identifier refers to an application handling UP traffic and is used by the UPF to detect the traffic of the application

  When the AF request is for influencing SMF routing decisions, the information is to identify the traffic to be routed.

  When the AF request is for subscription to notifications about UP path management events, the information is to identify the traffic that the events relate to.

2) Information about the N6 traffic routing requirements for traffic identified as defined in 1). This includes:

   - Information about the N6 traffic routing requirements that is provided per DNAI: for each DNAI, the N6 traffic routing requirements may contain a routing profile ID and/or N6 traffic routing information.

   - An optional indication of traffic correlation, when the information in 4) identifies a group of UEs. This implies the targeted PDU Sessions should be correlated by a common DNAI in the user plane for the traffic identified in 1). If this indication is provided by the AF, the 5GC should select a common DNAI for the target PDU Sessions from the list of DNAI(s) specified in 3).

NOTE 1: The N6 traffic routing requirements are related to the mechanism enabling traffic steering in the local access to the DN. The routing profile ID refers to a pre-agreed policy between the AF and the 5GC. This policy may refer to different steering policy ID(s) sent to SMF and e.g. based on time of the day etc.

NOTE 2: The mechanisms enabling traffic steering in the local access to the DN are not defined.

3) Potential locations of applications towards which the traffic routing should apply. The potential location of application is expressed as a list of DNAI(s). If the AF interacts with the PCF via the NEF, the NEF may map the AF-Service-Identifier information to a list of DNAI(s). The DNAI(s) may be used for UPF (re)selection.

4) Information on the UE(s). This may correspond to:

   - Individual UEs identified using GPSI, or an IP address/Prefix or a MAC address.

   - Groups of UEs identified by an External Group Identifier as defined in TS 23.682 [36] when the AF interacts via the NEF, or Internal-Group Identifier (see clause 5.9.7) when the AF interacts directly with the PCF.

   - Any UE accessing the combination of DNN, S-NSSAI and DNAI(s).

     When the PDU Session type is IPv4 or IPv6 or IPv4v6, and the AF provides an IP address and/or an IP Prefix, or when the PDU Session type is Ethernet and the AF provides a MAC address, this allows the PCF to identify the PDU Session for which this request applies and the AF request applies only to that specific PDU Session of the UE. In this case, additional information such as the UE identity may also be provided to help the PCF to identify the correct PDU Session.

     Otherwise the request targets multiple UE(s) and shall apply to any existing or future PDU Sessions that match the parameters in the AF request.

     When the AF request targets an individual UE and GPSI is provided within the AF request, the GPSI is mapped to SUPI according to the subscription information received from UDM.

     When the AF request targets any UE or a group of UE, the AF request is likely to influence multiple PDU Sessions possibly served by multiple SMFs and PCFs.

     When the AF request targets a group of UE it provides one or several group identifiers in its request. The group identifiers provided by the AF are mapped to Internal-Group identifiers. Members of the group have this Group Identifier in their subscription. The Internal-Group Identifier is stored in UDM, retrieved by SMF from UDM and passed by SMF to PCF at PDU Session set-up. The PCF can then map the AF requests with user subscription and determine whether an AF request targeting a Group of users applies to a PDU Session.

     When the AF request is for influencing SMF routing decisions, the information is to identify UE(s) whose traffic is to be routed.

When the AF request is for subscription to notifications about UP path management events, the information is to identify UE(s) whose traffic the events relate to.

When the AF request is for traffic forwarding in a PDU Session serving for TSC, the MAC address used by the PDU Session is determined by the AF to identify UE whose traffic is to be routed according to the previously stored binding relationship of the 5GS Bridge and the port number of the traffic forwarding information received from TSN network.

5) Indication of application relocation possibility. This indicates whether an application can be relocated once a location of the application is selected by the 5GC. If application relocation is not possible, the 5GC shall ensure that for the traffic related with an application, no DNAI change takes place once selected for this application.

6) Temporal validity condition. This is provided in the form of time interval(s) or duration(s) during which the AF request is to be applied.

   When the AF request is for influencing SMF routing decisions, the temporal validity condition indicates when the traffic routing is to apply.

   When the AF request is for subscription to notifications about UP path management events, the temporal validity condition indicates when the notifications are to be generated.

7) Spatial validity condition on the UE(s) location. This is provided in the form of validity area(s). If the AF interacts with the PCF via the NEF, it may provide a list of geographic zone identifier(s) and the NEF maps the information to areas of validity based on pre-configuration. The PCF in turn determines area(s) of interest based on validity area(s).

   When the AF request is for influencing SMF routing decisions, the spatial validity condition indicates that the request applies only to the traffic of UE(s) located in the specified location.

   When the AF request is for subscription to notifications about UP path management events, the spatial validity condition indicates that the subscription applies only to the traffic of UE(s) located in the specified location.

8) Information on AF subscription to corresponding SMF events.

   The AF may request to be subscribed to change of UP path associated with traffic identified in the bullet 1) above. The AF request contains:

   - A type of subscription (subscription for Early and/or Late notifications).

     The AF subscription can be for Early notifications and/or Late notifications. In the case of a subscription for Early notifications, the SMF sends the notifications before the (new) UP path is configured. In the case of a subscription for Late notifications, the SMF sends the notification after the (new) UP path has been configured.

   - Optionally, an indication of "AF acknowledgment to be expected".

     The indication implies that the AF will provide a response to the notifications of UP path management events to the 5GC. The SMF may, according to this indication, determine to wait for a response from the AF before the SMF configures in the case of early notification, or activates in the case of late notification, the new UP path as described in clause 5.6.7.2.

   The AF subscription can also request to receive information associating the GPSI of the UE with the IP address(es) of the UE and/or with actual N6 traffic routing to be used to reach the UE on the PDU Session; in this case the corresponding information is sent by the SMF regardless of whether a DNAI applies to the PDU Session.

9) An AF transaction identifier referring to the AF request. This allows the AF to update or remove the AF request and to identify corresponding UP path management event notifications. The AF transaction identifier is generated by the AF.

   When the AF interacts with the PCF via the NEF, the NEF maps the AF transaction identifier to an AF transaction internal identifier, which is generated by the NEF and used within the 5GC to identify the information associated to the AF request. The NEF maintains the mapping between the AF transaction identifier and the AF transaction internal identifier. The relation between the two identifiers is implementation specific.

When the AF interacts with the PCF directly, the AF transaction identifier provided by the AF is used as AF transaction internal identifier within the 5GC.

10) Indication of UE IP address preservation. This indicates UE IP address related to the traffic identified in bullet 1) should be preserved. If this indication is provided by the AF, the 5GC should preserve the UE IP address by preventing reselection of PSA UPF for the identified traffic once the PSA UPF is selected.

An AF may send requests to influence SMF routeing decisions, for event subscription or for both.

The AF may request to be subscribed to notifications about UP path management events, i.e. a UP path change occurs for the PDU Session. The corresponding notification about a UP path change sent by the SMF to the AF may indicate the DNAI and /or the N6 traffic routing information that has changed as described in clause 4.3.6.3 of TS 23.502 [3]. It may include the AF transaction internal identifier, the type of notification (i.e. early notification or late notification), the Identity of the source and/or target DNAI, the IP address/prefix of the UE or the MAC address used by the UE, the GPSI and the N6 traffic routing information related to the 5GC UP.

NOTE 3: The change from the UP path status where no DNAI applies to a status where a DNAI applies indicates the activation of this AF request; the change from the UP path status where a DNAI applies to a status where no DNAI applies indicates the de-activation of this AF request.

In the case of IP PDU Session Type, the IP address/prefix of the UE together with N6 traffic routing information indicates to the AF how to reach over the User Plane the UE identified by its GPSI. N6 traffic routing information indicates any tunnelling that may be used over N6. The nature of this information depends on the deployment.

NOTE 4: N6 traffic routing information can e.g. correspond to the identifier of a VPN or to explicit tunnelling information such as a tunnelling protocol identifier together with a Tunnel identifier.

NOTE 5: In the case of Unstructured PDU Session type the nature of the N6 traffic routing information related to the 5GC UP is described in clause 5.6.10.3.

In the case of Ethernet PDU Session Type, the MAC address of the UE together with N6 traffic routing information indicates to the AF how to reach over the User Plane the UE identified by its GPSI. The UE MAC address (es) is reported by the UPF as described in clause 5.8.2.12. The N6 traffic routing information can be, e.g. a VLAN ID or the identifier of a VPN or a tunnel identifier at the UPF.

In the case of PDU Session serving for TSC, the SMF informs AF of the 5GS Bridge user plane information as defined in clause 5.28.1, as well as the association between the MAC address used by the PDU Session, 5GS Bridge ID and port ID on DS-TT.

When notifications about UP path management events are sent to the AF via the NEF, if required, the NEF maps the UE identify information, e.g. SUPI, to the GPSI and the AF transaction internal identifier to the AF transaction identifier before sending the notifications to the AF.

The PCF authorizes the request received from the AF based on information received from the AF, operator's policy, etc. and determines for each DNAI, a traffic steering policy ID (derived from the routing profile ID provided by the AF) and/or the N6 traffic routing information (as provided by the AF) to be sent to the SMF as part of the PCC rules. The traffic steering policy IDs are configured in the SMF or in the UPF. The traffic steering policy IDs are related to the mechanism enabling traffic steering to the DN.

The DNAIs are related to the information considered by the SMF for UPF selection, e.g. for diverting (locally) some traffic matching traffic filters provided by the PCF.

The PCF acknowledges a request targeting an individual PDU Session to the AF or to the NEF.

For PDU Session that corresponds to the AF request, the PCF provides the SMF with a PCC rule that is generated based on the AF request, Local routing indication from the PDU Session policy control subscription information and taking into account UE location presence in area of interest (i.e. Presence Reporting Area). The PCC rule contains the information to identify the traffic, information about the DNAI(s) towards which the traffic routing should apply and optionally, an indication of traffic correlation and/or an indication of application relocation possibility and/or indication of UE IP address preservation. The PCC rule also contains per DNAI a traffic steering policy ID and/or N6 traffic routing information, if the N6 traffic routing information is explicitly provided in the AF request. The PCF may also provide in the PCC rule information to subscribe the AF (or the NEF) to SMF events (UP path changes) corresponding to the AF request in which case it provides the information on AF subscription to corresponding SMF events received in the AF request. This is done by providing policies at PDU Session set-up or by initiating a PDU Session Modification

procedure. When initiating a PDU Session set-up or PDU Session Modification procedure, the PCF considers the latest known UE location to determine the PCC rules provided to the SMF. The PCF evaluates the temporal validity condition of the AF request and informs the SMF to activate or deactivate the corresponding PCC rules according to the evaluation result. When policies specific to the PDU Session and policies general to multiple PDU Sessions exist, the PCF gives precedence to the PDU Session specific policies over the general policies.

The spatial validity condition is resolved at the PCF. In order to do that, the PCF subscribes to the SMF to receive notifications about change of UE location in an area of interest (i.e. Presence Reporting Area). The subscribed area of interest may be the same as spatial validity condition, or may be a subset of the spatial validity condition (e.g. a list of TAs) based on the latest known UE location. When the SMF detects that UE entered the area of interest subscribed by the PCF, the SMF notifies the PCF and the PCF provides to the SMF the PCC rules described above by triggering a PDU Session Modification. When the SMF becomes aware that the UE left the area subscribed by the PCF, the SMF notifies the PCF and the PCF provides updated PCC rules by triggering a PDU Session Modification. SMF notifications to the PCF about UE location in or out of the subscribed area of interest are triggered by UE location change notifications received from the AMF or by UE location information received during a Service Request or Handover procedure.

When the PCC rules are activated, the SMF may, based on local policies, take the information in the PCC rules into account to:

- (re)select UP paths (including DNAI(s)) for PDU Sessions. The SMF is responsible for handling the mapping between the UE location (TAI / Cell-Id) and DNAI(s) associated with UPF and applications and the selection of the UPF(s) that serve a PDU Session. This is described in clause 6.3.3. If the PDU Session is of IP type and if Indication of UE IP address preservation is included in the PCC rules, the SMF should preserve the UE IP address, by not reselecting the related PSA UPF once the PSA UPF is selected, for the traffic identified in the PCC rule. If the PCC rules are related to a 5G VN group served by the SMF and if the Information about the N6 traffic routing requirements includes an indication of traffic correlation, the SMF should select a common DNAI for the PDU Sessions of the 5G VN group.

- configure traffic steering at UPF, including activating mechanisms for traffic multi-homing or enforcement of an UL Classifier (UL CL). Such mechanisms are defined in clause 5.6.4. This may include that the SMF is providing the UPF with packet handling instructions (i.e. PDRs and FARs) for steering traffic to the local access to the DN. The packet handling instructions are generated by the SMF using the traffic steering policy ID and/or the N6 traffic routing information in the PCC rules corresponding to the applied DNAI. In the case of UP path reselection, the SMF may configure the source UPF to forward traffic to the UL CL/BP so that the traffic is steered towards the target UPF.

- if Information on AF subscription to corresponding SMF events has been provided in the PCC rule, inform the AF of the (re)selection of the UP path (UP path change). If the information includes an indication of "AF acknowledgment to be expected", the SMF may decide to wait for a response from the AF before it activates the new UP path, as described in clause 5.6.7.2.

When an I-SMF is inserted for a PDU Session, the I-SMF insertion, relocation or removal to a PDU session shall be transparent (i.e. not aware) to the PCF and to the AF. The processing of the AF influence on traffic routing is described in clause 5.34 and detail procedure is described in clause 4.23.6 of TS 23.502 [3].

5.6.7.2 Enhancement of UP path management based on the coordination with AFs

In order to avoid or minimize service interruption during PSA relocation for a PDU session of SSC mode 3, or a PDU session with UL CL or branch point, according to the indication of "AF acknowledgment to be expected" on AF subscription to corresponding SMF events (DNAI change) in the PCC rules received from the PCF and local configuration (e.g. DN-related policies) the SMF may wait for a response from the AF after sending a notification (an early notification or a late notification) to the AF. In the case of late notification, based on the indication of "AF acknowledgment to be expected" on AF subscription, the SMF may send the notification before activating the UP path towards a new DNAI (possibly through a new PSA).

NOTE 1: Before the UP path toward the new DNAI is activated, application traffic data (if any exists) is still routed toward the old DNAI.

The notification sent from the SMF to the AF indicates UP path management events (DNAI change) as described in clause 5.6.7.1. The AF can confirm the DNAI change indicated in the notification with the SMF by sending a positive response to the notification to the SMF or reject the DNAI change by sending a negative response.

NOTE 2: The AF can determine whether application relocation is needed according to the notification of DNAI change. If not, the AF can send a positive response to the SMF immediately; otherwise, the AF sends the positive response after application relocation is completed or a negative response if the AF determines that the application relocation cannot be completed on time (e.g. due to temporary congestion). The AF decision and behaviours on application relocation are not defined. However, the new DNAI may be associated with a new AF. In such cases, the SMF and the old AF cancel earlier subscribed UP path management event notifications, and the new AF subscribes to receive UP path management event notifications from the SMF.

The AF can include N6 traffic routing information related to the target DNAI in a positive response sent to the SMF. The SMF configures the N6 traffic routing information from the AF response to the PSA on the UP path.

In the case of early notification, based on the indication of "AF acknowledgment to be expected" on AF subscription, the SMF does not configure the UP path towards the new DNAI until it receives a positive AF response as specified in clause 4.3.6.3 of TS 23.502 [3].

In the case of late notification, based on the indication of "AF acknowledgment to be expected" on AF subscription, the SMF does not activate the UP path towards the new DNAI until it receives a positive AF response as specified in clause 4.3.5 of TS 23.502 [3].

NOTE 3: After the UP path toward the new DNAI is activated, data is routed toward the new DNAI.

If the SMF receives a negative response at any time, the SMF keeps using the original DNAI and may cancel related PSA relocation or addition. The SMF may perform DNAI reselection afterwards if needed.

The SMF can assume according to local policy a negative response if a response is expected and but not received from the AF within a certain time window.

5.6.8 Selective activation and deactivation of UP connection of existing PDU Session

This clause applies to the case when a UE has established multiple PDU Sessions. The activation of a UP connection of an existing PDU Session causes the activation of its UE-CN User Plane connection (i.e. data radio bearer and N3 tunnel).

For the UE in the CM-IDLE state in 3GPP access, either UE or Network-Triggered Service Request procedure may support independent activation of UP connection of existing PDU Session. For the UE in the CM-IDLE state in non-3GPP access, UE-Triggered Service Request procedure allows the re-activation of UP connection of existing PDU Sessions, and may support independent activation of UP connection of existing PDU Session.

A UE in the CM-CONNECTED state invokes a Service Request (see TS 23.502 [3] clause 4.2.3.2) procedure to request the independent activation of the UP connection of existing PDU Sessions.

Network Triggered re-activation of UP connection of existing PDU Sessions is handled as follows:

- If the UE CM state in the AMF is already CM-CONNECTED on the access (3GPP, non-3GPP) associated to the PDU Session in the SMF, the network may re-activate the UP connection of a PDU Session using a Network Initiated Service Request procedure.

Otherwise:

- If the UE is registered in both 3GPP and non-3GPP accesses and the UE CM state in the AMF is CM-IDLE in non-3GPP access, the UE can be paged or notified through the 3GPP access for a PDU Session associated in the SMF (i.e. last routed) to the non-3GPP access:

  - If the UE CM state in the AMF is CM-IDLE in 3GPP access, the paging message may include the access type associated with the PDU Session in the SMF. The UE, upon reception of the paging message containing an access type, shall reply to the 5GC via the 3GPP access using the NAS Service Request message, which shall contain the list of PDU Sessions associated with the received access type and whose UP connections can be re-activated over 3GPP (i.e. the list does not contain the PDU Sessions whose UP connections cannot be re-activated on 3GPP based on UE policies and whether the S-NSSAIs of these PDU Sessions are within the Allowed NSSAI for 3GPP access). If the PDU Session for which the UE has been paged is in the list of the PDU Sessions provided in the NAS Service Request and the paging was triggered by pending DL data, the 5GC shall re-activate the PDU Session UP connection over 3GPP access. If the paging was triggered by

pending DL signalling, the Service Request succeeds without re-activating the PDU session UP connection over the 3GPP access and the pending DL signalling is delivered to the UE over the 3GPP access;

- If the UE CM state in the AMF is CM-CONNECTED in 3GPP access, the notification message shall include the non-3GPP Access Type. The UE, upon reception of the notification message, shall reply to the 5GC via the 3GPP access using the NAS Service Request message, which shall contain the List of Allowed PDU Sessions that can be re-activated over 3GPP or an empty List of Allowed PDU Sessions if no PDU Sessions are allowed to be re-activated over 3GPP access.

NOTE: A UE that is in a coverage of a non-3GPP access and has PDU Session(s) that are associated in the UE (i.e. last routed) to non-3GPP access, is assumed to attempt to connect to it without the need to be paged.

- If the UE is registered in both 3GPP and non-3GPP accesses served by the same AMF and the UE CM state in the AMF is CM-IDLE in 3GPP access and is in CM-CONNECTED in non 3GPP access, the UE can be notified through the non-3GPP for a PDU Session associated in the SMF (i.e. last routed) to the 3GPP access. The notification message shall include the 3GPP Access Type. Upon reception of the notification message, when 3GPP access is available, the UE shall reply to the 5GC via the 3GPP access using the NAS Service Request message.

In addition to the above, a PDU Session may be established as an always-on PDU Session as described in clause 5.6.13.

The deactivation of the UP connection of an existing PDU Session causes the corresponding data radio bearer and N3 tunnel to be deactivated. The UP connection of different PDU Sessions can be deactivated independently when a UE is in CM-CONNECTED state in 3GPP access or non-3GPP access. At the deactivation of the UP of a PDU Session using a N9 tunnel whose end-point is controlled by an I-SMF, the N9 tunnel is preserved. If a PDU Session is an always-on PDU Session, the SMF should not deactivate a UP connection of this PDU Session due to inactivity.

5.6.9 Session and Service Continuity

5.6.9.1 General

The support for session and service continuity in 5G System architecture enables to address the various continuity requirements of different applications/services for the UE. The 5G System supports different session and service continuity (SSC) modes defined in this clause. The SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session. The following three modes are specified with further details provided in the next clause:

- With SSC mode 1, the network preserves the connectivity service provided to the UE. For the case of PDU Session of IPv4 or IPv6 or IPv4v6 type, the IP address is preserved.

- With SSC mode 2, the network may release the connectivity service delivered to the UE and release the corresponding PDU Session(s). For the case of IPv4 or IPv6 or IPv4v6 type, the release of the PDU Session induces the release of IP address(es) that had been allocated to the UE.

- With SSC mode 3, changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. For the case of IPv4 or IPv6 or IPv4v6 type, the IP address is not preserved in this mode when the PDU Session Anchor changes.

NOTE: In this Release of the specification, the addition/removal procedure of additional PDU Session Anchor in a PDU Session for local access to a DN is independent from the SSC mode of the PDU Session.

5.6.9.2 SSC mode

5.6.9.2.1 SSC Mode 1

For a PDU Session of SSC mode 1, the UPF acting as PDU Session Anchor at the establishment of the PDU Session is maintained regardless of the access technology (e.g. Access Type and cells) a UE is successively using to access the network.

In the case of a PDU Session of IPv4 or IPv6 or IPv4v6 type, IP continuity is supported regardless of UE mobility events.

In this Release of the specification, when IPv6 multihoming or UL CL applies to a PDU Session of in SSC mode 1, and the network allocates (based on local policies) additional PDU Session Anchors to such a PDU Session, these additional PDU Session Anchors may be released or allocated, and the UE does not expect that the additional IPv6 prefix is maintained during the lifetime of PDU Session.

SSC mode 1 may apply to any PDU Session type and to any access type.

5.6.9.2.2 SSC Mode 2

If a PDU Session of SSC mode 2 has a single PDU Session Anchor, the network may trigger the release of the PDU Session and instruct the UE to establish a new PDU Session to the same data network immediately. The trigger condition depends on operator policy e.g. request from Application Function, based on load status, etc. At establishment of the new PDU Session, a new UPF acting as PDU Session Anchor can be selected.

Otherwise, if a PDU Session of SSC mode 2 has multiple PDU Session Anchors (i.e. in the case of multi-homed PDU Sessions or in the case that UL CL applies to a PDU Session of SSC mode 2), the additional PDU Session Anchors may be released or allocated.

SSC mode 2 may apply to any PDU Session type and to any access type.

NOTE: In UL CL mode, the UE is not involved in PDU Session Anchor re-allocation, so that the existence of multiple PDU Session Anchors is not visible to the UE.

5.6.9.2.3 SSC Mode 3

For PDU Session of SSC mode 3, the network allows the establishment of UE connectivity via a new PDU Session Anchor to the same data network before connectivity between the UE and the previous PDU Session Anchor is released. When trigger conditions apply, the network decides whether to select a PDU Session Anchor UPF suitable for the UE's new conditions (e.g. point of attachment to the network).

In this Release of specification, SSC mode 3 only applies to IP PDU Session type and to any access type.

In the case of a PDU Session of IPv4 or IPv6 or IPv4v6 type, during the procedure of change of PDU Session Anchor, the following applies:

a. For a PDU Session of IPv6 type, the new IP prefix anchored on the new PDU Session Anchor may be allocated within the same PDU Session (relying on IPv6 multi-homing specified in clause 5.6.4.3), or

b. The new IP address and/or IP prefix may be allocated within a new PDU Session that the UE is triggered to establish.

After the new IP address/prefix has been allocated, the old IP address/prefix is maintained during some time indicated to the UE via NAS signalling (as described in TS 23.502 [3] clause 4.3.5.2) or via Router Advertisement (as described in TS 23.502 [3] clause 4.3.5.3) and then released.

If a PDU Session of SSC mode 3 has multiple PDU Session Anchors (i.e., in the case of multi-homed PDU Sessions or in the case that UL CL applies to a PDU Session of SSC mode 3), the additional PDU Session Anchors may be released or allocated.

5.6.9.3 SSC mode selection

SSC mode selection is done by the SMF based on the allowed SSC modes -including the default SSC mode) in the user subscription as well as the PDU Session type and if present, the SSC mode requested by the UE.

The operator may provision a SSC mode selection policy (SSCMSP) to the UE as part of the URSP rule -see TS 23.503 [45] clause 6.6.2). The UE shall use the SSCMSP to determine the type of session and service continuity mode associated with an application or group of applications for the UE as described in TS 23.503 [45] clause 6.6.2.3. If the UE does not have SSCMSP, the UE can select a SSC mode based on UE Local Configuration as described in TS 23.503 [45], if applicable. If the UE cannot select a SSC mode, the UE requests the PDU Session without providing the SSC mode.

NOTE: The UE can use the SSC Mode Selection component of the URSP rule with match-all traffic descriptor if there is no SSC mode in the UE local configuration.

The SSC mode selection policy rules provided to the UE can be updated by the operator by updating the URSP rule.

The SMF receives from the UDM the list of allowed SSC modes and the default SSC mode per DNN per S-NSSAI as part of the subscription information.

If a UE provides an SSC mode when requesting a new PDU Session, the SMF selects the SSC mode by either accepting the requested SSC mode or rejecting the PDU Session Establishment Request message with the cause value and the SSC mode(s) allowed to be used back to UE based on the PDU Session type, subscription and/or local configuration. Based on that cause value and the SSC mode(s) allowed to be used, the UE may re-attempt to request the establishment of that PDU Session with the SSC mode allowed to be used or using another URSP rule.

If a UE does not provide an SSC mode when requesting a new PDU Session, then the SMF selects the default SSC mode for the data network listed in the subscription or applies local configuration to select the SSC mode.

SSC mode 1 shall be assigned to the PDU Session when static IP address/prefix is allocated to the PDU Session based on the static IP address/prefix subscription for the DNN and S-NSSAI. The SMF shall inform the UE of the selected SSC mode for a PDU Session.

The UE shall not request and the network shall not assign SSC mode 3 for the PDU Session of Unstructured type or Ethernet type.

5.6.10 Specific aspects of different PDU Session types

5.6.10.1 Support of IP PDU Session type

The IP address allocation is defined in clause 5.8.1

The UE may acquire following configuration information from the SMF, during the lifetime of a PDU Session:

- Address(es) of P-CSCF(s);
- Address(es) of DNS server(s).

NOTE 1: When DNS over (D)TLS is supported by the network, the configuration information sent by the SMF may also include the corresponding DNS server security information as specified in TS 33.501 [29].

- the GPSI of the UE.

The UE may acquire from the SMF, at PDU Session Establishment, the MTU that the UE shall consider, see clause 5.6.10.4.

The UE may provide following information to the SMF during the lifetime of a PDU Session:

- an indication of the support of P-CSCF re-selection based on procedures specified in TS 24.229 [62] (clauses B.2.2.1C and L.2.2.1C).
- PS data off status of the UE.

NOTE 2: An operator can deploy NAT functionality in the network; the support of NAT is not specified in this release of the specification.

5.6.10.2 Support of Ethernet PDU Session type

For a PDU Session set up with the Ethernet PDU Session type, the SMF and the UPF acting as PDU Session Anchor (PSA) can support specific behaviours related with the fact the PDU Session carries Ethernet frames.

Depending on operator configuration related with the DNN, different configurations for how Ethernet traffic is handled on N6 may apply, for example:

- Configurations with a 1-1 relationship between a PDU Session and a N6 interface possibly corresponding to a dedicated tunnel established over N6. In this case the UPF acting as PSA transparently forwards Ethernet frames between the PDU Session and its corresponding N6 interface, and it does not need to be aware of MAC addresses used by the UE in order to route down-link traffic.

- Configurations, where more than one PDU Session to the same DNN (e.g. for more than one UE) corresponds to the same N6 interface. In this case the UPF acting as PSA needs to be aware of MAC addresses used by the UE in the PDU Session in order to map down-link Ethernet frames received over N6 to the appropriate PDU Session. Forwarding behaviour of the UPF acting as PSA is managed by SMF as specified in clause 5.8.2.5.

NOTE 1: The "MAC addresses used by the UE" correspond to any MAC address used by the UE or any device locally connected to the UE and using the PDU Session to communicate with the DN.

Based on operator configuration, the SMF may request the UPF acting as the PDU Session Anchor to respond to ARP/IPv6 Neighbour Solicitation requests based on local cache information, i.e. the mapping between the UE MAC address to the UE IP address, and the DN where the PDU Session is connected to, or to redirect the ARP traffic from the UPF to the SMF. Responding to ARP/IPv6 ND based on local cache information applies to ARP/IPv6 ND received in both UL and DL directions.

NOTE 2: Responding to ARP/ND from a local cache assumes the UE or the devices behind the UE acquire their IP address via in-band mechanisms that the SMF/UPF can detect and by this link the IP address to the MAC address.

NOTE 3: This mechanism is intended to avoid broadcasting or multicasting the ARP/IPv6 ND to every UE.

Ethernet Preamble and Start of Frame delimiter are not sent over 5GS:

- For UL traffic the UE strips the preamble and frame check sequence (FCS) from the Ethernet frame.

- For DL traffic the PDU Session Anchor strips the preamble and frame check sequence (FCS) from the Ethernet frame.

Neither a MAC nor an IP address is allocated by the 5GC to the UE for a PDU Session.

The PSA shall store the MAC addresses received from the UE, and associate those with the appropriate PDU Session.

The UPF handles VLAN tags (addition/removal) as instructed by the SMF via PDR (Outer header removal) and FAR (UPF applying Outer header creation of a Forwarding policy). For example:

- The UPF may insert (for uplink traffic) and remove (for downlink traffic) a S-TAG on N6 interface on top of the C-TAG of the UE.

- The UPF may insert (for uplink traffic) and remove (for downlink traffic) a VLAN tag on the N6 interface while there is no VLAN in the traffic to and from the UE.

NOTE 4: This can be used for traffic steering to N6-LAN but also for N6-based traffic forwarding related with 5G-VN service described in clause 5.29.4

Apart from specific conditions related to the support of PDU sessions over W-5GAN defined in TS 23.316 [84], the UPF shall not remove VLAN tags sent by the UE and the UPF shall not insert VLAN tags for the traffic sent to the UE.

PDU(s) containing a VLAN tag shall be switched only within the same VLAN by a PDU Session Anchor.

The UE may acquire from the SMF, at PDU Session Establishment, the MTU of the Ethernet frames' payload that the UE shall consider, see clause 5.6.10.4.

NOTE 5: The UE may operate in bridge mode with regard to a LAN it is connecting to the 5GS, thus different MAC addresses may be used as source address of different frames sent UL over a single PDU Session (and destination MAC address of different frames sent DL over the same PDU Session).

NOTE 6: Entities on the LAN connected to the 5GS by the UE may have an IP address allocated by the DN but the IP layer is considered as an application layer which is not part of the Ethernet PDU Session.

NOTE 7: In this Release of the specification, only the UE connected to the 5GS is authenticated, not the devices behind such UE.

NOTE 8: 5GS does not support the scenario where a MAC address or if VLAN applies a (MAC address, VLAN) combination is used on more than one PDU Session for the same DNN and S-NSSAI.

NOTE 9: This Release of the specification does not guarantee that the Ethernet network remains loop-free. Deployments need to be verified on an individual basis that loops in the Ethernet network are avoided.

NOTE 10: This Release of the specification does not guarantee that the Ethernet network properly and quickly reacts to topology changes. Deployments need to be verified on an individual basis how they react to topology changes.

Different Frames exchanged on a PDU Session of Ethernet type may be served with different QoS over the 5GS. Thus, the SMF may provide to the UPF Ethernet Packet Filter Set and forwarding rule(s) based on the Ethernet frame structure and UE MAC address(es). The UPF detects and forwards Ethernet frames based on the Ethernet Packet Filter Set and forwarding rule(s) received from the SMF. This is further defined in clauses 5.7 and 5.8.2.

When a PDU Session of Ethernet PDU type is authorized by a DN as described in clause 5.6.6, the DN-AAA server may, as part of authorization data, provide the SMF with a list of allowed MAC addresses and/or a list of allowed VIDs for this PDU Session; the list is limited to a maximum of 16 MAC addresses and/or a maximum of 16 VIDs accordingly. When such list(s) have been provided for a PDU Session, the SMF sets corresponding filtering rules in the UPF(s) acting as PDU Session Anchor for the PDU Session. The UPF discards any UL traffic that does not contain one of these MAC addresses as a source address if the list of allowed MAC addresses is provided. The UPF discards any UL traffic that does not contain one of these VIDs if the list of allowed VIDs is provided.

In this Release of specification, the PDU Session of Ethernet PDU Session type is restricted to SSC mode 1 and SSC mode 2.

For a PDU Session established with the Ethernet PDU Session type, the SMF may, upon PCF request, need to ensure reporting to the PCF of all Ethernet MAC addresses used as UE address in a PDU Session. In this case, as defined in clause 5.8.2.12, the SMF controls the UPF to report the different MAC addresses used as source address of frames sent UL by the UE in the PDU Session.

NOTE 11: This relates to whether AF control on a per MAC address is allowed on the PDU Session as defined in TS 23.503 [45] clause 6.1.1.2.

The PCF may activate or deactivate the reporting of the UE MAC address using the "UE MAC address change" Policy Control Request Trigger as defined in Table 6.1.3.5-1 of TS 23.503 [45].

The SMF may relocate the UPF acting as the PDU Session Anchor for an Ethernet PDU Session as defined in clause 4.3.5.8 of TS 23.502 [3]. The relocation may be triggered by a mobility event such as a handover, or may be triggered independent of UE mobility, e.g. due to load balancing reasons. In order to relocate the PSA UPF, the reporting of the UE MAC addresses needs to be activated by the SMF.

5.6.10.3 Support of Unstructured PDU Session type

Different Point-to-Point (PtP) tunnelling techniques may be used to deliver Unstructured PDU Session type data to the destination (e.g. application server) in the Data Network via N6.

Point-to-point tunnelling based on UDP/IP encapsulation as described below may be used. Other techniques may be supported. Regardless of addressing scheme used from the UPF to the DN, the UPF shall be able to map the address used between the UPF and the DN to the PDU Session.

When Point-to-Point tunnelling based on UDP/IPv6 is used, the following considerations apply:

- IPv6 prefix allocation for PDU Sessions are performed locally by the (H-)SMF without involving the UE.
- The UPF(s) acts as a transparent forwarding node for the payload between the UE and the destination in the DN.
- For uplink, the UPF forwards the received Unstructured PDU Session type data to the destination in the data network over the N6 PtP tunnel using UDP/IPv6 encapsulation.
- For downlink, the destination in the data network sends the Unstructured PDU Session type data using UDP/IPv6 encapsulation with the IPv6 address of the PDU Session and the 3GPP defined UDP port for Unstructured PDU Session type data. The UPF acting as PDU Session Anchor decapsulates the received data (i.e. removes the UDP/IPv6 headers) and forwards the data identified by the IPv6 prefix of the PDU Session for delivery to the UE.
- The (H-)SMF performs the IPv6 related operations but the IPv6 prefix is not provided to the UE, i.e. Router Advertisements and DHCPv6 are not performed. The SMF assigns an IPv6 Interface Identifier for the PDU Session. The allocated IPv6 prefix identifies the PDU Session of the UE.

- For AF influence on traffic routing (described in clause 5.6.7), when the N6 PtP tunnelling is used over the DNAI and the AF provides, by value, information about N6 traffic routing requirements in the AF request, the AF provides N6 PtP tunnelling requirements (IPv6 address and UDP port of the tunnel end in the DN) as the N6 traffic routing information associated to the DNAI; when the SMF notifies the AF of UP path management events, it includes the N6 PtP tunnel information related to the UP (the IPv6 address and the 3GPP defined UDP port of the tunnel end at the UPF) as N6 traffic routing information in the notification.

In this Release of the specification there is support for maximum one 5G QoS Flow per PDU Session of Type Unstructured.

In this Release of specification, the PDU Session of Unstructured PDU Session type is restricted to SSC mode 1 and SSC mode 2.

The UE may acquire from the SMF, at PDU Session Establishment, the MTU that the UE shall consider, see clause 5.6.10.4.

5.6.10.4 Maximum Transfer Unit size considerations

In order to avoid data packet fragmentation between the UE and the UPF acting as PSA, the link MTU size in the UE should be set to the value provided by the network as part of the IP configuration. The link MTU size for IPv4 is sent to the UE by including it in the PCO (see TS 24.501 [47]). The link MTU size for IPv6 is sent to the UE by including it in the IPv6 Router Advertisement message (see RFC 4861 [54]).

NOTE 1: Ideally the network configuration ensures that for PDU Session type IPv4v6 the link MTU values provided to the UE via PCO and in the IPv6 Router Advertisement message are the same. In cases where this condition cannot be met, the MTU size selected by the UE is unspecified.

When using a PDU Session type Unstructured, the maximum uplink packet size, and when using Ethernet, the Ethernet frames' payload, that the UE should use may be provided by the network as a part of the session management configuration by encoding it within the PCO (see TS 24.501 [47]).

When using a PDU Session type Unstructured, to provide a consistent environment for application developers, the network shall use a maximum packet size of at least 128 octets (this applies to both uplink and downlink).

When the MT and the TE are separated, the TE may either be pre-configured to use a specific default MTU size or the TE may use an MTU size provided by the network via the MT. Thus, it is not always possible to set the MTU value by means of information provided by the network.

NOTE 2: In network deployments that have MTU size of 1500 octets in the transport network, providing a link MTU value of 1358 octets (as shown in Figure J-1) to the UE as part of the IP configuration information from the network will prevent the IP layer fragmentation within the transport network between the UE and the UPF. For network deployments that uniformly support transport with larger MTU size than 1500 octets (for example with ethernet jumbo frames of MTU size up to 9216 octets), providing a link MTU value of MTU minus 142 octets to the UE as part of the IP configuration information from the network will prevent the IP layer fragmentation within the transport network between the UE and the UPF. Link MTU considerations are discussed further in Annex J.

NOTE 3: As the link MTU value is provided as a part of the session management configuration information, a link MTU value can be provided during each PDU Session establishment. In this release, dynamic adjustment of link MTU for scenarios where MTU is not uniform across transport are not addressed.

5.6.11 UE presence in Area of Interest reporting usage by SMF

When a PDU Session is established or modified, or when the user plane path has been changed (e.g. UPF re-allocation/addition/removal), SMF may determine an Area of Interest, e.g. based on UPF Service Area, subscription by PCF for reporting UE presence in Presence Reporting Area, etc.

For 3GPP access, the Area of Interest corresponds:

- either to Presence Information that may correspond to:
  - a list of Tracking Areas; or

- a list of Presence Reporting Area ID(s) and optionally the elements comprising TAs and/or NG-RAN nodes and/or cells identifiers corresponding to the PRA ID(s); or

- a LADN DNN.

For Non-3GPP access, the Area of Interest corresponds to:

- N3GPP TAI (see clause 5.3.2.3).

For UE location change into or out of an "area of interest", the SMF subscribes to "UE mobility event notification" service provided by AMF for reporting of UE presence in Area of Interest as described in clause 5.3.4.4. The AMF may send the UE location to the SMF along with the notification, e.g. for UPF selection. Upon reception of a notification from AMF, the SMF determines how to deal with the PDU Session, e.g. reallocate UPF.

In the case of LADN, the SMF provides the LADN DNN to the AMF to subscribe to "UE mobility event notification" for reporting UE presence in LADN service area. Upon reception of a notification from the AMF, the SMF determines how to deal with the PDU Session as described in clause 5.6.5.

For use cases related to policy control and charging decisions, the PCF may subscribe to event reporting from the SMF or the AMF, for UE presence in a Presence Reporting Area.

A Presence Reporting Area can be:

- A "UE-dedicated Presence Reporting Area", defined in the subscriber profile and composed of a short list of TAs and/or NG-RAN nodes and/or cells identifiers in a PLMN; or derived from the Area of Interest provided by the Application Function to the PCF (see clause 5.6.7) and composed of a short list of TAs and/or NG-RAN nodes and/or cells identifiers in a PLMN; or

- A "Core Network predefined Presence Reporting Area", predefined in the AMF and composed of a short list of TAs and/or NG-RAN nodes and/or cells identifiers in a PLMN.

In the case of Change of UE Presence in Presence Reporting Area, for core network predefined Presence Reporting Area, the AMF determines the "area of interest" corresponding to the Presence Reporting Area Identifier(s), provided by the PCF or the SMF, as a list of TAIs and/or cell identifiers and/or NG-RAN node identifiers based on local configuration. For UE-dedicated Presence Reporting Areas, the subscription for UE location change notification for an "area of interest" shall contain the PRA Identifier(s) and the list(s) of TAs, or NG-RAN Node identifier and/or cell identifiers composing the Presence Reporting Area(s). For Core Network predefined Presence Reporting Areas, the subscription for UE location change notification for an "area of interest" shall contain the PRA identifier(s).

NOTE 1: If the Presence Reporting Area (PRA) and RAN Notification Area (RNA) are partially overlapping, the PCF will not get notified for the change of PRA when UE enters or leaves the PRA but remains in the RNA in CM-CONNECTED with RRC Inactive state, because AMF is not informed.

Each Core Network predefined Presence Reporting Area can be configured with a priority level in the AMF. In order to prevent overload, the AMF may set the reporting for one or more of the received Presence Reporting Area(s) to inactive under consideration of the priority configured for each of Core Network predefined Presence Reporting Area(s), while storing the reporting request for this Presence Reporting Area in the UE context.

NOTE 2: Change of UE presence in Presence Reporting Area reporting does not apply to home routed roaming.

The AMF may be configured with a PRA identifier which refers to a Set of Core Network predefined Presence Reporting Areas. If the PCF subscribes to change of UE location for an area of interest for a Set of Presence reporting areas and provides a PRA identifier then the SMF may subscribe for event reporting for this Set of Presence Reporting Areas by only indicating this PRA Identifier in the area of interest. When the Presence Reporting Area(s) to be reported belong to a set of Core Network predefined Presence Reporting Areas in which the AMF is requested to report on change of UE presence, the AMF shall additionally add to the report the PRA Identifier of the Set of Core Network predefined Presence Reporting Areas.

Upon change of AMF, the PRA identifier(s) and if provided, the list(s) of Presence Reporting Area elements are transferred for all PDU sessions as part of MM Context information to the target AMF during the mobility procedure. If one or more Presence Reporting Area(s) was set to inactive, the target AMF may decide to reactivate one or more of the inactive Presence Reporting Area(s). The target AMF indicates per PDU session to the corresponding SMF/PCF the PRA identifier(s) and whether the UE is inside or outside the Presence Reporting Area(s) as well as the inactive Presence Reporting Area(s), if any.

NOTE 3: The target AMF cannot set the Presence Reporting Area(s) received from the source serving node to inactive.

The subscription may be maintained during the life of PDU Session, regardless of the UP activation state of PDU Session (i.e. whether UP connection of the PDU Session is activated or not).

SMF may determine a new area of interest, and send a new subscription to the AMF with the new area of interest.

SMF un-subscribes to "UE mobility event notification" service when PDU Session is released.

5.6.12 Use of Network Instance

The SMF may provide a Network Instance to the UPF in FAR and/or PDR via N4 Session Establishment or N4 Modification procedures.

NOTE 1: a Network Instance can be defined e.g. to separate IP domains, e.g. when a UPF is connected to 5G-ANs in different IP domains, overlapping UE IP addresses assigned by multiple Data Networks, transport network isolation in the same PLMN, etc.

NOTE 2: As the SMF can provide over N2 the Network Instance it has selected for the N3 CN Tunnel Info, the 5G AN does not need to provide Network Instance to the 5GC.

The SMF determines the Network Instance based on local configuration.

The SMF may determine the Network Instance for N3 and N9 interfaces, taking into account e.g. UE location, registered PLMN ID of UE, S-NSSAI of the PDU Session.

The SMF may determine the Network Instance for N6 interface taking into account e.g. (DNN, S-NSSAI) of the PDU Session.

The SMF may determine the Network Instance for N19 interface taking into account e.g. the (DNN, S-NSSAI) identifying a 5G VN group.

NOTE 3: As an example, the UPF can use the Network Instance included in the FAR, together with other information such as Outer header creation (IP address part) and Destination interface in the FAR, to determine the interface in UPF (e.g. VPN or Layer 2 technology) for forwarding of the traffic.

5.6.13 Always-on PDU session

An always-on PDU Session is a PDU Session for which User Plane resources have to be activated during every transition from CM-IDLE mode to CM-CONNECTED state.

Based on an indication from upper layers, a UE may request to establish a PDU Session as an always-on PDU Session. The SMF decides whether the PDU Session can be established as an always-on PDU Session. In Home Routed roaming case, based on local policies, the V-SMF shall be involved to determine whether the PDU Session can be established as an always-on PDU Session.

If the UE requests the 5GC to modify a PDU Session, which was established in EPS, to an always-on PDU Session after the first inter-system change from EPS to 5GS, the SMF decides whether the PDU Session can be established as an always-on PDU Session based on the procedure described above.

The UE shall request activation of User Plane resources for always-on PDU Sessions even if there are no pending uplink data for this PDU Session or when the Service Request is triggered for signalling only or when the Service Request is triggered for paging response only.

If the UE has one or more established PDU Sessions which are not accepted by the network as always-on PDU Sessions and the UE has no uplink user data pending to be sent for those PDU Sessions, the UE shall not request for activating User Plane resources for those PDU sessions.

5.6.14 Support of Framed Routing

Framed Routing is only defined for PDU Sessions of the IP type (IPv4, IPv6, IPv4v6) and allows to support an IP network behind a UE, such that a range of IPv4 addresses or IPv6 prefixes is reachable over a single PDU Session, e.g. for enterprise connectivity. Framed Routes are IP routes behind the UE.

A PDU Session may be associated with multiple Framed Routes. Each Framed Route refers to a range of IPv4 addresses (i.e. an IPv4 address and an IPv4 address mask) or a range of IPv6 Prefixes (i.e. an IPv6 Prefix and an IPv6 Prefix length). The set of one or more Framed Routes associated to a PDU Session is contained in the Framed Route information. The network does not send Framed Route information to the UE: devices in the network(s) behind the UE get their IP address by mechanisms out of the scope of 3GPP specifications. See RFC 2865 [73], RFC 3162 [74].

Framed Route information is provided by the SMF to the UPF (acting as PSA) as part of Packet Detection Rule (PDR, see clause 5.8.2.11.3) related with the network side (N6) of the UPF.

The Framed Route information may be provided to the SMF by:

- the DN-AAA server as part of PDU Session Establishment authentication/authorization by a DN-AAA server (as defined in clause 5.6.6); or by
- Session Management Subscription data associated with DNN and S-NSSAI sent by UDM (as defined in TS 23.502 [3] clause 5.2.3.3.1).

  If the SMF receives Framed Route information both from DN-AAA and from UDM, the information received from DN-AAA takes precedence and supersedes the information received from UDM.

The IPv4 address / IPv6 Prefix allocated to the UE as part of the PDU Session establishment (e.g. delivered in NAS PDU Session Establishment Accept) may belong to one of the Framed Routes associated with the PDU Session or may be dynamically allocated outside of such Framed Routes.

If PCC applies to the PDU Session, at PDU Session establishment the SMF reports to the PCF the Framed Route information corresponding to the PDU Session (as described in clause 6.1.3.5 of TS 23.503 [45]). In this case, in order to support session binding, the PCF may further report to the BSF the Framed Route information corresponding to the PDU Session (as described in clause 6.1.2.2 of TS 23.503 [45]).

If the UDM or DN-AAA updates the Framed Route information during the lifetime of the PDU Session, the SMF releases the PDU Session and may include in the release request an indication for the UE to re-establish the PDU Session.

5.7 QoS model

5.7.1 General Overview

5.7.1.1 QoS Flow

The 5G QoS model is based on QoS Flows. The 5G QoS model supports both QoS Flows that require guaranteed flow bit rate (GBR QoS Flows) and QoS Flows that do not require guaranteed flow bit rate (Non-GBR QoS Flows). The 5G QoS model also supports Reflective QoS (see clause 5.7.5).

The QoS Flow is the finest granularity of QoS differentiation in the PDU Session. A QoS Flow ID (QFI) is used to identify a QoS Flow in the 5G System. User Plane traffic with the same QFI within a PDU Session receives the same traffic forwarding treatment (e.g. scheduling, admission threshold). The QFI is carried in an encapsulation header on N3 (and N9) i.e. without any changes to the e2e packet header. QFI shall be used for all PDU Session Types. The QFI shall be unique within a PDU Session. The QFI may be dynamically assigned or may be equal to the 5QI (see clause 5.7.2.1).

Within the 5GS, a QoS Flow is controlled by the SMF and may be preconfigured, or established via the PDU Session Establishment procedure (see TS 23.502 [3], clause 4.3.2), or the PDU Session Modification procedure (see TS 23.502 [3] clause 4.3.3.

Any QoS Flow is characterised by:

- A QoS profile provided by the SMF to the AN via the AMF over the N2 reference point or preconfigured in the AN;

- One or more QoS rule(s) and optionally QoS Flow level QoS parameters (as specified in TS 24.501 [47]) associated with these QoS rule(s) which can be provided by the SMF to the UE via the AMF over the N1 reference point and/or derived by the UE by applying Reflective QoS control; and

- One or more UL and DL PDR(s) provided by the SMF to the UPF.

Within the 5GS, a QoS Flow associated with the default QoS rule is required to be established for a PDU Session and remains established throughout the lifetime of the PDU Session. This QoS Flow should be a Non-GBR QoS Flow (further details are described in clause 5.7.2.7).

A QoS Flow is associated with QoS requirements as specified by QoS parameters and QoS characteristics.

NOTE: The above QoS Flow provides the UE with connectivity throughout the lifetime of the PDU Session. Possible interworking with EPS motivates the recommendation for this QoS Flow to be of type Non-GBR.

5.7.1.2 QoS Profile

A QoS Flow may either be 'GBR' or 'Non-GBR' depending on its QoS profile. The QoS profile of a QoS Flow is sent to the (R)AN and it contains QoS parameters as described below (details of QoS parameters are described in clause 5.7.2):

- For each QoS Flow, the QoS profile shall include the QoS parameters:
  - 5G QoS Identifier (5QI); and
  - Allocation and Retention Priority (ARP).
- For each Non-GBR QoS Flow only, the QoS profile may also include the QoS parameter:
  - Reflective QoS Attribute (RQA).
- For each GBR QoS Flow only, the QoS profile shall also include the QoS parameters:
  - Guaranteed Flow Bit Rate (GFBR) - UL and DL; and
  - Maximum Flow Bit Rate (MFBR) - UL and DL; and
- In the case of a GBR QoS Flow only, the QoS profile may also include one or more of the QoS parameters:
  - Notification control;
  - Maximum Packet Loss Rate - UL and DL.

NOTE: In this Release of the specification, the Maximum Packet Loss Rate (UL, DL) is only provided for a GBR QoS flow belonging to voice media.

Each QoS profile has one corresponding QoS Flow identifier (QFI) which is not included in the QoS profile itself.

The usage of a dynamically assigned 5QI for a QoS Flow requires in addition the signalling of the complete 5G QoS characteristics (described in clause 5.7.3) as part of the QoS profile.

When a standardized or pre-configured 5QI is used for a QoS Flow, some of the 5G QoS characteristics may be signalled as part of the QoS profile (as described in clause 5.7.3).

5.7.1.2a Alternative QoS Profile

The Alternative QoS Profile(s) can be optionally provided for a GBR QoS Flow with Notification control enabled. If the corresponding PCC rule contains the related information (as described in TS 23.503 [45]), the SMF shall provide, in addition to the QoS profile, a prioritized list of Alternative QoS Profile(s) to the NG-RAN. If the SMF provides a new prioritized list of Alternative QoS Profile(s) to the NG-RAN (if the corresponding PCC rule information changes), the NG-RAN shall replace any previously stored list with it.

An Alternative QoS Profile represents a combination of QoS parameters PDB, PER and GFBR to which the application traffic is able to adapt.

NOTE: There is no requirement that the GFBR monotonically decreases, nor that the PDB or PER monotonically increase as the Alternative QoS Profiles become less preferred.

When the NG-RAN sends a notification to the SMF that the QoS profile is not fulfilled, the NG-RAN shall, if the currently fulfilled values match an Alternative QoS Profile, include also the reference to the Alternative QoS Profile to indicate the QoS that the NG-RAN currently fulfils (see clause 5.7.2.4). The NG-RAN shall enable the SMF to determine when an NG-RAN node supports the Alternative QoS feature but cannot fulfil even the least preferred Alternative QoS Profile.

5.7.1.3 Control of QoS Flows

The following options are supported to control QoS Flows:

1) For Non-GBR QoS Flows, and when standardized 5QIs or pre-configured 5QIs are used and when the 5QI is within the range of the QFI (i.e. a value less than 64), the 5QI value may be used as the QFI of the QoS Flow.

   (a) A default ARP shall be pre-configured in the AN; or

   (b)The ARP and the QFI shall be sent to RAN over N2 at PDU Session Establishment or at PDU Session Modification and when NG-RAN is used every time the User Plane of the PDU Session is activated; and

2) For all other cases (including GBR and Non-GBR QoS Flows), a dynamically assigned QFI shall be used. The 5QI value may be a standardized, pre-configured or dynamically assigned. The QoS profile and the QFI of a QoS Flow shall be provided to the (R)AN over N2 at PDU Session Establishment/Modification and when NG-RAN is used every time the User Plane of the PDU Session is activated.

Only options 1b and 2 may apply to 3GPP ANs. Options 1a, 1b and 2 may apply to Non-3GPP access.

NOTE: Pre-configured 5QI values cannot be used when the UE is roaming.

5.7.1.4 QoS Rules

The UE performs the classification and marking of UL User plane traffic, i.e. the association of UL traffic to QoS Flows, based on QoS rules. These QoS rules may be explicitly provided to the UE (i.e. explicitly signalled QoS rules using the PDU Session Establishment/Modification procedure), pre-configured in the UE or implicitly derived by the UE by applying Reflective QoS (see clause 5.7.5). A QoS rule contains the QFI of the associated QoS Flow, a Packet Filter Set (see clause 5.7.6) and a precedence value (see clause 5.7.1.9). An explicitly signalled QoS rule contains a QoS rule identifier which is unique within the PDU Session and is generated by SMF.

There can be more than one QoS rule associated with the same QoS Flow (i.e. with the same QFI).

When the UE informs the network about the number of supported Packet Filters for signalled QoS rules for the PDU Session (during the PDU Session Establishment procedure or using the PDU Session Modification procedure as described in clause 5.17.2.2.2 after the first inter-system change from EPS to 5GS for a PDU Session established in EPS and transferred from EPS with N26 interface), the SMF shall ensure that the sum of the Packet Filters used by all signalled QoS rules for a PDU Session does not exceed the number indicated by the UE.

A default QoS rule is required to be sent to the UE for every PDU Session establishment and it is associated with a QoS Flow. For IP type PDU Session or Ethernet type PDU Session, the default QoS rule is the only QoS rule of a PDU Session which may contain a Packet Filter Set that allows all UL packets, and in this case, the highest precedence value shall be used for the QoS rule.

NOTE 2: How the UE evaluates UL packets against the Packet Filter Set in a QoS rule is described in clause 5.7.1.5.

NOTE 3: The QoS rule pre-configured in the UE is only used together with option 1a for control QoS Flows as described in clause 5.7.1.3. How to keep the consistency of QFI and Packet Filter Set between UE and network is out of scope in this release of the specification.

For Unstructured type PDU Session, the default QoS rule does not contain a Packet Filter Set, and in this case the default QoS rule defines the treatment of all packets in the PDU Session.

As long as the default QoS rule does not contain a Packet Filter Set or contains a Packet Filter Set that allows all UL packets, Reflective QoS should not be applied for the QoS Flow which the default QoS rule is associated with and the RQA should not be sent for this QoS Flow.

5.7.1.5 QoS Flow mapping

The SMF performs the binding of PCC rules to QoS Flows based on the QoS and service requirements (as defined in TS 23.503 [45]). The SMF assigns the QFI for a new QoS Flow and derives its QoS profile, corresponding UPF instructions and QoS Rule(s) from the PCC rule(s) bound to the QoS Flow and other information provided by the PCF.

When applicable, the SMF provides the following information for the QoS Flow to the (R)AN:

- QFI;
- QoS profile as described in clause 5.7.1.2.
- optionally, Alternative QoS Profile(s) as described in clause 5.7.1.2a;

For each PCC rule bound to a QoS Flow, the SMF provides the following information to the UPF enabling classification, bandwidth enforcement and marking of User Plane traffic (the details are described in clause 5.8):

- a DL PDR containing the DL part of the SDF template;
- an UL PDR containing the UL part of the SDF template;

NOTE 1: If a DL PDR for an bidirectional SDF is associated with a QoS Flow other than the one associated with the default QoS rule and the UE has not received any instruction to use this QoS Flow for the SDF in uplink direction (i.e. neither a corresponding QoS rule is sent to the UE nor the Reflective QoS Indication is set in the PCC rule), it means that the UL PDR for the same SDF has to be associated with the QoS Flow associated with the default QoS rule.

- the PDR precedence value (see clause 5.7.1.9) for both PDRs is set to the precedence value of the PCC rule;
- QoS related information (e.g. MBR for an SDF, GFBR and MFBR for a GBR QoS Flow) as described in clause 5.8.2;
- the corresponding packet marking information (e.g. the QFI, the transport level packet marking value (e.g. the DSCP value of the outer IP header);
- optionally, the Reflective QoS Indication is included in the QER associated with the DL PDR (as described in clause 5.7.5.3).

For each PCC rule bound to a QoS Flow, when applicable, the SMF generates an explicitly signalled QoS rule (see clause 5.7.1.4) according to the following principles and provides it to the UE together with an add operation:

- A unique (for the PDU Session) QoS rule identifier is assigned;
- The QFI in the QoS rule is set to the QFI of the QoS Flow to which the PCC rule is bound;
- The Packet Filter Set of the QoS rule is generated from the UL SDF filters and optionally the DL SDF filters of the PCC rule (but only from those SDF filters that have an indication for being signalled to the UE, as defined in TS 23.503 [45]);
- The QoS rule precedence value is set to the precedence value of the PCC rule for which the QoS rule is generated;
- for a dynamically assigned QFI, the QoS Flow level QoS parameters (e.g. 5QI, GFBR, MFBR, Averaging Window, see TS 24.501 [47]) are signalled to UE in addition to the QoS rule(s) associated to the QoS Flow. The QoS Flow level QoS parameters (i.e. GFBR and MFBR) of an existing QoS Flow may be updated based on the MBR and GBR information received in the PCC rule (MBR and GBR per SDF are not provided to UE over N1) or, if the PCF has not indicated differently, when Notification control or handover related signalling indicates that the QoS parameter the NG-RAN is currently fulfilling for the QoS Flow have changed (see clause 5.7.2.4).

Changes in the binding of PCC rules to QoS Flows as well as changes in the PCC rules or other information provided by the PCF can require QoS Flow changes which the SMF has to provide to (R)AN, UPF and/or UE. In the case of

changes in the explicitly signalled QoS rules associated to a QoS Flow, the SMF provides the explicitly signalled QoS rules and their operation (i.e. add/modify/delete) to the UE.

NOTE 2: The SMF cannot provide, update or remove pre-configured QoS rules or UE derived QoS rules.

The principle for classification and marking of User Plane traffic and mapping of QoS Flows to AN resources is illustrated in Figure 5.7.1.5-1.

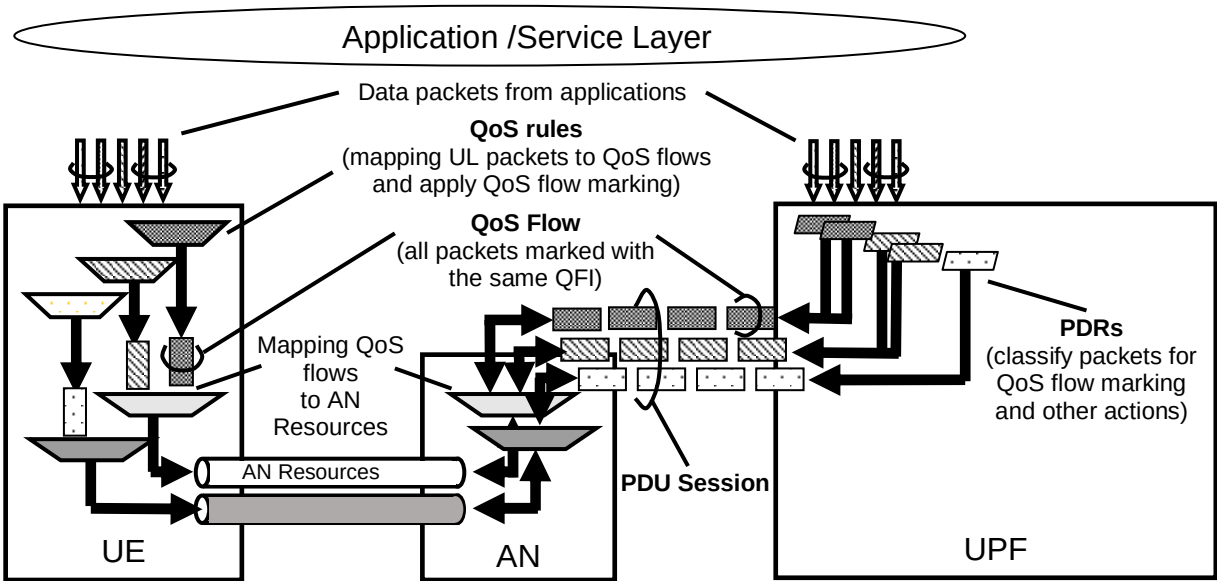


Figure 5.7.1.5-1: The principle for classification and User Plane marking for QoS Flows and mapping to AN Resources

In DL, incoming data packets are classified by the UPF based on the Packet Filter Sets of the DL PDRs in the order of their precedence (without initiating additional N4 signalling). The UPF conveys the classification of the User Plane traffic belonging to a QoS Flow through an N3 (and N9) User Plane marking using a QFI. The AN binds QoS Flows to AN resources (i.e. Data Radio Bearers of in the case of 3GPP RAN). There is no strict 1:1 relation between QoS Flows and AN resources. It is up to the AN to establish the necessary AN resources that QoS Flows can be mapped to, and to release them. The AN shall indicate to the SMF when the AN resources onto which a QoS Flow is mapped are released.

If no matching DL PDR is found, the UPF shall discard the DL data packet.

In UL:

- For a PDU Session of Type IP or Ethernet, the UE evaluates UL packets against the UL Packet Filters in the Packet Filter Set in the QoS rules based on the precedence value of QoS rules in increasing order until a matching QoS rule (i.e. whose Packet Filter matches the UL packet) is found.
- If no matching QoS rule is found, the UE shall discard the UL data packet.
- For a PDU Session of Type Unstructured, the default QoS rule does not contain a Packet Filter Set and allows all UL packets.

NOTE 3: Only the default QoS rule exist for a PDU Session of Type Unstructured.

The UE uses the QFI in the corresponding matching QoS rule to bind the UL packet to a QoS Flow. The UE then binds QoS Flows to AN resources.

5.7.1.6 DL traffic

The following characteristics apply for processing of DL traffic:

- UPF maps User Plane traffic to QoS Flows based on the PDRs.
- UPF performs Session-AMBR enforcement as specified in clause 5.7.1.8 and performs counting of packets for charging.

- UPF transmits the PDUs of the PDU Session in a single tunnel between 5GC and (R)AN, the UPF includes the QFI in the encapsulation header. In addition, UPF may include an indication for Reflective QoS activation in the encapsulation header.

- UPF performs transport level packet marking in DL on a per QoS Flow basis. The UPF uses the transport level packet marking value provided by the SMF (as described in clause 5.8.2.7).

- (R)AN maps PDUs from QoS Flows to access-specific resources based on the QFI and the associated 5G QoS profile, also taking into account the N3 tunnel associated with the DL packet.

NOTE: Packet Filters are not used for the mapping of QoS Flows onto access-specific resources in (R)AN.

- If Reflective QoS applies, the UE creates a new derived QoS rule as defined in clause 5.7.5.2.

5.7.1.7 UL Traffic

Following characteristics apply for processing of UL traffic:

- UE uses the stored QoS rules to determine mapping between UL User Plane traffic and QoS Flows. UE marks the UL PDU with the QFI of the QoS rule containing the matching Packet Filter and transmits the UL PDUs using the corresponding access specific resource for the QoS Flow based on the mapping provided by (R)AN. For NG-RAN, the UL behaviour is specified in TS 38.300 [27] clause 10.5.2.

- (R)AN transmits the PDUs over N3 tunnel towards UPF. When passing an UL packet from (R)AN to CN, the (R)AN includes the QFI value, in the encapsulation header of the UL PDU, and selects the N3 tunnel.

- (R)AN performs transport level packet marking in the UL on a per QoS Flow basis with a transport level packet marking value that is determined based on the 5QI, the Priority Level (if explicitly signalled) and the ARP priority level of the associated QoS Flow.

- UPF verifies whether QFIs in the UL PDUs are aligned with the QoS Rules provided to the UE or implicitly derived by the UE in the case of Reflective QoS).

- UPF and UE perform Session-AMBR enforcement as specified in clause 5.7.1.8 and the UPF performs counting of packets for charging.

5.7.1.8 AMBR/MFBR enforcement and rate limitation

UL and DL Session-AMBR (see clause 5.7.2.6) shall be enforced by the UPF, if the UPF receives the Session-AMBR values from the SMF as described in clause 5.8.2.7 and clause 5.8.2.11.4.

For UL Classifier PDU Sessions, UL and DL Session-AMBR (see clause 5.7.2.6) shall be enforced in the SMF selected UPF that supports the UL Classifier functionality. In addition, the DL Session-AMBR shall be enforced separately in every UPF that terminates the N6 interface (i.e. without requiring interaction between the UPFs) (see clause 5.6.4).

For multi-homed PDU Sessions, UL and DL Session-AMBR shall be enforced in the UPF that supports the Branching Point functionality. In addition, the DL Session-AMBR shall be enforced separately in every UPF that terminates the N6 interface (i.e. without requiring interaction between the UPFs) (see clause 5.6.4).

NOTE: The DL Session-AMBR is enforced in every UPF terminating the N6 interface to reduce unnecessary transport of traffic which may be discarded by the UPF performing the UL Classifier/Branching Point functionality due to the amount of the DL traffic for the PDU Session exceeding the DL Session-AMBR. Discarding DL packets in the UL Classifier/Branching Point could cause erroneous PDU counting for support of charging

The (R)AN shall enforce UE-AMBR (see clause 5.7.2.6) in UL and DL per UE for Non-GBR QoS Flows.

The UE shall perform UL rate limitation on PDU Session basis for Non-GBR traffic using Session-AMBR, if the UE receives a Session-AMBR.

MBR per SDF is mandatory for GBR QoS Flows but optional for Non-GBR QoS Flows. The MBR is enforced in the UPF.

The MFBR is enforced in the UPF in the Downlink for GBR QoS Flows. The MFBR is enforced in the (R)AN in the Downlink and Uplink for GBR QoS Flows. For non-3GPP access, the UE should enforce MFBR in the Uplink for GBR QoS Flows.

The QoS control for Unstructured PDUs is performed at the PDU Session level and in this Release of the specification there is only support for maximum of one 5G QoS Flow per PDU Session of Type Unstructured.

When a PDU Session is set up for transferring unstructured PDUs, SMF provides the QFI which will be applied to any packet of the PDU Session to the UPF and UE.

5.7.1.9 Precedence Value

The QoS rule precedence value and the PDR precedence value determine the order in which a QoS rule or a PDR, respectively, shall be evaluated. The evaluation of the QoS rules or PDRs is performed in increasing order of their precedence value.

5.7.2 5G QoS Parameters

5.7.2.1 5QI

A 5QI is a scalar that is used as a reference to 5G QoS characteristics defined in clause 5.7.4, i.e. access node-specific parameters that control QoS forwarding treatment for the QoS Flow (e.g. scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, etc.).

Standardized 5QI values have one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in Table 5.7.4-1.

The 5G QoS characteristics for pre-configured 5QI values are pre-configured in the AN.

Standardized or pre-configured 5G QoS characteristics, are indicated through the 5QI value, and are not signalled on any interface, unless certain 5G QoS characteristics are modified as specified in clauses 5.7.3.3, 5.7.3.4, 5.7.3.6, and 5.7.3.7.

The 5G QoS characteristics for QoS Flows with dynamically assigned 5QI are signalled as part of the QoS profile.

NOTE: On N3, each PDU (i.e. in the tunnel used for the PDU Session) is associated with one 5QI via the QFI carried in the encapsulation header.

5.7.2.2 ARP

The QoS parameter ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. This allows deciding whether a QoS Flow establishment/modification/handover may be accepted or needs to be rejected in the case of resource limitations (typically used for admission control of GBR traffic). It may also be used to decide which existing QoS Flow to pre-empt during resource limitations, i.e. which QoS Flow to release to free up resources.

The ARP priority level defines the relative importance of a QoS Flow. The range of the ARP priority level is 1 to 15 with 1 as the highest level of priority.

The ARP priority levels 1-8 should only be assigned to QoS Flows for services that are authorized to receive prioritized treatment within an operator domain (i.e. that are authorized by the serving network). The ARP priority levels 9-15 may be assigned to QoS Flows for services that are authorized by the home network and thus applicable when a UE is roaming.

NOTE: This ensures that future releases may use ARP priority level 1-8 to indicate e.g. emergency and other priority services within an operator domain in a backward compatible manner. This does not prevent the use of ARP priority level 1-8 in roaming situation in the case that appropriate roaming agreements exist that ensure a compatible use of these priority levels.

The ARP pre-emption capability defines whether a QoS Flow may get resources that were already assigned to another QoS Flow with a lower ARP priority level. The ARP pre-emption vulnerability defines whether a QoS Flow may lose

the resources assigned to it in order to admit a QoS Flow with higher ARP priority level. The ARP pre-emption capability and the ARP pre-emption vulnerability shall be either set to 'enabled' or 'disabled'.

The ARP pre-emption vulnerability of the QoS Flow which the default QoS rule is associated with should be set appropriately to minimize the risk of a release of this QoS Flow.

The details of how the SMF sets the ARP for a QoS Flow are further described in clause 5.7.2.7.

5.7.2.3 RQA

The Reflective QoS Attribute (RQA) is an optional parameter which indicates that certain traffic (not necessarily all) carried on this QoS Flow is subject to Reflective QoS. Only when the RQA is signalled for a QoS Flow, the (R)AN enables the transfer of the RQI for AN resource corresponding to this QoS Flow. The RQA may be signalled to NG-RAN via the N2 reference point at UE context establishment in NG-RAN and at QoS Flow establishment or modification.

5.7.2.4 Notification control

5.7.2.4.1 General

The QoS Parameter Notification control indicates whether notifications are requested from the NG-RAN when the "GFBR can no longer (or can again) be guaranteed" for a QoS Flow during the lifetime of the QoS Flow. Notification control may be used for a GBR QoS Flow if the application traffic is able to adapt to the change in the QoS (e.g., if the AF is capable to trigger rate adaptation).

The SMF shall only enable Notification control when the QoS Notification Control parameter is set in the PCC rule (received from the PCF) that is bound to the QoS Flow. The Notification control parameter is signalled to the NG-RAN as part of the QoS profile.

5.7.2.4.1a Notification Control without Alternative QoS Profiles

If, for a given GBR QoS Flow, Notification control is enabled and the NG-RAN determines that the GFBR, the PDB or the PER of the QoS profile cannot be fulfilled, NG-RAN shall send a notification towards SMF that the "GFBR can no longer be guaranteed". Furthermore, the NG-RAN shall keep the QoS Flow (i.e. while the NG-RAN is not fulfilling the requested QoS profile for this QoS Flow), unless specific conditions at the NG-RAN require the release of the NG-RAN resources for this GBR QoS Flow, e.g. due to Radio link failure or RAN internal congestion. The NG-RAN should try to fulfil the GFBR, the PDB and the PER of the QoS profile again.

NOTE 1: NG-RAN can decide that the "GFBR can no longer be guaranteed" based on, e.g. measurements like queuing delay or system load.

Upon receiving a notification from the NG-RAN that the "GFBR can no longer be guaranteed", the SMF may forward the notification to the PCF, see TS 23.503 [45].

When the NG-RAN determines that the GFBR, the PDB and the PER of the QoS profile can be fulfilled again for a QoS Flow (for which a notification that the "GFBR can no longer be guaranteed" has been sent), the NG-RAN shall send a notification, informing the SMF that the "GFBR can be guaranteed" again and the SMF may forward the notification to the PCF, see TS 23.503 [45]. The NG-RAN shall send a subsequent notification that the "GFBR can no longer be guaranteed" whenever necessary.

NOTE 2: It is assumed that NG-RAN implementation will apply some hysteresis before determining that the "GFBR can be guaranteed again" and therefore a frequent signalling of "GFBR can be guaranteed again" followed by "GFBR can no longer be guaranteed" is not expected.

NOTE 3: If the QoS Flow is modified, the NG-RAN restarts the check whether the "GFBR can no longer be guaranteed" according to the updated QoS profile. If the Notification control parameter is not included in the updated QoS profile, the Notification control is disabled.

During a handover, the Source NG-RAN does not inform the Target NG-RAN about whether the Source NG-RAN has sent a notification for a QoS Flow that the "GFBR can no longer be guaranteed". The Target NG-RAN performs admission control rejecting any QoS Flows for which resources cannot be permanently allocated. The accepted QoS Flows are included in the N2 Path Switch Request or N2 Handover Request Acknowledge message from the NG-RAN

to the AMF. The SMF shall interpret the fact that a QoS Flow is listed as transferred QoS Flow in the Nsmf_PDUSession_UpdateSMContext Request received from the AMF as a notification that "GFBR can be guaranteed again" for this QoS Flow unless the SMF is also receiving a reference to an Alternative QoS Profile for this QoS Flow (which is described in clause 5.7.2.4.2). After the handover is successfully completed, the Target NG-RAN shall send a subsequent notification that the "GFBR can no longer be guaranteed" for such a QoS Flow whenever necessary. If the SMF has previously notified the PCF that the "GFBR can no longer be guaranteed" and the SMF does not receive an explicit notification that the "GFBR can no longer be guaranteed" for that QoS Flow from the Target NG-RAN within a configured time, the SMF shall notify the PCF that the "GFBR can be guaranteed again".

5.7.2.4.1b Notification control with Alternative QoS Profiles

If, for a given GBR QoS Flow, Notification control is enabled and the NG-RAN has received a list of Alternative QoS Profile(s) for this QoS Flow and supports the Alternative QoS Profile handling, the following shall apply:

1) If the NG-RAN determines that the GFBR, the PDB or the PER of the QoS profile cannot be fulfilled, NG-RAN shall send a notification towards SMF that the "GFBR can no longer be guaranteed". Before sending a notification that the "GFBR can no longer be guaranteed" towards the SMF, the NG-RAN shall check whether the the GFBR, the PDB and the PER that the NG-RAN currently fulfils match any of the Alternative QoS Profile(s) in the indicated priority order. If there is a match, the NG-RAN shall indicate the reference to the matching Alternative QoS Profile with the highest priority together with the notification to the SMF.

   If there is no match, the NG-RAN shall send a notification that the "GFBR can no longer be guaranteed" towards the SMF without referencing any of the Alternative QoS Profile(s) (unless specific conditions at the NG-RAN require the release of the NG-RAN resources for this GBR QoS Flow, e.g. due to Radio link failure or RAN internal congestion).

2) If a notification that the "GFBR can no longer be guaranteed" has been sent to the SMF and the NG-RAN determines that the currently fulfilled GFBR, PDB or PER are different (better or worse) from the situation indicated in the last notification, the NG-RAN shall send a further notification to the SMF and indicate the currently fulfilled situation.

NOTE 1: The fulfilled situation is either the QoS Profile, an Alternative QoS Profile, or an indication that the lowest priority Alternative QoS Profile cannot be fulfilled.

3)- The NG-RAN should always try to fulfil the QoS profile and any Alternative QoS Profile that has higher priority than the currently fulfilled situation.

NOTE 2: In order to avoid a too frequent signalling to the SMF, it is assumed that NG-RAN implementation can apply hysteresis (e.g., via a configurable time interval) before notifying the SMF that the currently fulfilled values match the QoS Profile or a different Alternative QoS Profile of higher priority. It is also assumed that the PCF has ensured that the QoS values within the different Alternative QoS Profile(s) are not too close to each other.

4) Upon receiving a notification from the NG-RAN, the SMF may inform the PCF. If it does so, the SMF shall indicate the currently fulfilled situation to the PCF. See TS 23.503 [45].

5)- If the PCF has not indicated differently, the SMF uses NAS signalling (that is sent transparently through the RAN) to inform the UE about changes in the QoS parameters (i.e., 5QI, GFBR, MFBR) that the NG-RAN is currently fulfilling for the QoS Flow after Notification control has occurred.

5.7.2.4.2 Usage of Notification control with Alternative QoS Profiles at handover

During handover, the prioritized list of Alternative QoS Profile(s) (if available) is provided to the Target NG-RAN per QoS Flow in addition to the QoS profile. If the Target NG-RAN is not able to guarantee the GFBR, the PDB and the PER included in the QoS profile and if Alternative QoS Profiles are provided to the Target NG-RAN and the Target NG-RAN supports Alternative QoS Profiles, the Target NG-RAN checks whether the GFBR, the PDB and the PER values that it can fulfil match any of the Alternative QoS Profile(s) taking the priority order into account. If there is a match between one of the Alternative QoS Profiles and the GFBR, the PDB and the PER values that Target NG-RAN can fulfil, the Target NG-RAN shall accept the QoS Flow and indicate the reference to that Alternative QoS Profile to the Source NG-RAN.

If there is no match to any Alternative QoS Profile, the Target NG-RAN rejects QoS Flows for which the Target NG-RAN is not able to guarantee the GFBR, the PDB and the PER included in the QoS profile.

After the handover is completed and a QoS Flow has been accepted by the Target NG-RAN based on an Alternative QoS Profile, the Target NG-RAN shall treat this QoS Flow in the same way as if it had sent a notification that the "GFBR can no longer be guaranteed" with a reference to that Alternative QoS Profile to the SMF (as described in clause 5.7.2.4.1b).

If a QoS Flow has been accepted by the Target NG-RAN based on an Alternative QoS Profile, the reference to the matching Alternative QoS Profile is provided from the Target NG-RAN to the AMF (which forwards the message to the SMF) during the Xn and N2 based handover procedures as described in TS 23.502 [3]. After the handover is completed successfully, the SMF shall send a notification to the PCF that the "GFBR can no longer be guaranteed" for a QoS Flow (see TS 23.503 [45] for details) if the SMF has received a reference to an Alternative QoS Profile and this reference indicates a change in the previously notified state of this QoS Flow. If the PCF has not indicated differently, the SMF shall also use NAS signalling (that is sent transparently through the RAN) to inform the UE about the QoS parameters (i.e. 5QI, GFBR, MFBR) corresponding to the new state of the QoS Flow.

NOTE: A state change for the QoS Flow comprises a change from QoS profile fulfilled to Alternative QoS Profile fulfilled as well as the state change between fulfilled Alternative QoS Profiles.

If a QoS Flow has been accepted by the Target NG-RAN based on the QoS Profile, the SMF shall interpret the fact that a QoS Flow is listed as transferred QoS Flow in the message received from the AMF as a notification that "GFBR can be guaranteed again" for this QoS Flow. After the handover is successfully completed, the Target NG-RAN performs as described in clause 5.7.2.4.1b. If the SMF has previously notified the PCF that the "GFBR can no longer be guaranteed" and the SMF does not receive an explicit notification that the "GFBR can no longer be guaranteed" for that QoS Flow from the Target NG-RAN within a configured time, the SMF shall notify the PCF that the "GFBR can be guaranteed again".

If a QoS Flow has been accepted by the Target NG-RAN and SMF did not receive from the Target NG-RAN a reference to any Alternative QoS Profile and the SMF has previously informed the UE about QoS parameters corresponding to any of the Alternative QoS Profile(s), the SMF shall use NAS signalling to inform the UE about the QoS parameters corresponding to the QoS Profile.

5.7.2.5 Flow Bit Rates

For GBR QoS Flows only, the following additional QoS parameters exist:

- Guaranteed Flow Bit Rate (GFBR) - UL and DL;
- Maximum Flow Bit Rate (MFBR) -- UL and DL.

The GFBR denotes the bit rate that is guaranteed to be provided by the network to the QoS Flow over the Averaging Time Window. The MFBR limits the bit rate to the highest bit rate that is expected by the QoS Flow (e.g. excess traffic may get discarded or delayed by a rate shaping or policing function at the UE, RAN, UPF). Bit rates above the GFBR value and up to the MFBR value, may be provided with relative priority determined by the Priority Level of the QoS Flows (see clause 5.7.3.3).

GFBR and MFBR are signalled to the (R)AN in the QoS Profile and signalled to the UE as QoS Flow level QoS parameter (as specified in TS 24.501 [47]) for each individual QoS Flow.

NOTE 1: The GFBR is recommended as the lowest acceptable service bitrate where the service will survive.

NOTE 2: For each QoS Flow of Delay Critical GBR resource type, the SMF can ensure that the GFBR of the QoS Flow can be achieved with the MDBV of the QoS Flow using the QoS Flow binding functionality described in clause 6.1.3.2.4 in TS 23.503 [45].

NOTE 3: The network can set MFBR larger than GFBR for a particular QoS Flow based on operator policy and the knowledge of the end point capability, i.e. support of rate adaptation at application / service level.

5.7.2.6 Aggregate Bit Rates

Each PDU Session of a UE is associated with the following aggregate rate limit QoS parameter:

- per Session Aggregate Maximum Bit Rate (Session-AMBR).

The Session-AMBR is signalled to the appropriate UPF entity/ies to the UE and to the (R)AN (to enable the calculation of the UE-AMBR). The Session-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-

GBR QoS Flows for a specific PDU Session. The Session-AMBR is measured over an AMBR averaging window which is a standardized value. The Session-AMBR is not applicable to GBR QoS Flows.

Each UE is associated with the following aggregate rate limit QoS parameter:

- per UE Aggregate Maximum Bit Rate (UE-AMBR).

The UE-AMBR limits the aggregate bit rate that can be expected to be provided across all Non-GBR QoS Flows of a UE. Each (R)AN shall set its UE-AMBR to the sum of the Session-AMBR of all PDU Sessions with active user plane to this (R)AN up to the value of the received UE-AMBR from AMF. The UE-AMBR is a parameter provided to the (R)AN by the AMF based on the value of the subscribed UE-AMBR retrieved from UDM or the dynamic serving network UE-AMBR retrieved from PCF (e.g. for roaming subscriber). The AMF provides the UE-AMBR provided by PCF to (R)AN if available. The UE-AMBR is measured over an AMBR averaging window which is a standardized value. The UE-AMBR is not applicable to GBR QoS Flows.

NOTE: The AMBR averaging window is only applied to Session-AMBR and UE-AMBR measurement and the AMBR averaging windows for Session-AMBR and UE-AMBR are standardised to the same value.

5.7.2.7 Default values

For each PDU Session Setup, the SMF retrieves the subscribed Session-AMBR values as well as the subscribed default values for the 5QI and the ARP and optionally, the 5QI Priority Level, from the UDM. The subscribed default 5QI value shall be a Non-GBR 5QI from the standardized value range.

NOTE 1: The 5QI Priority Level can be added to the subscription information to achieve an overwriting of the standardized or preconfigured 5QI Priority Level e.g. in scenarios where dynamic PCC is not deployed or the PCF is unavailable or unreachable.

The SMF may change the subscribed values for the default 5QI and the ARP and if received, the 5QI Priority Level, based on interaction with the PCF as described in TS 23.503 [45] or, if dynamic PCC is not deployed, based on local configuration, to set QoS parameters for the QoS Flow associated with the default QoS rule.

For QoS Flow(s) of the PDU Session other than the QoS Flow associated with the default QoS rule, the SMF shall set the ARP priority level, the ARP pre-emption capability and the ARP pre-emption vulnerability to the respective values in the PCC rule(s) bound to that QoS Flow (as described in TS 23.503 [45]). If dynamic PCC is not deployed, the SMF shall set the ARP priority level, the ARP pre-emption capability and the ARP pre-emption vulnerability based on local configuration.

NOTE 2: The local configuration in the SMF can e.g. make use of the subscribed value for the ARP priority level and apply locally configured values for the ARP pre-emption capability and ARP pre-emption vulnerability.

If dynamic PCC is not deployed, the SMF can have a DNN based configuration to enable the establishment of a GBR QoS Flow as the QoS Flow that is associated with the default QoS rule. This configuration contains a standardized GBR 5QI as well as GFBR and MFBR for UL and DL.

NOTE 3: Interworking with EPS is not possible for a PDU Session with a GBR QoS Flow as the QoS Flow that is associated with the default QoS rule.

The SMF may change the subscribed Session-AMBR values (for UL and/or DL), based on interaction with the PCF as described in TS 23.503 [45] or, if dynamic PCC is not deployed, based on local configuration, to set the Session-AMBR values for the PDU Session.

5.7.2.8 Maximum Packet Loss Rate

The Maximum Packet Loss Rate (UL, DL) indicates the maximum rate for lost packets of the QoS flow that can be tolerated in the uplink and downlink direction. This is provided to the QoS flow if it is compliant to the GFBR

NOTE: In this Release of the specification, the Maximum Packet Loss Rate (UL, DL) can only be provided for a GBR QoS flow belonging to voice media.

5.7.2.9 Wireline access network specific 5G QoS parameters

QoS parameters that are applicable only for or wireline access networks (W-5GAN) are specified in TS 23.316 [84].

5.7.3 5G QoS characteristics

5.7.3.1 General

This clause specifies the 5G QoS characteristics associated with 5QI. The characteristics describe the packet forwarding treatment that a QoS Flow receives edge-to-edge between the UE and the UPF in terms of the following performance characteristics:

1 Resource Type (GBR, Delay critical GBR or Non-GBR);

2 Priority Level;

3 Packet Delay Budget (including Core Network Packet Delay Budget);

4 Packet Error Rate;

5 Averaging window (for GBR and Delay-critical GBR resource type only);

6 Maximum Data Burst Volume (for Delay-critical GBR resource type only).

The 5G QoS characteristics should be understood as guidelines for setting node specific parameters for each QoS Flow e.g. for 3GPP radio access link layer protocol configurations.

Standardized or pre-configured 5G QoS characteristics, are indicated through the 5QI value, and are not signalled on any interface, unless certain 5G QoS characteristics are modified as specified in clauses 5.7.3.3, 5.7.3.4, 5.7.3.6, and 5.7.3.7.

NOTE: As there are no default values specified, pre-configured 5G QoS characteristics have to include all of the characteristics listed above.

Signalled 5G QoS characteristics are provided as part of the QoS profile and shall include all of the characteristics listed above.

5.7.3.2 Resource Type

The Resource Type determines if dedicated network resources related to a QoS Flow-level Guaranteed Flow Bit Rate (GFBR) value are permanently allocated (e.g. by an admission control function in a radio base station).

GBR QoS Flows are therefore typically authorized "on demand" which requires dynamic policy and charging control. A GBR QoS Flow uses either the GBR resource type or the Delay-critical GBR resource type. The definition of PDB and PER are different for GBR and Delay-critical GBR resource types, and the MDBV parameter applies only to the Delay-critical GBR resource type.

A Non-GBR QoS Flow may be pre-authorized through static policy and charging control. A Non-GBR QoS Flow uses only the Non-GBR resource type.

5.7.3.3 Priority Level

The Priority Level associated with 5G QoS characteristics indicates a priority in scheduling resources among QoS Flows. The lowest Priority Level value corresponds to the highest priority.

The Priority Level shall be used to differentiate between QoS Flows of the same UE, and it shall also be used to differentiate between QoS Flows from different UEs.

In the case of congestion, when all QoS requirements cannot be fulfilled for one or more QoS Flows, the Priority Level shall be used to select for which QoS Flows the QoS requirements are prioritised such that a QoS Flow with Priority Level value N is priorized over QoS Flows with higher Priority Level values (i.e. N+1, N+2, etc).In the case of no congestion, the Priority Level should be used to define the resource distribution between QoS Flows. In addition, the

scheduler may prioritize QoS Flows based on other parameters (e.g. resource type, radio condition) in order to optimize application performance and network capacity.

Every standardized 5QI is associated with a default value for the Priority Level -specified in QoS characteristics Table 5.7.4.1). Priority Level may also be signalled together with a standardized 5QI to the -R)AN, and if it is received, it shall be used instead of the default value.

Priority Level may also be signalled together with a pre-configured 5QI to the (R)AN, and if it is received, it shall be used instead of the pre-configured value.

5.7.3.4 Packet Delay Budget

The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the UE and the UPF that terminates the N6 interface. For a certain 5QI the value of the PDB is the same in UL and DL. In the case of 3GPP access, the PDB is used to support the configuration of scheduling and link layer functions (e.g. the setting of scheduling priority weights and HARQ target operating points). For GBR QoS Flows using the Delay-critical resource type, a packet delayed more than PDB is counted as lost if the data burst is not exceeding the MDBV within the period of PDB and the QoS Flow is not exceeding the GFBR. For GBR QoS Flows with GBR resource type not exceeding GFBR, 98 percent of the packets shall not experience a delay exceeding the 5QI's PDB.

The 5G Access Network Packet Delay Budget (5G-AN PDB) is determined by subtracting a static value for the Core Network Packet Delay Budget (CN PDB), which represents the delay between any UPF terminating N6 (that may possibly be selected for the PDU Session) and the 5G-AN from a given PDB.

NOTE 1: For a standardized 5QI, the static value for the CN PDB is specified in the QoS characteristics Table 5.7.4-1.

NOTE 2: For a non-standardized 5QI, the static value for the CN PDB is homogeneously configured in the network.

For GBR QoS Flows using the Delay-critical resource type, in order to obtain a more accurate delay budget PDB available for the NG-RAN, a dynamic value for the CN PDB, which represents the delay between the UPF terminating N6 for the QoS Flow and the 5G-AN, can be used. If used for a QoS Flow, the NG-RAN shall apply the dynamic value for the CN PDB instead of the static value for the CN PDB (which is only related to the 5QI). Different dynamic value for CN PDB may be configured per uplink and downlink direction.

NOTE 3: The configuration of transport network on CN tunnel can be different per UL and DL, which can be different value for CN PDB per UL and DL.

NOTE 4: It is expected that the UPF deployment ensures that the dynamic value for the CN PDB is not larger than the static value for the CN PDB. This avoids that the functionality that is based on the 5G-AN PDB (e.g. MDBV, NG-RAN scheduler) has to handle an unexpected value.

The dynamic value for the CN PDB of a Delay-critical GBR 5QI may be configured in the network in two ways:

- Configured in each NG-RAN node, based on a variety of inputs such as different IP address(es) or TEID range of UPF terminating the N3 tunnel and based on different combinations of PSA UPF to NG-RAN under consideration of any potential I-UPF, etc;

- Configured in the SMF, based on different combinations of PSA UPF to NG-RAN under consideration of any potential I-UPF. The dynamic value for the CN PDB for a particular QoS Flow shall be signalled to NG-RAN (during PDU Session Establishment, PDU Session Modification, Xn/N2 handover and the Service Request procedures) when the QoS Flow is established or the dynamic value for the CN PDB of a QoS Flow changes, e.g. when an I-UPF is inserted by the SMF.

If the NG-RAN node is configured locally with a dynamic value for the CN PDB for a Delay-critical GBR 5QI, and receives a different value via N2 signalling for a QoS Flow with the same 5QI, local configuration in RAN node determines which value takes precedence.

Services using a GBR QoS Flow and sending at a rate smaller than or equal to the GFBR can in general assume that congestion related packet drops will not occur.

NOTE 5: Exceptions (e.g. transient link outages) can always occur in a radio access system which may then lead to congestion related packet drops. Packets surviving congestion related packet dropping may still be subject to non-congestion related packet losses (see PER below).

Services using Non-GBR QoS Flows should be prepared to experience congestion-related packet drops and delays. In uncongested scenarios, 98 percent of the packets should not experience a delay exceeding the 5QI's PDB.

The PDB for Non-GBR and GBR resource types denotes a "soft upper bound" in the sense that an "expired" packet, e.g. a link layer SDU that has exceeded the PDB, does not need to be discarded and is not added to the PER. However, for a Delay critical GBR resource type, packets delayed more than the PDB are added to the PER and can be discarded or delivered depending on local decision.

5.7.3.5 Packet Error Rate

The Packet Error Rate (PER) defines an upper bound for the rate of PDUs (e.g. IP packets) that have been processed by the sender of a link layer protocol (e.g. RLC in RAN of a 3GPP access) but that are not successfully delivered by the corresponding receiver to the upper layer (e.g. PDCP in RAN of a 3GPP access). Thus, the PER defines an upper bound for a rate of non-congestion related packet losses. The purpose of the PER is to allow for appropriate link layer protocol configurations (e.g. RLC and HARQ in RAN of a 3GPP access). For every 5QI the value of the PER is the same in UL and DL. For GBR QoS Flows with Delay critical GBR resource type, a packet which is delayed more than PDB is counted as lost, and included in the PER unless the data burst is exceeding the MDBV within the period of PDB or the QoS Flow is exceeding the GFBR.

5.7.3.6 Averaging Window

Each GBR QoS Flow shall be associated with an Averaging window. The Averaging window represents the duration over which the GFBR and MFBR shall be calculated (e.g. in the (R)AN, UPF, UE).

Every standardized 5QI (of GBR and Delay-critical GBR resource type) is associated with a default value for the Averaging window (specified in QoS characteristics Table 5.7.4.1). The averaging window may also be signalled together with a standardized 5QI to the (R)AN and UPF, and if it is received, it shall be used instead of the default value.

The Averaging window may also be signalled together with a pre-configured 5QI to the (R)AN, and if it is received, it shall be used instead of the pre-configured value.

5.7.3.7 Maximum Data Burst Volume

Each GBR QoS Flow with Delay-critical resource type shall be associated with a Maximum Data Burst Volume (MDBV).

MDBV denotes the largest amount of data that the 5G-AN is required to serve within a period of 5G-AN PDB.

Every standardized 5QI (of Delay-critical GBR resource type) is associated with a default value for the MDBV (specified in QoS characteristics Table 5.7.4.1). The MDBV may also be signalled together with a standardized 5QI to the (R)AN, and if it is received, it shall be used instead of the default value.

The MDBV may also be signalled together with a pre-configured 5QI to the (R)AN, and if it is received, it shall be used instead of the pre-configured value.

5.7.4 Standardized 5QI to QoS characteristics mapping

Standardized 5QI values are specified for services that are assumed to be frequently used and thus benefit from optimized signalling by using standardized QoS characteristics. Dynamically assigned 5QI values (which require a signalling of QoS characteristics as part of the QoS profile) can be used for services for which standardized 5QI values are not defined. The one-to-one mapping of standardized 5QI values to 5G QoS characteristics is specified in table 5.7.4-1.

Table 5.7.4-1: Standardized 5QI to QoS characteristics mapping

5QI Value	Resource Type	Default Priority Level	Packet Delay Budget (NOTE 3)	Packet Error Rate	Default Maximum Data Burst Volume (NOTE 2)	Default Averaging Window	Example Services
1	GBR (NOTE 1)	20	100 ms (NOTE 11, NOTE 13)	10^{-2}	N/A	2000 ms	Conversational Voice
2		40	150 ms (NOTE 11, NOTE 13)	10^{-3}	N/A	2000 ms	Conversational Video (Live Streaming)
3		30	50 ms (NOTE 11, NOTE 13)	10^{-3}	N/A	2000 ms	Real Time Gaming, V2X messages (see TS 23.287 [121]). Electricity distribution – medium voltage, Process automation monitoring
4		50	300 ms (NOTE 11, NOTE 13)	10^{-6}	N/A	2000 ms	Non-Conversational Video (Buffered Streaming)
65 (NOTE 9, NOTE 12)		7	75 ms (NOTE 7, NOTE 8)	10^{-2}	N/A	2000 ms	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66 (NOTE 12)		20	100 ms (NOTE 10, NOTE 13)	10^{-2}	N/A	2000 ms	Non-Mission-Critical user plane Push To Talk voice
67 (NOTE 12)		15	100 ms (NOTE 10, NOTE 13)	10^{-3}	N/A	2000 ms	Mission Critical Video user plane
75 (NOTE 14)							
71		56	150 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-6}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
72		56	300 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-4}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
73		56	300 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-8}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
74		56	500 ms (NOTE 11, NOTE 15)	10^{-8}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
76		56	500 ms (NOTE 11, NOTE 13, NOTE 15)	10^{-4}	N/A	2000 ms	"Live" Uplink Streaming (e.g. TS 26.238 [76])
5	Non-GBR (NOTE 1)	10	100 ms NOTE 10, NOTE 13)	10^{-6}	N/A	N/A	IMS Signalling
6		60	300 ms (NOTE 10, NOTE 13)	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100 ms (NOTE 10, NOTE 13)	10^{-3}	N/A	N/A	Voice, Video (Live Streaming) Interactive Gaming

8		80	300 ms (NOTE 13)	10^{-6}	N/A	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		90					
69 (NOTE 9, NOTE 12)		5	60 ms (NOTE 7, NOTE 8)	10^{-6}	N/A	N/A	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
70 (NOTE 12)		55	200 ms (NOTE 7, NOTE 10)	10^{-6}	N/A	N/A	Mission Critical Data (e.g. example services are the same as 5QI 6/8/9)
79		65	50 ms (NOTE 10, NOTE 13)	10^{-2}	N/A	N/A	V2X messages (see TS 23.287 [121])
80		68	10 ms (NOTE 5, NOTE 10)	10^{-6}	N/A	N/A	Low Latency eMBB applications Augmented Reality
82	Delay Critical GBR	19	10 ms (NOTE 4)	10^{-4}	255 bytes	2000 ms	Discrete Automation (see TS 22.261 [2])
83		22	10 ms (NOTE 4)	10^{-4}	1354 bytes (NOTE 3)	2000 ms	Discrete Automation (see TS 22.261 [2]); V2X messages (UE - RSU Platooning, Advanced Driving: Cooperative Lane Change with low LoA. See TS 22.186 [111], TS 23.287 [121])
84		24	30 ms (NOTE 6)	10^{-5}	1354 bytes (NOTE 3)	2000 ms	Intelligent transport systems (see TS 22.261 [2])
85		21	5 ms (NOTE 5)	10^{-5}	255 bytes	2000 ms	Electricity Distribution-high voltage (see TS 22.261 [2]). V2X messages (Remote Driving. See TS 22.186 [111], NOTE 16, see TS 23.287 [121])
86		18	5 ms (NOTE 5)	10^{-4}	1354 bytes	2000 ms	V2X messages (Advanced Driving: Collision Avoidance, Platooning with high LoA. See TS 22.186 [111], TS 23.287 [121])

NOTE 1: A packet which is delayed more than PDB is not counted as lost, thus not included in the PER.
NOTE 2: It is required that default MDBV is supported by a PLMN supporting the related 5QIs.
NOTE 3: The Maximum Transfer Unit (MTU) size considerations in clause 9.3 and Annex C of TS 23.060 [56] are also applicable. IP fragmentation may have impacts to CN PDB, and details are provided in clause 5.6.10.
NOTE 4: A static value for the CN PDB of 1 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. When a dynamic CN PDB is used, see clause 5.7.3.4.
NOTE 5: A static value for the CN PDB of 2 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. When a dynamic CN PDB is used, see clause 5.7.3.4.
NOTE 6: A static value for the CN PDB of 5 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface. When a dynamic CN PDB is used, see clause 5.7.3.4.
NOTE 7: For Mission Critical services, it may be assumed that the UPF terminating N6 is located "close" to the 5G_AN (roughly 10 ms) and is not normally used in a long distance, home routed roaming situation. Hence a static value for the CN PDBof 10 ms for the delay between a UPF terminating N6 and a 5G_AN should be subtracted from this PDB to derive the packet delay budget that applies to the radio interface.
NOTE 8: In both RRC Idle and RRC Connected mode, the PDB requirement for these 5QIs can be relaxed (but not to a value greater than 320 ms) for the first packet(s) in a downlink data or signalling burst in order to permit reasonable battery saving (DRX) techniques.
NOTE 9: It is expected that 5QI-65 and 5QI-69 are used together to provide Mission Critical Push to Talk service (e.g., 5QI-5 is not used for signalling). It is expected that the amount of traffic per UE will be similar or less compared to the IMS signalling.
NOTE 10: In both RRC Idle and RRC Connected mode, the PDB requirement for these 5QIs can be relaxed for the first packet(s) in a downlink data or signalling burst in order to permit battery saving (DRX) techniques.
NOTE 11: In RRC Idle mode, the PDB requirement for these 5QIs can be relaxed for the first packet(s) in a downlink data or signalling burst in order to permit battery saving (DRX) techniques.
NOTE 12: This 5QI value can only be assigned upon request from the network side. The UE and any application running on the UE is not allowed to request this 5QI value.
NOTE 13: A static value for the CN PDB of 20 ms for the delay between a UPF terminating N6 and a 5G-AN should be subtracted from a given PDB to derive the packet delay budget that applies to the radio interface.
NOTE 14: This 5QI is not supported in this Release of the specification as it is only used for transmission of V2X messages over MBMS bearers as defined in TS 23.285 [72] but the value is reserved for future use.
NOTE 15: For "live" uplink streaming (see TS 26.238 [76]), guidelines for PDB values of the different 5QIs correspond to the latency configurations defined in TR 26.939 [77]. In order to support higher latency reliable streaming services (above 500ms PDB), if different PDB and PER combinations are needed these configurations will have to use non-standardised 5QIs.
NOTE 16: These services are expected to need much larger MDBV values to be signalled to the RAN. Support for such larger MDBV values with low latency and high reliability is likely to require a suitable RAN configuration, for which, the simulation scenarios in TR 38.824 [112] may contain some guidance.

NOTE: It is preferred that a value less than 64 is allocated for any new standardised 5QI of non-GBR Resource Type. This is to allow for option 1 to be used as described in clause 5.7.1.3 (as the QFI is limited to less than 64).

5.7.5 Reflective QoS

5.7.5.1 General

Reflective QoS enables the UE to map UL User Plane traffic to QoS Flows without SMF provided QoS rules and it applies for IP PDU Session and Ethernet PDU Session. This is achieved by creating UE derived QoS rules in the UE based on the received DL traffic. It shall be possible to apply Reflective QoS and non-Reflective QoS concurrently within the same PDU Session.

For a UE supporting Reflective QoS functionality, the UE shall create a UE derived QoS rule for the uplink traffic based on the received DL traffic if Reflective QoS function is used by the 5GC for some traffic flows. The UE shall use the UE derived QoS rules to determine mapping of UL traffic to QoS Flows.

If the 3GPP UE supports Reflective QoS functionality, the UE should indicate support of Reflective QoS to the network (i.e. SMF) for every PDU Session. For PDU Sessions established in EPS and PDU Sessions transferred from EPS without N26 interface, the UE indicates Reflective QoS support using the PDU Session Establishment procedure. After the first inter-system change from EPS to 5GS for PDU Sessions established in EPS and transferred from EPS with N26 interface, the UE indicates Reflective QoS support using the PDU Session Modification procedure as described in clause 5.17.2.2.2. The UE as well as the network shall apply the information whether or not the UE indicated support of Reflective QoS throughout the lifetime of the PDU Session.

NOTE: The logic driving a supporting UE under exceptional circumstances to not indicate support of Reflective QoS for a PDU Session is implementation dependent.

Under exceptional circumstances, which are UE implementation dependent, the UE may decide to revoke previously indicated support for Reflective QoS using the PDU Session Modification procedure. In such a case, the UE shall delete all derived QoS rules for this PDU Session and the network shall stop any user plane enforcement actions related to Reflective QoS for this PDU Session. In addition, the network may provide signalled QoS rules for the SDFs for which Reflective QoS was used before. The UE shall not indicate support for Reflective QoS for this PDU Session for the remaining lifetime of the PDU Session.

If under the same exceptional circumstances mentioned above and while NAS level MM or SM congestion control timer is running, the UE needs to revoke a previously indicated support for Reflective QoS, the UE performs PDU Session Release procedure that is exempt from MM and SM congestion control as defined in clause 5.19.7.

5.7.5.2 UE Derived QoS Rule

The UE derived QoS rule contains following parameters:

- One UL Packet Filter (in the Packet Filter Set as defined in clause 5.7.6);
- QFI;
- Precedence value (see clause 5.7.1.9).

Upon receiving DL packet, one UL Packet Filter derived from the received DL packet as described in this clause is used to identify a UE derived QoS rule within a PDU Session.

For PDU Session of IP type the UL Packet Filter is derived based on the received DL packet as follows:

- When Protocol ID / Next Header is set to TCP or UDP, by using the source and destination IP addresses, source and destination port numbers, and the Protocol ID / Next Header field itself.
- When Protocol ID / Next Header is set to ESP, by using the source and destination IP addresses, the Security Parameter Index, and the Protocol ID / Next Header field itself. If the received DL packet is an IPSec protected packet, and an uplink IPSec SA corresponding to a downlink IPSec SA of the SPI in the DL packet exists, then the UL Packet Filter contains an SPI of the uplink IPSec SA.

NOTE 1: In this Release of the specification for PDU Sessions of IP type the use of Reflective QoS is restricted to service data flows for which Protocol ID / Next Header is set to TCP, UDP or ESP.

NOTE 2: The UE does not verify whether the downlink packets with RQI indication match the restrictions on Reflective QoS.

For PDU Session of Ethernet type the UL Packet Filter is derived based on the received DL packet by using the source and destination MAC addresses, the Ethertype on received DL packet is used as Ethertype for UL packet. In the case of presence of 802.1Q [98], the VID and PCP in IEEE 802.1Q [98] header(s) of the received DL packet is also used as the VID and PCP field for the UL Packet Filter. When double 802.1Q [98] tagging is used, only the outer (S-TAG) is taken into account for the UL Packet Filter derivation.

NOTE 3: In this Release of the specification for PDU Sessions of Ethernet type the use of Reflective QoS is restricted to service data flows for which 802.1Q [98] tagging is used.

The QFI of the UE derived QoS rule is set to the value received in the DL packet.

When Reflective QoS is activated the precedence value for all UE derived QoS rules is set to a standardised value.

5.7.5.3 Reflective QoS Control

Reflective QoS is controlled on per-packet basis by using the Reflective QoS Indication (RQI) in the encapsulation header on N3 (and N9) reference point together with the QFI and together with a Reflective QoS Timer (RQ Timer) value that is either signalled to the UE upon PDU Session Establishment (or upon PDU Session Modification as described in clause 5.17.2.2.2) or set to a default value. The RQ Timer value provided by the core network is at the granularity of PDU Session (the details are specified in TS 24.501 [47]).

When the 5GC determines that Reflective QoS has to be used for a specific SDF belonging to a QoS Flow, the SMF shall provide the RQA (Reflective QoS Attribute) within the QoS Flow's QoS profile to the NG-RAN on N2 reference point unless it has been done so before. When the RQA has been provided to the NG-RAN for a QoS Flow and the 5GC determines that the QoS Flow carries no more SDF for which Reflective QoS has to be used, the SMF should signal the removal of the RQA (Reflective QoS Attribute) from the QoS Flow's QoS profile to the NG-RAN on N2 reference point.

NOTE 1: The SMF could have a timer to delay the sending of the removal of the RQA. This would avoid signalling to the RAN in the case of new SDFs subject to Reflective QoS are bound to this QoS Flow in the meantime.

When the 5GC determines to use Reflective QoS for a specific SDF, the SMF shall ensure that the UPF applies the RQI marking (e.g. by setting the indication to use Reflective QoS in the QER associated with the DL PDR if not already set) for this SDF. The SMF shall also ensure that the uplink packets for this SDF can be received by the UPF from the QoS Flow to which the DL PDR of the SDF is associated with as specified in TS 29.244 [65], e.g. by generating a new UL PDR for this SDF for that QoS Flow and providing it to the UPF.

When the UPF is instructed by the SMF to apply RQI marking, the UPF shall set the RQI in the encapsulation header on the N3 (or N9) reference point for every DL packet corresponding to this SDF.

When an RQI is received by (R)AN in a DL packet on N3 reference point, the (R)AN shall indicate to the UE the QFI and the RQI of that DL packet.

Upon reception of a DL packet with RQI:

- if a UE derived QoS rule with a Packet Filter corresponding to the DL packet does not already exist,
  - the UE shall create a new UE derived QoS rule with a Packet Filter corresponding to the DL packet (as described in clause 5.7.5.2); and
  - the UE shall start, for this UE derived QoS rule, a timer set to the RQ Timer value.
- otherwise,
  - the UE shall restart the timer associated to this UE derived QoS rule; and
  - if the QFI associated with the downlink packet is different from the QFI associated with the UE derived QoS rule, the UE shall update this UE derived QoS rule with the new QFI.

NOTE 2: Non-3GPP ANs does not need N2 signalling to enable Reflective QoS. Non 3GPP accesses are expected to send transparently the QFI and RQI to the UE. If the UPF does not include the RQI, no UE derived QoS rule will be generated. If RQI is included to assist the UE to trigger an update of the UE derived QoS rule, the reception of PDU for a QFI restarts the RQ Timer.

Upon timer expiry associated with a UE derived QoS rule the UE deletes the corresponding UE derived QoS rule.

When the 5GC determines not to use Reflective QoS for a specific SDF any longer:

- the SMF shall ensure that the UPF stops applying RQI marking as specified in TS 29.244 [65] (e.g. by removing the indication to use Reflective QoS from the QER associated with the DL PDR) for this SDF.
- When the UPF receives this instruction to stop applying RQI marking, the UPF shall no longer set the RQI in the encapsulation header on the N3 (or N9) reference point DL packets corresponding to this SDF.
- The SMF shall also ensure that, after an operator configurable time, the uplink packets for this SDF will not be accepted by the UPF over the QoS Flow on which Reflective QoS was applied for this SDF as specified in TS 29.244 [65], e.g. by removing the UL PDR for this SDF from that QoS Flow.

NOTE 3: The operator configurable time has to be at least as long as the RQ Timer value to ensure that no UL packet would be dropped until the UE derived QoS rule is deleted by the UE.

When the 5GC determines to change the binding of the SDF while Reflective QoS is used for this SDF, the SMF shall ensure that the uplink packets for this SDF are accepted over the newly bound QoS Flow and, for an operator configurable time, over the previously bound QoS Flow.

5.7.6 Packet Filter Set

5.7.6.1 General

The Packet Filter Set is used in the QoS rule and the PDR to identify one or more packet (IP or Ethernet) flow(s).

NOTE 1: A QoS Flow is characterised by PDR(s) and QoS rule(s) as described in clause 5.7.1.1.

NOTE 2: DL Packet Filter in a Packet Filter Set of a QoS rule may be needed by the UE e.g. for the purpose of IMS precondition.

The Packet Filter Set may contain one or more Packet Filter(s). Every Packet Filter is applicable for the DL direction, the UL direction or both directions.

NOTE 3: The Packet Filter in the Packet Filter Set of the default QoS rule that allows all UL traffic (also known as match-all Packet Filter) is described in TS 24.501 [47].

There are two types of Packet Filter Set, i.e. IP Packet Filter Set, and Ethernet Packet Filter Set, corresponding to those PDU Session Types.

5.7.6.2 IP Packet Filter Set

For IP PDU Session Type, the Packet Filter Set shall support Packet Filters based on at least any combination of:

- Source/destination IP address or IPv6 prefix.
- Source / destination port number.
- Protocol ID of the protocol above IP/Next header type.
- Type of Service (TOS) (IPv4) / Traffic class (IPv6) and Mask.
- Flow Label (IPv6).
- Security parameter index.
- Packet Filter direction.

NOTE 1: A value left unspecified in a Packet Filter matches any value of the corresponding information in a packet.

NOTE 2: An IP address or Prefix may be combined with a prefix mask.

NOTE 3: Port numbers may be specified as port ranges.

5.7.6.3 Ethernet Packet Filter Set

For Ethernet PDU Session Type, the Packet Filter Set shall support Packet Filters based on at least any combination of:

- Source/destination MAC address.
- Ethertype as defined in IEEE 802.3.
- Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) VID fields as defined in IEEE 802.1Q [98].
- Customer-VLAN tag (C-TAG) and/or Service-VLAN tag (S-TAG) PCP/DEI fields as defined in IEEE 802.1Q [98].
- IP Packet Filter Set, in the case that Ethertype indicates IPv4/IPv6 payload.
- Packet Filter direction.

NOTE 1: The MAC address may be specified as address ranges.

NOTE 2: A value left unspecified in a Packet Filter matches any value of the corresponding information in a packet.

5.8 User Plane Management

5.8.1 General

User Plane Function(s) handle the user plane path of PDU Sessions. 3GPP specifications support deployments with a single UPF or multiple UPFs for a given PDU Session. UPF selection is performed by SMF. The details of UPF selection is described in clause 6.3.3. The number of UPFs supported for a PDU Session is unrestricted.

For an IPv4 type PDU Session or an IPv6 type PDU Session without multi-homing or an IPv4v6 type PDU Session, when multiple PDU Session Anchors are used (due to UL CL being inserted), only one IPv4 address and/or IPv6 prefix is allocated for the PDU Session. For an IPv6 multi-homed PDU Session there are multiple IPv6 prefixes allocated for the PDU Session as described in clause 5.6.4.3.

If the SMF had requested the UPF to proxy ARP or IPv6 Neighbour Solicitation for an Ethernet DNN, the UPF should respond to the ARP or IPv6 Neighbour Solicitation Request, itself.

Deployments with one single UPF used to serve a PDU Session do not apply to the Home Routed case and may not apply to the cases described in clause 5.6.4.

Deployments where a UPF is controlled either by a single SMF or multiple SMFs (for different PDU Sessions) are supported.

UPF traffic detection capabilities may be used by the SMF in order to control at least following features of the UPF:

- Traffic detection (e.g. classifying traffic of IP type, Ethernet type, or unstructured type)
- Traffic reporting (e.g. allowing SMF support for charging).
- QoS enforcement (The corresponding requirements are defined in clause 5.7).
- Traffic routing (e.g. as defined in clause 5.6.4. for UL CL or IPv6 multi-homing).

5.8.2 Functional Description

5.8.2.1 General

This clause contains detailed functional descriptions for some of the functions provided by the UPF. It is described how the SMF instructs it's corresponding UP function and which control parameters are used.

5.8.2.2 UE IP Address Management

5.8.2.2.1 General

The UE IP address management includes allocation and release of the UE IP address as well as renewal of the allocated IP address, where applicable.

- If there is a matching URSP rule or a matching UE Local Configuration containing a PDU Session Type of "IPv4", "IPv6" or "IPv4v6", then the UE shall set the requested PDU Session Type to the PDU Session Type contained in the matching URSP rule or in the matching UE Local Configuration, if this PDU Session Type is supported by the UE's IP stack capabilities. If there is no PDU Session Type value in the matching URSP rule or in the matching UE Local Configuration, the UE shall not include the requested PDU Session Type in the PDU Session Establishment Request message.
- Otherwise, if there is no matching URSP rule and no matching UE Local Configuration, the UE shall set the requested PDU Session Type during the PDU Session Establishment procedure based on its IP stack capabilities as follows:
- A UE which supports IPv6 and IPv4 shall set the requested PDU Session Type "IPv4v6".

- A UE which supports only IPv4 shall request for PDU Session Type "IPv4".
- A UE which supports only IPv6 shall request for PDU Session Type "IPv6".
- When the IP version capability of the UE is unknown in the UE (as in the case when the MT and TE are separated and the capability of the TE is not known in the MT), the UE shall request for PDU Session Type "IPv4v6".

The SMF selects PDU Session Type of the PDU Session as follows:

- If the SMF receives a request with PDU Session Type set to "IPv4v6", the SMF selects either PDU Session Type "IPv4" or "IPv6" or "IPv4v6" based on DNN configuration, subscription data and operator policies.
- If the SMF receives a request for PDU Session Type "IPv4" or "IPv6" and the requested IP version is supported by the DNN the SMF selects the requested PDU Session type.

In its answer to the UE, the SMF may indicate the PDU Session Types not allowed for the combination of (DNN, S-NNSAI). In this case, the UE shall not request another PDU Session to the same (DNN, S-NNSAI) for PDU Session Types indicated as not allowed by the network. In the case that the initial PDU Session was established with a PDU Session Type and the UE needs another single IP version PDU Session Type, the UE may initiate another PDU Session Establishment procedure to this (DNN, S-NNSAI) in order to activate a second PDU session with that PDU Session Type.

An SMF shall ensure that the IP address management procedure is based on the selected PDU Session Type. If IPv4 PDU Session Type is selected, an IPv4 address is allocated to the UE. Similarly, if IPv6 PDU Session type is selected, an IPv6 prefix is allocated. If IPv4v6 PDU Session Type is selected, both an IPv4 address and an IPv6 prefix are allocated. For Roaming case, the SMF in this clause refers to the SMF controlling the UPF(s) acting as PDU Session Anchor. i.e. H-SMF in home routed case and V-SMF in local breakout case. For home routed case, V-SMF forwards the PDU Session Type requested by UE to H-SMF without interpreting it. V-SMF sends back to UE the PDU Session Type selected by H-SMF. The SMF shall process the UE IP address management related messages, maintain the corresponding state information and provide the response messages to the UE.

The 5GC and UE support the following mechanisms:

a. During PDU Session Establishment procedure, the SMF sends the IP address to the UE via SM NAS signalling. The IPv4 address allocation and/or IPv4 parameter configuration via DHCPv4 (according to RFC 2131 [9]) can also be used once PDU Session is established.

b. /64 IPv6 prefix allocation shall be supported via IPv6 Stateless Auto-configuration according to RFC 4862 [10], if IPv6 is supported. The details of Stateless IPv6 Address Autoconfiguration are described in clause 5.8.2.2.3. IPv6 parameter configuration via Stateless DHCPv6 (according to RFC 3736 [14]) may also be supported.

For scenarios with RG connecting to 5GC, additional features for IPv6 address allocation and IPv6 prefix delegation are supported, as described in TS 23.316 [84].

To allocate the IP address via DHCPv4, the UE may indicate to the network within the Protocol Configuration Options that the UE requests to obtain the IPv4 address with DHCPv4, or obtain the IP address during the PDU Session Establishment procedure. This implies the following behaviour both for static and dynamic address allocation:

- The UE may indicate that it requests to obtain an IPv4 address as part of the PDU Session Establishment procedure. In such a case, the UE relies on the 5GC network to provide IPv4 address to the UE as part of the PDU Session Establishment procedure.
- The UE may indicate that it requests to obtain the IPv4 address after the PDU Session Establishment procedure by DHCPv4. That is, when the 5GC network supports DHCPv4 and allows that, it does not provide the IPv4 address for the UE as part of the PDU Session Establishment procedure. The network may respond to the UE by setting the allocated IPv4 Address to 0.0.0.0. After the PDU Session Establishment procedure is completed, the UE uses the connectivity with the 5GC and initiates the IPv4 address allocation on its own using DHCPv4. However, if the 5GC network provides IPv4 address to the UE as part of the PDU Session Establishment procedure, the UE should accept the IPv4 address indicated in the PDU Session Establishment procedure.
- If the UE sends no IP Address Allocation request, the SMF determines whether DHCPv4 is used between the UE and the SMF or not, based on per DNN configuration.

If dynamic policy provisioning is deployed, and the PCF was not informed of the IPv4 address at PDU Session Establishment procedure, the SMF shall inform the PCF about an allocated IPv4 address. If the IPv4 address is released, the SMF shall inform the PCF about the de-allocation of an IPv4 address.

In order to support DHCP based IP address configuration, the SMF shall act as the DHCP server towards the UE. The PDU Session Anchor UPF does not have any related DHCP functionality. The SMF instructs the PDU Session Anchor UPF serving the PDU Session to forward DHCP packets between the UE and the SMF over the user plane.

When DHCP is used for external data network assigned addressing and parameter configuration, the SMF shall act as the DHCP client towards the external DHCP server. The UPF does not have any related DHCP functionality. In the case of DHCP server on the external data network, the SMF instructs a UPF with N6 connectivity to forward DHCP packets between the UE and the SMF and the external DHCP server over the user plane.

The 5GC may also support the allocation of a static IPv4 address and/or a static IPv6 prefix based on subscription information in the UDM or based on the configuration on a per-subscriber, per-DNN basis and per-S-NSSAI.

If the static IP address/prefix is stored in the UDM, during PDU Session Establishment procedure, the SMF retrieves this static IP address/prefix from the UDM. If the static IP address/prefix is not stored in the UDM subscription record, it may be configured on a per-subscriber, per-DNN and per-S-NSSAI basis in the DHCP/DN-AAA server and the SMF retrieves the IP address/prefix for the UE from the DHCP/DN-AAA server. This IP address/prefix is delivered to the UE in the same way as a dynamic IP address/prefix. It is transparent to the UE whether the PLMN or the external data network allocates the IP address and whether the IP address is static or dynamic.

For IPv4 or IPv6 or IPv4v6 PDU Session Type, during PDU Session Establishment procedure, if UE IP address/prefix was not already allocated and provided to PCF, the SMF may receive a Subscribers IP Index from the PCF, the SMF may use this to assist in selecting how the IP address is to be allocated when multiple allocation methods, or multiple instances of the same method are supported. In the case of Home Routed roaming, the H-SMF may receive the IP index from the H-PCF.

When Static IP addresses for a PDU session are not used, the actual allocation of the IP Address(es) for a PDU Session may use any of the following mechanisms:

- The SMF allocates the IP address from a pool that corresponds to the PDU Session Anchor (UPF) that has been selected

- The UE IP address is obtained from the UPF. In that case the SMF shall interact with the UPF via N4 procedures to obtain a suitable IP address. The SMF provides the UPF with the necessary information allowing the UPF to derive the proper IP address (e.g. the network instance).

- In the case that the UE IP address is obtained from the external data network, additionally, the SMF shall also send the allocation, renewal and release related request messages to the external data network, i.e. DHCP/DN-AAA server, and maintain the corresponding state information. The IP address allocation request sent to DHCP/DN-AAA server may include the IP address pool ID to identify which range of IP address is to be allocated. In this case the SMF is provisioned with separate IP address pool ID(s), and the mapping between IP address pool ID and UPF Id, DNN, S-NSSAI, IP version. The provision is done by OAM or during the N4 Association Setup procedure.

A given IP address pool is controlled by a unique entity (either the SMF or the UPF or an external server). The IP address managed by the UPF can be partitioned into multiple IP address pool partition(s), i.e. associated with multiple IP address pool ID(s).

When the SMF is configured to obtain UE IP addresses from the UPF, the SMF may select a UPF based upon support of this feature. The SMF determines whether the UPF supports this feature via NRF or via N4 capability negotiation during N4 Association Setup. If no appropriate UPF support the feature, the SMF may allocate UE IP addresses, if configured to do so.

The IP address/prefix is released by the SMF (e.g. upon release of the PDU Session), likewise the UPF considers that any IP address it has allocated within a N4 session are released when this N4 session is released.

5.8.2.2.2 Routing rules configuration

When the UE has an IPv6 multi-homed PDU Session the UE selects the source IPv6 prefix according to IPv6 multi-homed routing rules pre-configured in the UE or received from network. IPv6 multi-homed routing rules received from the network have a higher priority than IPv6 multi-homed routing rules pre-configured in the UE

The SMF can generate the IPv6 multi-homed routing rules for a UE based on local configuration or dynamic PCC rules received from the PCF as defined in TS 23.503 [45]. If dynamic PCC is deployed, the SMF generates the IPv6 multi-home routing rules for a source IPv6 prefix based on the SDF Templates of those PCC rules which contain the DNAI corresponding to the newly assigned IPv6 prefix. The SMF can send IPv6 multi-homed routing rules to the UE to influence the source IPv6 prefix selection in IPv6 Router Advertisement (RA) messages according to RFC 4191 [8] at any time during the lifetime of the IPv6 multi-homed PDU Session. Such messages are sent via the UPF.

NOTE: For multiple IPv4 PDU Session and multiple IPv6 PDU Session cases, routing rule based PDU Session selection is not specified in this Release of the specification.

5.8.2.2.3 The procedure of Stateless IPv6 Address Autoconfiguration

If Stateless IPv6 Address Autoconfiguration is used for IPv6 address allocation to the UE, after PDU Session Establishment the UE may send a Router Solicitation message to the SMF to solicit a Router Advertisement message. The SMF sends a Router Advertisement message (solicited or unsolicited) to the UE. The Router Advertisement messages shall contain the IPv6 prefix.

After the UE has received the Router Advertisement message, it constructs a full IPv6 address via IPv6 Stateless Address Autoconfiguration in accordance with RFC 4862 [10]. To ensure that the link-local address generated by the UE does not collide with the link-local address of the UPF and the SMF, the SMF shall provide an interface identifier (see RFC 4862 [10]) to the UE and the UE shall use this interface identifier to configure its link-local address. For Stateless Address Autoconfiguration however, the UE can choose any interface identifier to generate IPv6 addresses, other than link-local, without involving the network. However, the UE shall not use any identifiers defined in TS 23.003 [19] as the basis for generating the interface identifier. For privacy, the UE may change the interface identifier used to generate full IPv6 address, as defined in TS 23.221 [23] without involving the network. Any prefix that the SMF advertises to the UE is globally unique. The SMF shall also record the relationship between the UE's identity (SUPI) and the allocated IPv6 prefix. Because any prefix that the SMF advertises to the UE is globally unique, there is no need for the UE to perform Duplicate Address Detection for any IPv6 address configured from the allocated IPv6 prefix. Even if the UE does not need to use Neighbor Solicitation messages for Duplicate Address Detection, the UE may, for example, use them to perform Neighbor Unreachability Detection towards the SMF, as defined in RFC 4861 [54]. Therefore, the SMF shall respond with a Neighbor Advertisement upon receiving a Neighbor Solicitation message from the UE.

In IPv6 multi-homing PDU session, SMF shall not allocate an interface identifier when a new IPv6 prefix allocated corresponding to the new PDU Session Anchor.

The above IPv6 related messages (e.g. Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement) are transferred between the SMF and UE via the UPF(s). If the Control Plane CIoT 5GS Optimisation is enabled for a PDU session, the above IPv6 related messages are transferred between the SMF and UE via the AMF after PDU Session Establishment, see TS 23.502 [3] clause 4.3.2.2.1 and clause 4.3.2.2.2, using the Mobile Terminated Data Transport in Control Plane CIoT 5GS Optimisation procedures.

5.8.2.3 Management of CN Tunnel Info

5.8.2.3.1 General

CN Tunnel Info is the Core Network address of a N3/N9 tunnel corresponding to the PDU Session. It comprises the TEID and the IP address which is used by the UPF on the N3/N9 tunnel for the PDU Session.

The CN Tunnel Info allocation and release is performed by the UPF. The SMF shall indicate to the UPF when the UPF is required to allocate/release CN Tunnel Info.

5.8.2.3.2 Void

5.8.2.3.3 Management of CN Tunnel Info in the UPF

The UPF shall manage the CN Tunnel Info space. When a new CN Tunnel Info is needed, the SMF shall request over N4 the UPF to allocate CN Tunnel Info for the applicable N3/N9 reference point. In response, the UPF provides CN Tunnel Info to the SMF. In the case of PDU Session Release or a UPF is removed from the user plane path of an

existing PDU Session, the SMF shall request UPF to release CN Tunnel Info for the PDU Session. If the corresponding N4 Session is released the UPF releases the associated CN Tunnel Info.

5.8.2.4 Traffic Detection

5.8.2.4.1 General

This clause describes the detection process at the UPF that identifies the packets belonging to a session, or a service data flow.

The SMF is responsible for instructing the UP function about how to detect user data traffic belonging to a Packet Detection Rule (PDR). The other parameters provided within a PDR describe how the UP function shall treat a packet that matches the detection information.

5.8.2.4.2 Traffic Detection Information

The SMF controls the traffic detection at the UP function by providing detection information for every PDR.

For IPv4 or IPv6 or IPv4v6 PDU Session type, detection information is a combination of:

- CN tunnel info.
- Network instance.
- QFI.
- IP Packet Filter Set as defined in clause 5.7.6.2.
- Application Identifier: The Application ID is an index to a set of application detection rules configured in UPF.

For Ethernet PDU Session type, detection information is a combination of:

- CN tunnel info.
- Network instance.
- QFI.
- Ethernet Packet Filter Set as defined in clause 5.7.6.3.

In this Release of the specification for Unstructured PDU Session Type, the UPF does not perform-QoS Flow level traffic detection for QoS enforcement.

Traffic detection information sent by the SMF to the UPF for a PDU Session may be associated with Network instance for detection and routing of traffic over N6. In the case of IP PDU Session Type, Network Instances can e.g. be used by the UPF for traffic detection and routing in the case of different IP domains or overlapping IP addresses. In the case of Ethernet PDU Session Type, different Network Instances can e.g. be configured in the UPF with different ways to handle the association between N6 and the PDU Sessions.

5.8.2.5 Control of User Plane Forwarding

5.8.2.5.1 General

The SMF controls user-plane packet forwarding for traffic detected by a PDR by providing a FAR with instructions to the UPF, including:

- Forwarding operation information;
- Forwarding target information.

The details of the forwarding target and operation will depend on the scenario and is described below. The following forwarding functionality is required by the UPF:

- Apply N3 /N9 tunnel related handling, i.e. encapsulation.

- Forward the traffic to/from the SMF, e.g. as described in Table 5.8.2.5.2-1.
- Forward the SM PDU DN Request Container from SMF to DN-AAA server
- Forward the traffic according to locally configured policy for traffic steering.
- Forward the traffic according to N4 rules of a 5G VN group for 5G VN group communication.

Data forwarding between the SMF and UPF is transmitted on the user plane tunnel established on N4 interface, defined in TS 29.244 [65].

5.8.2.5.2 Data forwarding between the SMF and UPF

Scenarios for data forwarding between the SMF and UPF are defined as below:

Table 5.8.2.5.1-1: Scenarios for data forwarding between the SMF and UPF

	Scenario description	Data forwarding direction
1	Forwarding of user-plane packets between the UE and the SMF e.g. DHCP signalling.	UPF to SMF SMF to UPF
2	Forwarding of packets between the SMF and the external DN e.g. with DN-AAA server	UPF to SMF SMF to UPF
3	Forwarding of packets subject to buffering in the SMF.	UPF to SMF SMF to UPF
4	Forwarding of End Marker Packets constructed by the SMF to a downstream node.	SMF to UPF
5	Forwarding of user data using Control Plane CIoT 5GS Optimisation	UPF to SMF SMF to UPF

5.8.2.5.3 Support of Ethernet PDU Session type

When configuring an UPF acting as PSA for an Ethernet PDU Session Type, the SMF may instruct the UPF to route the traffic based on detected MAC addresses as follows.

- The UPF learns the MAC address(es) connected via N6 based on the source MAC addresses of the DL traffic received on a N6 Network Instance.
- The UPF learns the MAC address(es) of UE(s) and devices conncted behind, if any, based on the source MAC address contained within the UL traffic received on a PDU Session (N3/N9 interface).
- The UPF forwards DL unicast traffic (with a known destination address) on a PDU Session determined based on the source MAC address(es) used by the UE for the UL traffic.
- The UPF forwards UL unicast traffic (with a known destination address) on a port (PDU Session or N6 interface) determined based on the source MAC address(es) learned beforehand.
    - In the case of multicast and broadcast traffic (if the destination MAC address is a broadcast or multicast address):- for DL traffic received by UPF on a N6 Network Instance the UPF should forward the traffic to every DL PDU Session (corresponding to any N4 Session) associated with this Network Instance
    - for uplink traffic received by UPF over a PDU session on a N3/N9 interface, the UPF should forward the traffic to the N6 interface and downlink to every PDU session (except toward the one of the incoming traffic) associated with the same N6 Network Instance
- for uplink and downlink unicast traffic received by UPF, if the destination MAC has not been learnt, the UPF should forward the traffic to every PDU session associated with the same N6 Network Instance and towards the N6 interface. In any case the traffic is not replicated on the PDU Session or the N6 interface of the incoming traffic.

NOTE 1: The UPF can consider a PDU Session or a N6 interface to be active or inactive in order to avoid forwarding loops. User data traffic is not sent on inactive PDU sessions or inactive N6 interface. This release of the specification does not further specify how the UPF determines whether a PDU Session or N6 interface is considered active or inactive.

NOTE 2: This release of the specification supports only a single N6 interface in a UPF associated with the N6 Network Instance.

- if the traffic is received with a VLAN ID, the above criteria apply only towards the N6 interface or PDU session matching the same VLAN ID, unless the UPF is instructed to remove the VLAN ID in the incoming traffic.

- if the destination MAC address of traffic refers to the same N6 interface or PDU session on which the traffic has been received, the frame should be dropped.

In order to handle scenarios where a device behind a UE is moved from one UE to another UE, a MAC address is considered as no longer associated with a UPF interface when the MAC address has not been detected as Source MAC address in UL traffic for a pre-defined period of time or it has been detected under a different interface (PDU Session or N6).

For ARP/IPv6 Neighbour Solicitation traffic, a SMF's request to respond to ARP/IPv6 Neighbour Solicitation based on local cache information or to redirect such traffic from the UPF to the SMF overrules the traffic forwarding rules described above.

NOTE 3: Local policies in UPF associated with the Network Instance can prevent local traffic switching in the UPF between PDU Sessions either for unicast traffic only or for any traffic. In the case where UPF policies prevent local traffic switching for any traffic (thus for broadcast/multicast traffic) some mechanism such as responding to ARP/ND based on local cache information or local multicast group handling is needed to ensure that upper layer protocol can run on the Ethernet PDU sessions.

The SMF may ask to get notified with the source MAC addresses used by the UE.

In order to request the UPF to act as defined above, the SMF may, for each PDU Session corresponding to a Network Instance, set an Ethernet PDU Session Information in a DL PDR that identifies all (DL) Ethernet packets matching the PDU session. Alternatively, for unicast traffic the SMF may provide UPF with dedicated forwarding rules related with MAC addresses notified by the UPF.

5.8.2.6 Charging and Usage Monitoring Handling

5.8.2.6.1 General

The SMF shall support interfaces towards CHF and PCF. The SMF interacts with CHF and PCF based on information received from other control plane NFs and user plane related information received from the UPF.

QoS Flow level, PDU Session level and subscriber related information remain at the SMF, and only usage information is requested from the UPF.

5.8.2.6.2 Activation of Usage Reporting in UPF

Triggered by the PCC rules received from the PCF or preconfigured information available at SMF, as well as from the CHF for online charging via Credit-Control session mechanisms, the SMF shall provide Usage Reporting Rules to the UPF for controlling how usage reporting is performed.

The SMF shall request the report of the relevant usage information for Usage Monitoring, based on Monitoring Keys and triggers which are specified in TS 23.503 [45]. Each Usage Reporting Rule requested for usage monitoring control is associated with the PDR(s) whose traffic is to be accounted under this rule. The SMF shall generate the Usage Reporting Rule for each Monitoring-key within the active PCC Rule(s), either preconfigured or received from the PCF and also shall keep the mapping between them. Multiple Usage Reporting Rules may be associated with the same PDR.

The SMF shall request the report of the relevant usage information for offline and online charging, based on Charging keys and additional triggers which are specified in TS 32.240 [41]. Each Usage Reporting Rule requested for offline or online charging is associated with the PDR(s) whose traffic is to be accounted under this rule. The SMF shall generate the Usage Reporting Rule for each Charging key and Sponsor Identity (if applicable) within the active PCC Rule(s), either preconfigured or received from the PCF, and also shall keep the mapping between them. Multiple Usage Reporting Rules may be associated with the same PDR.

The SMF function shall also provide reporting trigger events to the UPF for when to report usage information. The reporting trigger events (e.g. triggers, threshold information etc.) shall be supported for the PDU Session level reporting as well as on Rule level basis as determined by the SMF. The triggers may be provided as a volume, time or event to cater for the different charging/usage monitoring models supported by the TS 23.503 [45] for usage monitoring and by TS 32.240 [41] for offline and online charging. The SMF shall decide on the thresholds value(s) based on allowance received from PCF, CHF or based on local configuration. Other parameters for instructing the UPF to report usage information are defined in TS 29.244 [65].

When the PCC Rule attribute Service Data flow handling while requesting credit (specified in TS 23.503 [45]) indicates "non-blocking", the SMF shall request the report of the relevant usage information for the Charging key and Sponsor Identity (if applicable) and provide a default threshold value to the UPF while waiting for the credit from the CHF.

In some cases, the same Usage Reporting Rule can be used for different purposes (for both usage monitoring and charging), e.g. in the case that the same set of PDR(s), measurement method, trigger event, threshold, etc. apply. Similarly a reported measurement can be used for different purposes by the SMF.

5.8.2.6.3 Reporting of Usage Information towards SMF

The UPF shall support reporting of usage information to the SMF. The UPF shall be capable to support reporting based on different triggers, including:

- Periodic reporting with period defined by the SMF.
- Usage thresholds provided by the SMF.
- Report on demand received from the SMF.

The SMF shall make sure that the multiple granularity levels required by the reporting keys in the Usage Reporting rules satisfy the following aggregation levels without requiring a knowledge of the granularity levels by the UPF:

- PDU Session level reporting;
- Traffic flow (for both charging and usage monitoring) level reporting as defined by the reporting keys in the Usage Reporting Rule (see the description above).

Based on the mapping between Monitoring key and PCC rule stored at the SMF, the SMF shall combine the reported information with session and subscriber related information which is available at the SMF, for Usage Monitoring reporting over the corresponding Npcf interface (N7 reference point).

Based on the mapping between Charging key and Sponsor Identity (if applicable) and PCC rule stored at the SMF, the SMF shall combine the reported information with session and subscriber related information which is available at the SMF, for offline and online charging reporting over the corresponding charging interfaces.

This functionality is specified in TS 32.240 [41].

The usage information shall be collected in the UPF and reported to the SMF as defined in 5.8.2.6, based on Monitoring Keys and triggers which are specified in TS 23.503 [45].

5.8.2.7 PDU Session and QoS Flow Policing

ARP is used for admission control (i.e. retention and pre-emption of the new QoS Flow). The value of ARP is not required to be provided to the UPF.

For every QoS Flow, the SMF shall determine the transport level packet marking value (e.g. the DSCP in the outer IP header) based on the 5QI, the Priority Level (if explicitly signalled) and optionally, the ARP priority level and provide the transport level packet marking value to the UPF.

The SMF shall provide the Session-AMBR values of the PDU Session to the UPF so that the UPF can enforce the Session-AMBR of the PDU Session across all Non-GBR QoS Flows of the PDU Session.

SMF shall provide the GFBR and MFBR value for each GBR QoS Flow of the PDU Session to the UPF. SMF may also provide the Averaging window to the UPF, if Averaging window is not configured at the UPF or if it is different from the default value configured at the UPF.

5.8.2.8 PCC Related Functions

5.8.2.8.1 Activation/Deactivation of predefined PCC rules

A predefined PCC rule is configured in the SMF.

The traffic detection filters, e.g. IP Packet Filter, required in the UP function can be configured either in the SMF and provided to the UPF, as service data flow filter(s), or be configured in the UPF, as the application detection filter identified by an application identifier. For the latter case, the application identifier has to be configured in the SMF and the UPF.

The traffic steering policy information can be only configured in the UPF, together with traffic steering policy identifier(s), while the SMF has to be configured with the traffic steering policy identifier(s).

Policies for traffic handling in the UPF, which are referred by some identifiers corresponding to the parameters of a PCC rule, can be configured in the UPF. These traffic handling policies are configured as predefined QER(s), FAR(s) and URR(s).

When a predefined PCC rule is activated/deactivated by the PCF, SMF shall decide what information has to be provided to the UPF to enforce the rule based on where the traffic detection filters (i.e. service data flow filter(s) or application detection filter), traffic steering policy information and the policies used for the traffic handling in the UPF are configured and where they are enforced:

- If the predefined PCC rule contains an application identifier for which corresponding application detection filters are configured in the UPF, the SMF shall provide a corresponding application identifier to the UPF;
- If the predefined PCC rule contains traffic steering policy identifier(s), the SMF shall provide a corresponding traffic steering policy identifier(s) to the UPF;
- If the predefined PCC rule contains service data flow filter(s), the SMF shall provide them to the UPF;
- If the predefined PCC rule contains some parameters for which corresponding policies for traffic handling in the UPF are configured in the UPF, the SMF shall activate those traffic handling policies via their rule ID(s).

The SMF shall maintain the mapping between a PCC rule received over Npcf and the flow level PDR rule(s) used on N4 interface.

5.8.2.8.2 Enforcement of Dynamic PCC Rules

The application detection filters required in the UPF can be configured either in the SMF and provided to the UPF as the service data flow filter, or be configured in the UP function identified by an application identifier.

When receiving a dynamic PCC rule from the PCF which contains an application identifier and/or parameters for traffic handling in the UPF:

- if the application detection filter is configured in the SMF, the SMF shall provide it in the service data flow filter to the UPF, as well as parameters for traffic handling in the UPF received from the dynamic PCC rule;
- otherwise, the application detection filters is configured in UPF, the SMF shall provide to UPF with the application identifier and the parameters for traffic handling in the UPF as required based on the dynamic PCC rule.

The SMF shall maintain the mapping between a PCC rule received over Npcf and the flow level PDR(s) used on N4 interface.

5.8.2.8.3 Redirection

The uplink application's traffic redirection may be enforced either in the SMF (as specified in 5.8.2.5 Control of user plane forwarding) or directly in the UPF. The redirect destination may be provided in the dynamic PCC rule or be preconfigured, either in the SMF or in the UPF.

When receiving redirect information (redirection enabled/disabled and redirect destination) within a dynamic PCC rule or being activated/deactivated by the PCF for the predefined redirection policies, SMF shall decide whether to provide and what information to be provided to the UPF based on where the redirection is enforced and where the redirect

destination is acquired/preconfigured. When redirection is enforced in the UPF and the redirect destination is acquired from the dynamic PCC rule or is configured in the SMF, SMF shall provide the redirect destination to the UPF. When redirection is enforced in the SMF, SMF shall instruct the UPF to forward applicable user plane traffic to the SMF.

5.8.2.8.4 Support of PFD Management

The NEF (PFDF)shall provide PFD(s) to the SMF on the request of SMF (pull mode) or on the request of PFD management from NEF (push mode), as described in TS 23.503 [45]. The SMF shall provide the PFD(s) to the UPF, which have active PDR(s) with the Application identifier corresponding to the PFD(s).

The SMF supports the procedures in clause 4.4.3.5 of TS 23.502 [3], for management of PFDs. PFD(s) is cached in the SMF, and the SMF maintains a caching timer associated to the PFD(s). When the caching timer expires and there's no active PCC rule that refers to the corresponding Application identifier, the SMF informs the UPF to remove the PFD(s) identified by the Application identifier using the PFD management message.

When a PDR is provided for an Application identifier corresponding to the PFD(s) that are not already provided to the UPF, the SMF shall provide the PFD(s) to the UPF (if there are no PFD(s) cached, the SMF retrieves them from the NEF (PFDF) as specified in TS 23.503 [45]). When any update of the PFD(s) is received from NEF (PFDF) by SMF (using "push" or "pull" mode), and there are still active PDRs in UPF for the Application ID, the SMF shall provision the updated PFD set corresponding to the Application identifier to the UPF using the PFD management message.

NOTE 1: SMF can assure not to overload N4 signalling while managing PFD(s) to the UPF, e.g. forwarding the PFD(s) to the right UPF where the PFD(s) is enforced.

When the UPF receives the updated PFD(s) from either the same or different SMF for the same Application identifier, the latest received PFD(s) shall overwrite any existing PFD(s) stored in the UPF.

NOTE 2: For the case a single UPF is controlled by multiple SMFs, the conflict of PFD(s) corresponding to the same application identifier provided by different SMF can be avoided by operator enforcing a well-planned NEF (PFDF) and SMF/UPF deployment.

When a PFD is removed/modified and this PFD was used to detect application traffic related to an application identifier in a PDR of an N4 session and the UPF has reported the application start to the SMF as defined in clause 4.4.2.2 of TS 23.502 [3] for the application instance corresponding to this PFD, the UPF shall report the application stop to the SMF for the corresponding application instance identifier if the removed/modified PFD in UPF results in that the stop of the application instance is not being able to be detected.

If the PFDs are managed by local O&M procedures, PFD retrieval is not used; otherwise, the PFDs retrieved from NEF (PFDF) override any PFDs pre-configured in the SMF. When all the PFDs retrieved from the NEF (PFDF) for an application identifier are removed, the pre-configured PFDs are used. The SMF shall provide either the PFDs retrieved from NEF (PFDF) or the pre-configured PFDs for an application identifier to the UPF.

5.8.2.9 Functionality of Sending of "End marker"

5.8.2.9.0 Introduction

Sending of "end marker" is a functionality which involve SMF and UPF in order to assist the reordering function in the Target RAN. As part of the functionality, constructing of end marker packets can either be done in the SMF or in the UPF, as described in clauses 5.8.2.9.1 and 5.8.2.9.2. Whether constructing of end marker packets is performed by SMF or UPF is determined by network configuration.

5.8.2.9.1 UPF Constructing the "End marker" Packets

In the case of inter NG-RAN Handover procedure without UPF change, SMF shall indicate the UPF to switch the N3 path(s) by sending an N4 Session Modification Request message with the new AN Tunnel Info of NG RAN and in addition, provide an indication to the UPF to send the end marker packet(s) on the old N3 user plane path.

On receiving this indication, the UPF shall construct end marker packet(s) and send it for each N3 GTP-U tunnel towards the source NG RAN after sending the last PDU on the old path.

In the case of inter NG-RAN Handover procedure with change of the UPF terminating N3, the SMF shall request the UPF with N9 reference point to the UPF terminating N3 to switch the N9 user plane path(s) by sending an N4 Session

Modification Request message (N4 session ID, new CN Tunnel Info of the UPF terminating N3) and in addition, provide an indication to this UPF to send the end marker packet(s) on the old path.

On receiving this indication, the UPF shall construct end marker packet(s) and send it for each N9 GTP-U tunnel towards the source UPF after sending the last PDU on the old path.

On receiving the end marker packet(s) on N9 GTP-U tunnel, source UPF shall forward the end marker packet(s) and send it for each N3 GTP-U tunnel towards the source NG RAN.

5.8.2.9.2 SMF Constructing the "End marker" Packets

UPF referred in this clause is the UPF terminates N3 reference point.

It is assumed that the PDU Session for the UE comprises of an UPF that acts as a PDU Session Anchor and an intermediate UPF terminating N3 reference point at the time of this Handover procedure.

In the case of inter NG-RAN Handover procedure without UPF change, SMF shall indicate the UPF to switch the N3 path(s) by sending an N4 Session Modification Request message (N4 session ID, new AN Tunnel Info of NG RAN). After sending the last PDU on the old path, UPF shall replace the old AN Tunnel Info with the new one and responds with an N4 Session Modification Response message to acknowledge the success of path switch.

When the path switch is finished, SMF constructs the end marker packet(s) and sends it to the UPF. UPF then forwards the packet(s) to the source NG RAN.

In the case of inter NG-RAN Handover procedure with UPF change, SMF shall indicate the PSA UPF to switch the N9 user plane path(s) by sending an N4 Session Modification Request message (N4 session ID, new CN Tunnel Info of UPF). After sending the last PDU on the old N9 path, PSA UPF shall replace the old CN Tunnel Info with the new one and responds with an N4 Session Modification Response message to acknowledge the success of path switch.

When the path switch is finished, SMF constructs the end marker packet(s) and sends it to PSA UPF. PSA UPF then forwards the packet(s) to the source UPF.

5.8.2.10 UP Tunnel Management

5GC shall support per PDU Session tunnelling on N3 between (R)AN and UPF and N9 between UPFs. If there exist more than one UPF involved for the PDU Session, any tunnel(s) between UPFs (e.g. in the case of two UPFs, between the UPF that is an N3 terminating point and the UPF for PDU Session Anchor) remains established when a UE enters CM-IDLE state. In the case of downlink data buffering by UPF, when mobile terminated (MT) traffic arrives at the PDU Session Anchor UPF, it is forwarded to the UPF which buffer the data packet via N9 tunnel. See clause 5.8.3 for more details on UPF buffering. In the case of Home Routed roaming, the SMF in HPLMN is not aware of the UP activation state of a PDU Session.

When the UP connection of the PDU Session is deactivated, the SMF may release the UPF of N3 terminating point. In that case the UPF (e.g. the Branching Point/UL CL or PDU Session Anchor) connecting to the released UPF of N3 terminating point will buffer the DL packets. Otherwise, when the UPF with the N3 connection is not released, this UPF will buffer the DL packets.

When the UP connection of the PDU Session is activated due to a down-link data arrived and a new UPF is allocated to terminate the N3 connection, a data forwarding tunnel between the UPF that has buffered packets and the newly allocated UPF is established, so that the buffered data packets are transferred from the old UPF that has buffered packets to the newly allocated UPF via the data forwarding tunnel.

For a PDU Session whose the UP connection is deactivated and the SMF has subscribed the location change notification, when the SMF is notified of UE's new location from the AMF and detects that the UE has moved out of the service area of the existing intermediate UPF, the SMF may decide to maintain the intermediate UPF, remove the established tunnel between UPFs (in the case of removal of the intermediate UPF) or reallocate the tunnel between UPFs (in the case of reallocation of the intermediate UPF).

5.8.2.11 Parameters for N4 session management

5.8.2.11.1 General

These parameters are used by SMF to control the functionality of the UPF as well as to inform SMF about events occurring at the UPF.

The N4 session management procedures defined in clause 4.4.1 of TS 23.502 [3] will use the relevant parameters in the same way for all N4 reference points: the N4 Session Establishment procedure as well as the N4 Session Modification procedure provide the control parameters to the UPF, the N4 Session Release procedure removes all control parameters related to an N4 session, and the N4 Session Level Reporting procedure informs the SMF about events related to the PDU Session that are detected by the UPF.

The parameters over N4 reference point provided from SMF to UPF comprises an N4 Session ID and may also contain:

- Packet Detection Rules (PDR) that contain information to classify traffic (PDU(s)) arriving at the UPF;
- Forwarding Action Rules (FAR) that contain information on whether forwarding, dropping or buffering is to be applied to a traffic identified by PDR(s);
- Multi-Access Rules (MAR) that contain information on how to handle traffic steering, switching and splitting for a MA PDU Session;
- Usage Reporting Rules (URR) contains information that defines how traffic identified by PDR(s) shall be accounted as well as how a certain measurement shall be reported;
- QoS Enforcement Rules (QER), that contain information related to QoS enforcement of traffic identified by PDR(s);
- Session Reporting Rules (SRR) that contain information to request the UP function to detect and report events for a PDU session that are not related to specific PDRs of the PDU session or that are not related to traffic usage measurement.
- Trace Requirements;
- Port Management Information Container in 5GS;
- Bridge Information.

The N4 Session ID is assigned by the SMF and uniquely identifies an N4 session.

If the UPF indicated support of Trace, the SMF may activate a trace session during a N4 Session Establishment or a N4 Session Modification procedure. In that case it provides Trace Requirements to the UPF. The SMF may deactivate an on-going trace session using a N4 Session Modification procedure. There shall be at most one trace session activated per N4 Session at a time.

For the MA PDU Session, the SMF may add an additional access tunnel information during an N4 Session Modification procedure by updating MAR with addition of an FAR ID which refers to an FAR containing the additional access tunnel information for the MA PDU session for traffic steering in the UPF. For the MA PDU Session, the SMF may request Access Availability report per N4 Session, during N4 Session Establishment procedure or N4 Session Modification procedure.

A N4 Session may be used to control both UPF and NW-TT behaviour in the UPF. A N4 session support and enable exchange of TSN bridge configuration between the SMF and the UPF:

- Information that the SMF needs for bridge management (clause 5.8.2.11.9);
- Information that 5GS transparently relays between the AF the NW-TT: transparent Port Management Information Container.

When a N4 Session related with bridge management is established, the UPF allocates a dedicated port number for the DS-TT side of the PDU Session. The UPF then provides to the SMF following configuration parameters for the N4 Session:

- NW-TT port number;

- DS-TT port number.

After the N4 session has been established, the SMF and UPF may at any time exchange transparent bridge Port Management Information Container over a N4 session.

5.8.2.11.2 N4 Session Context

N4 Session Context is identified by an N4 Session ID. An N4 Session Context is generated by SMF and UPF respectively to store the parameters related to an N4 session, including N4 session ID, all PDRs, URRs, QERs and FARs or MARs used for this N4 session.

5.8.2.11.3 Packet Detection Rule

The following table describes the Packet Detection Rule (PDR) containing information required to classify a packet arriving at the UPF. Every PDR is used to detect packets in a certain transmission direction, e.g. UL direction or DL direction.

Table 5.8.2.11.3-1: Attributes within Packet Detection Rule

Attribute		Description	Comment
N4 Session ID		Identifies the N4 session associated to this PDR. NOTE 5.	
Rule ID		Unique identifier to identify this rule.	
Precedence		Determines the order, in which the detection information of all rules is applied.	
Packet Detection Information. NOTE 4.	Source interface	Contains the values "access side", "core side", "SMF", "N6-LAN", "5G VN internal".	Combination of UE IP address (together with Network instance, if necessary), CN tunnel info, packet filter set, application ID, Ethernet PDU Session Information and QFI are used for traffic detection. Source interface identifies the interface for incoming packets where the PDR applies, e.g. from access side (i.e. up-link), from core side (i.e. down-link), from SMF, from N6-LAN (i.e. the DN or the local DN), or from "5G VN internal" (i.e. local switch). Details like all the combination possibilities on N3, N9 interfaces are left for stage 3 decision.
	UE IP address	One IPv4 address and/or one IPv6 prefix with prefix length (NOTE 3).	
	Network instance (NOTE 1)	Identifies the Network instance associated with the incoming packet.	
	CN tunnel info	CN tunnel info on N3, N9 interfaces, i.e. F-TEID.	
	Packet Filter Set	Details see clause 5.7.6.	
	Application ID		
	QoS Flow ID	Contains the value of 5QI or non-standardized QFI.	
	Ethernet PDU Session Information	Refers to all the (DL) Ethernet packets matching an Ethernet PDU session, as further described in clause 5.6.10.2 and in TS 29.244 [65].	
	Framed Route Information	Refers to Framed Routes defined in clause 5.6.14.	
Packet replication and detection carry on information NOTE 6	Packet replication skip information NOTE 7	Contains UE address indication or N19/N6 indication. If the packet matches the packet replication skip information, i.e., source address of the packet is the UE address or the packet has been received on the interface in the packet replication skip information, the UP function neither creates a copy of the packet nor applies the corresponding processing (i.e., FAR, QER, URR). Otherwise the UPF performs a copy and applies the corresponding processing (i.e., FAR, QER, URR).	
	Carry on indication	Instructs the UP function to continue the packet detection process, i.e., lookup of the other PDRs without higher precedence.	
Outer header removal		Instructs the UP function to remove one or more outer header(s) (e.g. IP+UDP+GTP, IP + possibly UDP, VLAN tag), from the incoming packet.	Any extension header shall be stored for this packet.
Forwarding Action Rule ID (NOTE 2)		The Forwarding Action Rule ID identifies a forwarding action that has to be applied.	
Multi-Access Rule ID (NOTE 2)		The Multi-Access Rule ID identifies an action to be applied for handling forwarding for a MA PDU Session.	
List of Usage Reporting Rule ID(s)		Every Usage Reporting Rule ID identifies a measurement action that has to be applied.	
List of QoS Enforcement Rule ID(s)		Every QoS Enforcement Rule ID identifies a QoS enforcement action that has to be applied.	

NOTE 1: Needed e.g. if:
- UPF supports multiple DNN with overlapping IP addresses;
- UPF is connected to other UPF or AN node in different IP domains.
- UPF "local switch", N6-based forwarding and N19 forwarding is used for different 5G LAN groups.

NOTE 2: Either a FAR ID or a MAR ID is included, not both.

NOTE 3: The SMF may provide an indication asking the UPF to allocate one IPv4 address and/or IPv6 prefix. When asking to provide an IPv6 Prefix the SMF provides also an IPv6 prefix length.

NOTE 4: When in the architecture defined in clause 5.34, a PDR is sent over N16a from SMF to I-SMF, the Packet Detection Information may indicate that CN tunnel info is to be locally determined. This is further defined in clause 5.34.6.

NOTE 5: In the architecture defined in clause 5.34, the rules exchanged between I-SMF and SMF are not associated with a N4 Session ID but are associated with a N16a association.

NOTE 6: Needed in the case of support for broadcast/multicast traffic forwarding using packet replication with SMF-provided PDRs and FARs as described in clause 5.8.2.13.3.2.

NOTE 7: Needed in the case of packet replication with SMF-provided PDRs and FARs as described in clause 5.8.2.13.3.2, to prevent UPF from sending the broadcast/multicast packets back to the source UE or source N19/N6.

5.8.2.11.4 QoS Enforcement Rule

The following table describes the QoS Enforcement Rule (QER) that defines how a packet shall be treated in terms of bit rate limitation and packet marking for QoS purposes. All Packet Detection Rules that refer to the same QER share the same QoS resources, e.g. MFBR.

Table 5.8.2.11.4-1: Attributes within QoS Enforcement Rule

Attribute	Description	Comment
N4 Session ID	Identifies the N4 session associated to this QER	
Rule ID	Unique identifier to identify this information.	
QoS Enforcement Rule correlation ID (NOTE 1)	An identity allowing the UP function to correlate multiple Sessions for the same UE and APN.	Is used to correlate QoS Enforcement Rules for APN-AMBR enforcement.
Gate status UL/DL	Instructs the UP function to let the flow pass or to block the flow.	Values are: open, close, close after measurement report (for termination action "discard").
Maximum bitrate	The uplink/downlink maximum bitrate to be enforced for the packets.	This field may e.g. contain any one of: - APN-AMBR (for a QER that is referenced by all relevant Packet Detection Rules of all PDN Connections to an APN) (NOTE 1). - Session-AMBR (for a QER that is referenced by all relevant Packet Detection Rules of the PDU Session) - QoS Flow MBR (for a QER that is referenced by all Packet Detection Rules of a QoS Flow) - SDF MBR (for a QER that is referenced by the uplink/downlink Packet Detection Rule of a SDF) - Bearer MBR (for a QER that is referenced by all relevant Packet Detection Rules of a bearer) (NOTE 1).
Guaranteed bitrate	The uplink/downlink guaranteed bitrate authorized for the packets.	This field contains: - QoS Flow GBR (for a QER that is referenced by all Packet Detection Rules of a QoS Flow) - Bearer GBR (for a QER that is referenced by all relevant Packet Detection Rules of a bearer) (NOTE 1).
Averaging window	The time duration over which the Maximum and Guaranteed bitrate shall be calculated.	This is for counting the packets received during the time duration.
Down-link flow level marking	Flow level packet marking in the downlink.	For UPF, this is for controlling the setting of the RQI in the encapsulation header as described in clause 5.7.5.3.
QoS Flow ID	QoS Flow ID to be inserted by the UPF.	The UPF inserts the QFI value in the tunnel header of outgoing packets.
Paging Policy Indicator	Indicates the PPI value the UPF is required to insert in outgoing packets (see clause 5.4.3.2).	PPI applies only for DL traffic. The UPF inserts the PPI in the outer header of outgoing PDU.

Packet rate (NOTE 1)	Number of packets per time interval to be enforced.	This field contains any one of: - downlink packet rate for Serving PLMN Rate Control (the QER is referenced by all PDRs of the UE belonging to PDN connections using CIoT EPS Optimisations as described in TS 23.401 [26]). - uplink/downlink packet rate for APN Rate Control (the QER is referenced by all PDRs of the UE belonging to PDN connections to the same APN using CIoT EPS Optimisations as described in TS 23.401 [26]).
NOTE 1: This parameter is only used for interworking with EPC.		

5.8.2.11.5 Usage Reporting Rule

The following table describes the Usage Reporting Rule (URR) that defines how a packet shall be accounted as well as when and how to report the measurements.

Table 5.8.2.11.5-1: Attributes within Usage Reporting Rule

Attribute	Description	Comment
N4 Session ID	Identifies the N4 session associated to this URR	
Rule ID	Unique identifier to identify this information.	Used by UPF when reporting usage.
Reporting triggers	One or multiple of the events can be activated for the generation and reporting of the usage report.	Applicable events include: - Start/stop of traffic detection with/without application instance identifier and deduced SDF filter reporting; Deletion of last PDR for a URR; Periodic measurement threshold reached; Volume/Time/Event measurement threshold reached; Immediate report requested; Measurement of incoming UL traffic; Measurement of discarded DL traffic; MAC address reporting in the UL traffic; unknown destination MAC/IP address; end marker packet has been received.
Periodic measurement threshold	Defines the point in time for sending a periodic report for this URR (e.g. timeofday).	This allows generation of periodic usage report for e.g. offline charging. It can also be used for realizing the Monitoring time of the usage monitoring feature. It can also be used for realizing the Quota-Idle-Timeout, i.e. to enable the CP function to check whether any traffic has passed during this time.
Volume measurement threshold	Value in terms of uplink and/or downlink and/or total byte-count when the measurement report is to be generated.	
Time measurement threshold	Value in terms of the time duration (e.g. in seconds) when the measurement report is to be generated.	
Event measurement threshold	Number of events (identified according to a locally configured policy) after which the measurement report is to be generated.	
Inactivity detection time	Defines the period of time after which the time measurement shall stop, if no packets are received.	Timer corresponding to this duration is restarted at the end of each transmitted packet.
Event based reporting	Points to a locally configured policy which is identifies event(s) trigger for generating usage report.	
Linked URR ID(s)	Points to one or more other URR ID.	This enables the generation of a combined Usage Report for this and other URRs by triggering their reporting. See clause 5.2.2.4, TS 29.244 [65].
Measurement Method	Indicates the method for measuring the network resources usage, i.e. the data volume, duration, combined volume/duration, or event.	

Measurement information	Indicates specific conditions to be applied for measurements	It is used to request: - measurement before QoS enforcement, and/or - to pause or set to active a measurement as for the Pause of charging described in clause 4.4.4 and clause 4.23.14 of TS 23.502 [3], and/or - to request reduced reporting for application start/stop events.

5.8.2.11.6 Forwarding Action Rule

The following table describes the Forwarding Action Rule (FAR) that defines how a packet shall be buffered, dropped or forwarded, including packet encapsulation/decapsulation and forwarding destination.

Table 5.8.2.11.6-1: Attributes within Forwarding Action Rule

Attribute	Description	Comment
N4 Session ID	Identifies the N4 session associated to this FAR.	NOTE 9.
Rule ID	Unique identifier to identify this information.	
Action	Identifies the action to apply to the packet	Indicates whether the packet is to be forwarded, duplicated, dropped or buffered. When action indicates forwarding or duplicating, a number of additional attributes are included in the FAR. For buffering action, a Buffer Action Rule is also included and the action can also indicate that a notification of the first buffered and/or a notification of first discarded packet is requested (see clause 5.8.3.2).
Network instance (NOTE 2)	Identifies the Network instance associated with the outgoing packet (NOTE 1).	NOTE 8.
Destination interface (NOTE 3) (NOTE 7)	Contains the values "access side", "core side", "SMF", "N6-LAN", "5G VN internal" or "5G VN N19".	Identifies the interface for outgoing packets towards the access side (i.e. down-link), the core side (i.e. up-link), the SMF, the N6-LAN (i.e. the DN or the local DN), to 5G VN internal (i.e. local switch), or to 5G VN N19 (i.e. N19 interface).
Outer header creation (NOTE 3)	Instructs the UP function to add an outer header (e.g. IP+UDP+GTP, VLAN tag), IP + possibly UDP to the outgoing packet.	Contains the CN tunnel info, N6 tunnel info or AN tunnel info of peer entity (e.g. NG-RAN, another UPF, SMF, local access to a DN represented by a DNAI) (NOTE 8). Any extension header stored for this packet shall be added. The time stamps should be added in the GTP-U header if QoS Monitoring is enabled for the traffic corresponding to the PDR(s).
Send end marker packet(s) (NOTE 2)	Instructs the UPF to construct end marker packet(s) and send them out as described in clause 5.8.1.	This parameter should be sent together with the "outer header creation" parameter of the new CN tunnel info.
Transport level marking (NOTE 3)	Transport level packet marking in the uplink and downlink, e.g. setting the DiffServ Code Point.	NOTE 8.
Forwarding policy (NOTE 3)	Reference to a preconfigured traffic steering policy or http redirection (NOTE 4).	Contains one of the following policies identified by a TSP ID: - an N6-LAN steering policy to steer the subscriber's traffic to the appropriate N6 service functions deployed by the operator, or - a local N6 steering policy to enable traffic steering in the local access to the DN according to the routing information provided by an AF as described in clause 5.6.7. or a Redirect Destination and values for the forwarding behaviour (always, after measurement report (for termination action "redirect")).
Request for Proxying in UPF	Indicates that the UPF shall perform ARP proxying and / or IPv6 Neighbour Solicitation Proxying as specified in clause 5.6.10.2.	Applies to the Ethernet PDU Session type.

Container for header enrichment (NOTE 2)	Contains information to be used by the UPF for header enrichment.	Only relevant for the uplink direction.
Buffering Action Rule (NOTE 5)	Reference to a Buffering Action Rule ID defining the buffering instructions to be applied by the UPF (NOTE 6)	

NOTE 1: Needed e.g. if:
- UPF supports multiple DNN with overlapping IP addresses;
- UPF is connected to other UPF or NG-RAN node in different IP domains;
- UPF "local switch" and N19 forwarding is used for different 5G LAN groups.

NOTE 2: These attributes are required for FAR action set to forwarding.
NOTE 3: These attributes are required for FAR action set to forwarding or duplicating.
NOTE 4: The TSP ID is preconfigured in the SMF, and included in the FAR according to the description in clauses 5.6.7 and 6.1.3.14 of 23.503 [45] for local N6 steering and 6.1.3.14 of 23.503 [45] for N6-LAN steering. The TSP ID action is enforced before the Outer header creation actions.
NOTE 5: This attribute is present for FAR action set to buffering.
NOTE 6: The buffering action rule is created by the SMF and associated with the FAR in order to apply a specific buffering behaviour for DL packets requested to be buffered, as described in clause 5.8.3 and clause 5.2.4 in TS 29.244 [65].
NOTE 7: The use of "5G VN internal" instructs the UPF to send the packet back for another round of ingress processing using the active PDRs pertaining to another N4 session of the same 5G VN group.
NOTE 8: When in architectures defined in clause 5.34, a FAR is sent over N16a from SMF to I-SMF, the FAR sent by the SMF may indicate that the I-SMF is to locally determine the value of this attribute in order to build the N4 FAR rule sent to the actual UPF controlled by the I-SMF. This is further defined in clause 5.34.6.
NOTE 9: In the architecture defined in clause 5.34, the rules exchanged between I-SMF and SMF are not associated with a N4 Session ID but are associated with a N16a association.

5.8.2.11.7 Usage Report generated by UPF

The UPF sends the usage report to inform the SMF about the measurement of an active URR or about the detection of application traffic of an active Packet Detection Rule, or about one or both accesses becomes available or unavailable in a MA-PDU session. For each URR, the usage report may be generated repeatedly, i.e. as long as any one of the valid event triggers applies. A final usage report is sent for a URR when it is no longer active, i.e. either the URR is removed or all the references to this URR in any of the Packet Detection Rules belonging to the N4 session.

Following attributes can be included in the usage report:

Table 5.8.2.11.7-1: Attributes within Usage Report

Attribute	Description	Comment
N4 Session ID	Uniquely identifies a session.	Identifies the N4 session associated to this Usage Report
Rule ID	Uniquely identifies the Packet Detection Rule or Usage Reporting Rule within a session which triggered the report.	Packet Detection Rule is only indicated when Reporting trigger is Detection of 1st DL packet for a QoS Flow or Start/stop of traffic detection. Usage Reporting Rule is indicated for all other Reporting triggers.
Reporting trigger	Identifies the trigger for the usage report.	Applicable values are: Detection of 1st DL packet for a QoS Flow; Start/stop of traffic detection with/without application instance identifier and deduced SDF filter reporting; Deletion of last PDR for a URR; Periodic measurement threshold reached; Volume/Time/Event measurement threshold reached; Immediate report requested; Measurement of incoming UL traffic; Measurement of discarded DL traffic; MAC address reporting in the UL traffic; reporting of unknown destination MAC/IP address; end marker packet has been received.
Start time	Provides the timestamp, in terms of absolute time, when the collection of the information provided within Usage-Information is started.	Not sent when Reporting trigger is Start/stop of traffic detection.
End time	Provides the timestamp, in terms of absolute time, when the information provided within Usage-Information is generated.	Not sent when Reporting trigger is Start/stop of traffic detection.
Measurement information	Defines the measured volume/time/events for this URR.	Details refer to TS 29.244 [65].

5.8.2.11.8 Multi-Access Rule

The following table describes the Multi-Access Rule (MAR) that includes the association to the two FARs for both 3GPP access and non-3GPP access in the case of supporting ATSSS.

Table 5.8.2.11.8-1: Attributes within Multi-Access Rule

Attribute		Description	Comment
N4 Session ID		Identifies the N4 session associated to this MAR.	
Rule ID		Unique identifier to identify this rule.	
Steering functionality		Indicates the applicable traffic steering functionality: Values "MPTCP functionality", "ATSSS-LL functionality".	
Steering mode		Values "Active-Standby", "Smallest Delay", "Load Balancing" or "Priority-based".	
Per-Access Forwarding Action information (NOTE 1)	Forwarding Action Rule ID	The Forwarding Action Rule ID identifies a forwarding action that has to be applied.	
	Weight	Identifies the weight for the FAR if steering mode is "Load Balancing"	The weights for all FARs need to sum up to 100
	Priority	Values "Active or Standby" or "High or Low" for the FAR	"Active or Standby" for "Active-Standby" steering mode and "High or Low" for "Priority-based" steering mode
	List of Usage Reporting Rule ID(s)	Every Usage Reporting Rule ID identifies a measurement action that has to be applied.	This enables the SMF to request separate usage reports for different FARs (i.e. different accesses)
NOTE 1: The Per-Access Forwarding Action information is provided per access type (i.e. 3GPP access or Non-3GPP access).			

5.8.2.11.9 Bridge Management Information

The following table describes the Bridge Management Information (BMI) that includes the information required to configure a 5GS logical bridge for TSC PDU Sessions.

Table 5.8.2.11.9-1: Bridge Management Information

Attribute	Description	Comment
NW-TT Port Number	Port Number allocated by the NW-TT for the TSC PDU Session	
DS-TT Port Number	Port Number allocated by the NW-TT for the DS-TT for a given TSC PDU Session	

5.8.2.11.10 Port Management Information Container

The following table describes the Port Management Information Container (PMIC) that includes information exchanged transparently via 5GS between TSN AF and NW-TT for TSC PDU Sessions.

Table 5.8.2.11.10-1: Port Management Information Container

Attribute	Description	Comment
Port Management Information as in Table 5.28.3.1-1	Information exchanged transparently between NW-TT and TSN AF via 5GS	

5.8.2.11.11 Session Reporting Rule

The following table describes the Session Reporting Rule (SRR) that defines the detection and reporting events that the UPF shall report, that are not related to specific PDRs of the PDU Session, as follows:

- Per QoS flow per UE QoS Monitoring Report, as specified in clause 5.33.3.2.
- Change of 3GPP or non-3GPP access availability, for an MA PDU session.

Table 5.8.2.11.11-1: Attributes within Session Reporting Rule

Attribute	Description	Comment
N4 Session ID	Identifies the N4 session associated to this SRR.	
Rule ID	Unique identifier to identify this information.	Used by UPF when reporting.
QoS Monitoring per QoS flow Control Information	Indicates the UPF to apply the QoS Monitoring report for one or more QoS Flows.	The IE is defined in clause 7.5.2.9 of the TS 29.244 [65].
Access Availability Control Information	Indicates the UPF to report when an access type becomes available or unavailable for an MA PDU Session.	The IE is defined in clause 7.5.2.9 of TS 29.244 [65].

5.8.2.11.12 Session reporting generated by UPF

The UPF sends the session report to inform the SMF the detected events for a PDU Session that are related to an SRR.

Table 5.8.2.11.12-1: Attributes within Session Reporting

Attribute	Description	Comment
N4 Session ID	Identifies the N4 session associated to the SRR which triggered the report.	
Rule ID	Unique identifier to identify the Session Reporting Rule within a session which triggered the report.	Used by UPF when reporting.
QoS Monitoring Report	Indicates the QoS Monitoring result for one or more QoS Flows.	The IE is defined in clause 7.5.8.6 of TS 29.244 [65].
Access Availability Report	Indicates the change of 3GPP or non-3GPP access availability, for an MA PDU session.	The IE is defined in clause 7.5.8.6 of TS 29.244 [65].

5.8.2.12 Reporting of the UE MAC addresses used in a PDU Session

For Ethernet PDU Session type, the SMF may control the UPF to report the different MAC (Ethernet) addresses used as source address of frames sent UL by the UE in a PDU Session. These MAC addresses are called UE MAC addresses.

This control and the corresponding reporting takes place over N4.

NOTE: This is e.g. used to support reporting of all UE MAC addresses in a PDU Session to the PCF as described in clause 5.6.10.2.

The UPF reports the removal of a UE MAC address based on the detection of absence of traffic during an inactivity time. The inactivity time value is provided by the SMF to the UPF.

5.8.2.13 Support for 5G VN group communication

5.8.2.13.0 General

The SMF may configure the UPF(s) to apply different traffic forwarding methods to route traffic between PDU Sessions for a single 5G VN group. For example, depending on the destination address, some packet flows may be forwarded locally, while other packet flows are forwarded via N19 and other packet flows are forwarded to N6.

The UPF local switching, N6-based forwarding and N19-based forwarding methods require that a common SMF is controlling the PSA UPFs for the 5G VN group.

5G VN group communication includes one to one communication and one to many communication. One to one communication supports forwarding of unicast traffic between two UEs within a 5G VN, or between a UE and a device on the DN. One to many communication supports forwarding of multicast traffic and broadcast traffic from one UE (or device on the DN) to many/all UEs within a 5G VN and devices on the DN.

Traffic forwarding within the 5G VN group is realized by using a UPF internal interface ("5G VN internal") and a two-step detection and forwarding process. In the first step, the packets received from any 5G VN group member (via it's

PDU Session, via N6 or via N19) are forwarded to the UPF internal interface (i.e. Destination Interface set to "5G VN internal"). In the second step, PDRs installed at the UPF internal interface (i.e. Source Interface set to "5G VN internal") detect the packet and forward it to the respective 5G VN group member (via it's PDU Session, via N6 or via N19). The details of the PDR and FAR configuration are described in the following clauses.

For UEs belonging to the same 5G VN group and having PDU Sessions that correspond to N4 Sessions in the same PSA UPF, the following applies for traffic that is sent from one of these UEs to another one of these UEs using local switching: The incoming traffic for one PDU Session will match the corresponding N4 Session's PDR(s) of the source PDU Session (based on GTP-U header information). The traffic is then sent back to classification in that UPF (via the internal interface) and will match another N4 Session corresponding to the destination PDU Session (based on destination address in the PDU). The PDU is then forwarded to the target UE.

If 5G VN group members' PDU Sessions are served by different PSA UPFs and N19-based forwarding is applied, the SMF creates a group-level N4 Session with each involved UPF to enable N19-based forwarding and N6-based forwarding. When the traffic is then sent back to classification in that UPF (via the internal interface) it may match group-level N4 Session corresponding to the 5G VN group (based on destination address in the PDU or a default PDR rule with match-all packet filter). The PDU is then forwarded to N6 or to the UPF indicated in the group-level N4 Session via corresponding N19 tunnel. This enables the PDU to be sent to the target group member in the other UPF or to the device in the DN.

In the case of N19-based forwarding is not applied for a 5G VN group, group level N4 session is not required.

If more than one 5G VN group has to be supported in the PLMN, the N4 rule attribute Network Instance is used in addition to the UPF internal interface and set to a value representing the 5G VN group. This keeps the traffic of different 5G VN groups separate from each other and thus enables isolation of the 5G VN group communication during the packet detection and forwarding process. The SMF shall provide the PDRs and FARs related to the UPF internal interface as follows whenever more than one 5G VN group has to be supported in the PLMN:

- The FAR with Destination Interface set to "5G VN internal" shall also contain the Network Instance set to the value representing the 5G VN group.

- The PDR with Source Interface set to "5G VN internal" shall also contain the Network Instance set to the value representing the 5G VN group.

Forwarding Ethernet unicast traffic towards the PDU Session corresponding to the Destination MAC address of an Ethernet frame may correspond:

- either to the SMF explicitly configuring DL PDR(s) with the MAC addresses detected by the UPF on PDU Sessions and reported to the SMF; this is further described in clause 5.8.2.13.1;

- or to the SMF relying on MAC address learning in UPF as defined in clause 5.8.2.5.3. To request this UPF behaviour the SMF sets the Ethernet PDU Session Information indication in the DL PDR of the "5G VN internal" interface related with a 5G VN group. This may apply in the case that all PDU Sessions related with this 5G VN group are served by the same PSA or by multiple PSAs not inter-connected via N19.

For Ethernet traffic on 5G-VN, in the former case above where SMF explicitly configures DL PDR with the MAC addresses detected on PDU Sessions supporting a 5G VN group, the SMF acts as a central controller which is responsible for setting up the forwarding rules in the UPFs so that it avoids forwarding loops. The SMF becomes aware of the MAC addresses in use within a 5G VN group by the UPF's reporting of the MAC addresses. The SMF is responsible to react to topology changes in the Ethernet network. Local switching without SMF involvement is not specified for a 5G-VN when different PDU Sessions related with this 5G VN group may be served by different PSA(s) connected over N19.

NOTE: The mechanisms described above implies signalling on N4 Sessions related with a VN group each time a new MAC address is detected as used (or no more used) within a PDU Session related with this 5G VN group. Hence the usage of the solution with SMF explicitly configuring DL PDR with the MAC addresses defined in this release can raise signalling scalability issues for large VN groups with lots of devices (MAC addresses) served by PDU sessions related with this VN group.

5.8.2.13.1 Support for unicast traffic forwarding of a 5G VN

To enable unicast traffic forwarding in a UPF, the following applies:

- The SMF provides for each 5G VN group member's N4 Session (i.e. N4 Session corresponding to PDU Session) the following N4 rules that enable the processing of packets received from this UE.
  - in order to detect the traffic, a PDR containing Source Interface set to "access side", and CN Tunnel Information set to PDU Session tunnel header (i.e., N3 or N9 GTP-U F-TEID); and
  - in order to forward the traffic, a FAR containing Destination Interface set to "5G VN internal".
- The SMF provides for each 5G VN group member's N4 Session (i.e. N4 session corresponding to PDU Session) the following N4 rules that enable the processing of packets towards this UE.
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", and Destination Address set to the IP/MAC address (es) of this 5G VN group member; and
  - in order to forward the traffic, a FAR containing Outer Header Creation indicating the N3/N9 tunnel information, and Destination Interface set "access side".
- If N19-based forwarding is applied, the SMF configures the group-level N4 Session for processing packets received from a N19 tunnel with the following N4 rules for each N19 tunnel.
  - in order to detect the traffic, a PDR containing Source Interface set to "core side", and CN Tunnel Information set to N19 tunnel header (i.e., N19 GTP-U F-TEID); and
  - in order to forward the traffic, a FAR containing Destination Interface set to "5G VN internal".
- If N19-based forwarding is applied, the SMF configures the group-level N4 Session for processing packets towards 5G VN group members anchored at other UPFs with the following N4 rules for each N19 tunnel.
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", and Destination Address set to the IP/MAC address (es) of UEs anchored at the peer UPF of this N19 tunnel; and
  - in order to forward the traffic to a 5G VN group member anchored at another UPF via the N19 tunnel, a FAR containing Outer Header Creation indicating the N19 tunnel information, Destination Interface set to "core side".
- The SMF configures the group-level N4 Session for processing packets received from a 5G VN group member connected via N6 with the following N4 rules.
  - in order to detect the traffic, a PDR containing Source Interface set to "core side", and Source Address set to the IP/MAC address (es) of this 5G VN group member; and
  - in order to forward the traffic, a FAR containing Destination Interface set to "5G VN internal".
- The SMF configures the group-level N4 Session for processing packets towards a 5G VN group member connected via N6 or packets towards a device residing in DN with the following N4 rules.
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", and Destination Address set to the IP/MAC address (es) of this 5G VN group member; and
  - in order to forward the traffic to the 5G VN group member or device via N6, a FAR containing Destination Interface set to "core side".
- The SMF shall update N4 rules for group-level N4 Session to enable correct forwarding of packets towards UE who's PSA UPF has been reallocated and address is unchanged.
- The SMF may also configure the following N4 rules for the group-level N4 Session to process packets with an unknown destination address:
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", a match-all Packet Filter, and a Precedence set to the lowest precedence value; and
  - in order to process the traffic, a FAR containing Destination Interface set to "core side" to route the traffic via N6 by default, or in the case of N6-based forwarding is not applied a FAR instructing the UPF to drop the traffic.

5.8.2.13.2 Support for unicast traffic forwarding update due to UE mobility

To enable the service continuity when the PSA UPF serving the UE changed, the following applies:

- Keep the UE address unchanged if N6-based forwarding is not used.
- Configure the UE's N4 Session with N4 rules (PDR, FAR) to detect and forward the traffic to this UE via its PDU Session tunnel(i.e.,N3 tunnel) on the target PSA UPF.
- If N19-based forwarding is applied: To switch the traffic towards this UE from the source PSA UPF to the target PSA UPF for N19-based forwarding, the SMF deletes the N4 rule (PDR) that detects the traffic towards this UE in the group-level N4 Session at UPFs involved in the 5G VN group (except the source PSA UPF), then adds or updates the PDR that detects the traffic towards this UE with the FAR containing the N19 tunnel information of the target PSA UPF in the group-level N4 Session at UPFs involved in the 5G VN group (except the target PSA UPF).

5.8.2.13.3 Support for user plane traffic replication in a 5G VN

5.8.2.13.3.1 User plane traffic replication based on UPF internal functionality

For Ethernet PDU Sessions, the SMF may instruct the UPF to route traffic to be replicated as described in clause 5.8.2.5.

For IP PDU Session types, the SMF may instruct the UPF to manage IP multicast traffic as described in TS 23.316 [84] clauses 4.6.6 and 7.7.1. The UPF replicates the IP multicast traffic received from PDU Sessions or N6 interface and sends the packets over other PDU Sessions and other N6 interface subscribed to the IP Multicast groups.

Mechanisms described in TS 23.316 [84] clauses 4.6.6 and 7.7.1 apply to support 5G VN group communication with following clarifications:

- These mechanisms are not limited to Wireline access and can apply on any access,
- IP Multicast traffic allowed for a PDU Session is not meant for IPTV services reachable over N6,
- IGMP /MLD signalling does not relate with STB or 5G-RG: TS 23.316 [84] clauses 4.6.6 and 7.7.1, apply to UE members of a 5G VN group instead of 5G-RG, and
- TS 23.316 [84] clauses 7.7.1.1.2 and 7.7.1.1.4 are not applicable to 5G VN groups: members of the 5G VN groups may receive any multicast traffic associated with the (DNN, S-NSSAI) of the 5G VN group.
- UPF exchange of signalling such as PIM (Protocol-Independent Multicast) may apply as defined in TS 23.316, with following clarification:
  - PIM signalling is generally exchanged over N6 but may be sent towards the PDU Session supporting the source address of multicast traffic identified by IGMP / MLD signalling for Source Specific Multicast. In the case of IGMP / MLD signalling not related with Source Specific Multicast no PIM signalling is sent towards any PDU Session

5.8.2.13.3.2 User plane traffic replication based on PDRs with replication instructions

Alternatively, for IP or Ethernet type data communication, the SMF instructs the UPF via PDRs and FARs how to replicate user plane traffic.

The mechanism is supported in the following conditions:

- When N19 is used, there is a full mesh of N19 tunnels between UPFs serving the 5G VN group;
- There is no support of forwarding packets with destination MAC address not known by SMF/UPF (i.e. no support for new UE MAC addresses from the UE during the PDU Session lifetime)
- There is no support for forwarding a broadcast/multicast packet with source address not known to SMF/UPF.
- Each UPF supports one N6 interface instance towards the data network, or only supports N19-based forwarding without N6;

- Multicast group formation of selected members of a 5G VN is not described in this release of the specification.

In this case, when the UPF receives a broadcast packet of a 5G VN group from N19 or N6, it shall distribute it to all 5G VN group members connected to this UPF. When the UPF receives a broadcast packet from a UE (source UE) via PDU Session associated with a 5G VN group, it shall distribute it to:

- All 5G VN group members (except the source UE) connected to this UPF via local switch, and
- All 5G VN group members connected to other UPFs via N19-based forwarding, and
- The devices on the DN via N6-based forwarding.

To enable broadcast traffic forwarding of a 5G VN group in a UPF, the following applies:

- The SMF provides group-level N4 Session and each 5G VN group member' N4 Session with the PDR that detect the broadcast packet sent via "internal interface". When UPF receives the broadcast packets sent via "internal interface", it matches the broadcast packet against all PDRs installed at the "internal interface". A successful matching with a PDR that detect the broadcast packet instructs the UPF to continue the lookup of the other PDRs without higher precedence. A matching PDR that detects the broadcast packet shall instruct the UPF to duplicate the broadcast packet and perform processing (using associated FAR, URR, QER) on the copy instead of the original packet if the broadcast packet does not satisfy the packet replication skip information, otherwise the PDR instructs the UPF to skip the processing of the broadcast packet.
- The broadcast packets received from N19 or N6 are forwarded to the UPF internal interface together with a N19 or N6 indication, GTP-U header can carry the N19 or N6 indication.
- The SMF provides for each 5G VN group member' N4 Session (i.e. N4 session corresponding to PDU Session) the following N4 rules that enable the processing of broadcast packets towards this UE.
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", Destination Address set to the broadcast address, the Packet replication skip information set to the IP/MAC address (es) of this 5G VN group member, and the indication to carry on matching; and
  - in order to forward the traffic, a FAR containing Outer Header Creation indicating the PDU Session tunnel information, and Destination Interface set "access side".
- The SMF configures the group-level N4 Session for processing packets received from a N19 tunnel with the following N4 rules for each N19 tunnel.
  - in order to detect the traffic, a PDR containing Source Interface set to "core side", Destination Address set to the broadcast address, and CN Tunnel Information set to N19 tunnel header (i.e., N19 GTP-U TEID); and
  - in order to forward the traffic, a FAR containing Destination Interface set to "5G VN internal", Outer Header Creation with the N19 indication.
- The SMF provides for the group-level N4 Session the following N4 rules that enable the processing of broadcast packets towards the other UPFs.
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", Destination Address set to the broadcast address, the Packet replication skip information set to the N19 indication, and the indication to carry on matching; and
  - in order to forward the traffic to each involved UPF via the corresponding N19 tunnel, a FAR containing "Duplication" instruction, Outer Header Creation indicating the N19 tunnel information, Destination Interface set to "core side".
- The SMF configures the group-level N4 Session for processing packets received from N6 with the following N4 rules.
  - in order to detect the traffic, a PDR containing Source Interface set to "core side", and Destination Address set to the broadcast address; and
  - in order to forward the traffic, a FAR containing Destination Interface set to "5G VN internal", Outer Header Creation with the N6 indication.

- The SMF provides for the group-level N4 Session the following N4 rules that enable the processing of broadcast packets towards N6.
  - in order to detect the traffic, a PDR containing Source Interface set to "5G VN internal", a match-all packet filter, and the Packet replication skip information set to the N6 indication; and
  - in order to forward the traffic to N6, a FAR containing Destination Interface set to "core side".

In this case, to enable multicast traffic forwarding of a 5G VN group in a UPF, broadcast traffic forwarding of a 5G VN applies to multicast traffic forwarding of a 5G VN with the following modifications:

- The SMF installs PDRs for the multicast address instead of the broadcast address.
- The PDRs and FARs are installed for PDU Sessions corresponding to the members of the multicast group.

5.8.2.14 Inter PLMN User Plane Security functionality

Operators can deploy UPF(s) supporting the Inter PLMN User Plane Security (IPUPS) functionality at the border of their network to protect their networks from invalid inter PLMN N9 traffic.

The IPUPS functionality forwards GTP-U packets (received via the N9 interface) only if they belong to an active PDU Session and are not malformed, as described in TS 33.501 [29].

The SMF can activate the IPUPS functionality together with other UP functionality in the same UPF, or insert a separate UPF in the UP path for the IPUPS functionality. In both cases the UPF with IPUPS functionality is controlled by the SMF via the N4 interface.

5.8.3 Explicit Buffer Management

5.8.3.1 General

5GC supports buffering of UE's data packets for deactivated PDU Sessions.

Support for buffering in the UPF is mandatory and optional in the SMF.

5.8.3.2 Buffering at UPF

The SMF provides instructions to the UPF for at least the following behaviour:

- buffer downlink packets with the following additional options:
  - reporting the arrival of first downlink packet, and/or
  - reporting the first discarded downlink packet, or
- drop packet.

When the UP connection of the PDU Session is deactivated and the SMF decides to activate buffering in UPF for the session, the SMF shall inform the UPF to start buffering packets for this PDU Session.

Buffering in the UPF may be configured based on timers or the amount of downlink data to be buffered. The SMF decides whether buffering timers or amount of downlink data are handled by the UPF or SMF.

After starting buffering, when the first downlink packet arrives, UPF shall inform the SMF if it is setup to report. UPF sends a downlink data notification message to the SMF via N4 unless specified otherwise and indicates the user plane path on which the downlink packet was received.

After starting buffering, when the first downlink packet in a configured period of time that has been buffered is discarded by the UPF because the configured buffering time or amount of downlink data to be buffered is exceeded, the UPF shall inform the SMF if it is setup to report. UPF sends a dropped downlink data notification message to the SMF via N4 and indicates the PDR for which the downlink packet was received. A new report is sent if the SMF terminates and subsequently re-activates the buffering action.at the UPF and the UPF again receives downlink packets.

NOTE: For the notification about the downlink data delivery status "buffered" or "discarded" related to packets from a particular AF as part of the Nsmf_EventExposure service, it is expected that a PDR with a traffic filter identifying that AF as source and a Forwarding Action rule with action "buffer" is installed.

When the UP connection of the PDU Session is activated, the SMF updates the UPF of the change in buffering state. The buffered data packets, if any, are then forwarded to the (R)AN by the UPF.

If the UP connection of the PDU Session has been deactivated for a long time, the SMF may indicate the UPF to stop buffering for this PDU Session.

5.8.3.3 Buffering at SMF

When the UP connection of the PDU Session is deactivated and the SMF supports buffering capability, the SMF may decide to activate buffering on SMF, the SMF shall inform the UPF to start forwarding the downlink data packets towards the SMF.

When the UP connection of the PDU Session is activated, if there are buffered packets available and their buffering duration has not expired, the SMF shall forward those packets to the UPF to relay them to the UE. These packets are then forwarded by the UPF to the (R)AN.

5.8.4 SMF Pause of Charging

The SMF Pause of Charging functionality is supported with the purpose that the charging and usage monitoring data in the core network more accurately reflects the downlink traffic actually sent to the (R)AN. When the amount of downlink data incoming at the UPF for a PDU Session that is in deactivated state goes above a pre-configured threshold, the pause of charging functionality ensures that data that dropped in the core network is not included in charging and usage monitoring records.

The procedures for SMF Pause of Charging are described in TS 23.502 [3].

5.9 Identifiers

5.9.1 General

Each subscriber in the 5G System shall be allocated one 5G Subscription Permanent Identifier (SUPI) for use within the 3GPP system. The 5G System supports identification of subscriptions independently of identification of the user equipment. Each UE accessing the 5G System shall be assigned a Permanent Equipment Identifier (PEI).

The 5G System supports allocation of a temporary identifier (5G-GUTI) in order to support user confidentiality protection.

5.9.2 Subscription Permanent Identifier

A globally unique 5G Subscription Permanent Identifier (SUPI) shall be allocated to each subscriber in the 5G System and provisioned in the UDM/UDR. The SUPI is used only inside 3GPP system, and its privacy is specified in TS 33.501 [29].

The SUPI may contain:

- an IMSI as defined in TS 23.003 [19], or
- a network-specific identifier, used for private networks as defined in TS 22.261 [2].
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [84].
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [84].

A SUPI containing a network-specific identifier shall take the form of a Network Access Identifier (NAI) using the NAI RFC 7542 [20] based user identification as defined in TS 23.003 [19].

When UE needs to indicate its SUPI to the network (e.g. as part of the Registration procedure), the UE provides the SUPI in concealed form as defined in TS 23.003 [19].

In order to enable roaming scenarios, the SUPI shall contain the address of the home network (e.g. the MCC and MNC in the case of an IMSI based SUPI).

For interworking with the EPC, the SUPI allocated to the 3GPP UE shall always be based on an IMSI to enable the UE to present an IMSI to the EPC.

The usage of SUPI for W-5GAN is further specified in TS 23.316 [84].

5.9.2a Subscription Concealed Identifier

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier containing the concealed SUPI. It is specified in TS 33.501 [29].

The usage of SUCI for W-5GAN access is further specified in TS 23.316 [84].

5.9.3 Permanent Equipment Identifier

A Permanent Equipment Identifier (PEI) is defined for the 3GPP UE accessing the 5G System.

The PEI can assume different formats for different UE types and use cases. The UE shall present the PEI to the network together with an indication of the PEI format being used.

If the UE supports at least one 3GPP access technology (i.e. NG-RAN, E-UTRAN, UTRAN or GERAN), the UE must be allocated a PEI in the IMEI or IMEISV format.

In the scope of this release, the PEI may be one of the following:

- for UEs that support at least one 3GPP access technology, an IMEI or IMEISV, as defined in TS 23.003 [19];
- PEI used in the case of W-5GAN access as further specified in TS 23.316 [84].
- for UEs not supporting any 3GPP access technologies, the IEEE Extended Unique Identifier EUI-64 [113] of the access technology the UE uses to connect to the 5GC.

5.9.4 5G Globally Unique Temporary Identifier

The AMF shall allocate a 5G Globally Unique Temporary Identifier (5G-GUTI) to the UE that is common to both 3GPP and non-3GPP access. It shall be possible to use the same 5G-GUTI for accessing 3GPP access and non-3GPP access security context within the AMF for the given UE. An AMF may re-assign a new 5G-GUTI to the UE at any time. The AMF provides a new 5G-GUTI to the UE under the conditions specified in clause 6.12.3 in TS 33.501 [29]. When the UE is in CM-IDLE, the AMF may delay providing the UE with a new 5G-GUTI until the next NAS transaction.

The 5G-GUTI shall be structured as:

<5G-GUTI> := <GUAMI> <5G-TMSI>

where GUAMI identifies one or more AMF(s).

When the GUAMI identifies only one AMF, the 5G-TMSI identifies the UE uniquely within the AMF. However, when AMF assigns a 5G-GUTI to the UE with a GUAMI value used by more than one AMF, the AMF shall ensure that the 5G-TMSI value used within the assigned 5G-GUTI is not already in use by the other AMF(s) sharing that GUAMI value.

The Globally Unique AMF ID (GUAMI) shall be structured as:

<GUAMI> := <MCC> <MNC> <AMF Region ID> <AMF Set ID> <AMF Pointer>

where AMF Region ID identifies the region, AMF Set ID uniquely identifies the AMF Set within the AMF Region and AMF Pointer identifies one or more AMFs within the AMF Set.

NOTE 1: The AMF Region ID addresses the case that there are more AMFs in the network than the number of AMFs that can be supported by AMF Set ID and AMF Pointer by enabling operators to re-use the same AMF Set IDs and AMF Pointers in different regions.

NOTE 2: In the case of SNPNs, the PLMN IDs may be shared among SNPNs such that the constructed GUAMIs are not globally unique. However, PLMN ID and NID are provided together, separate from the GUAMI, to uniquely identify selected or supported SNPN in RRC and N2.

NOTE 3: See TS 23.003 [19] for details on the structure of the fields of GUAMI.

The 5G-S-TMSI is the shortened form of the GUTI to enable more efficient radio signalling procedures (e.g. during Paging and Service Request) and is defined as:

<5G-S-TMSI> := <AMF Set ID> <AMF Pointer> <5G-TMSI>

As specified in TS 38.304 [50] and TS 36.304 [52] for 3GPP access, the NG-RAN uses the 10 Least Significant Bits of the 5G-TMSI in the determination of the time at which different UEs are paged. Hence, the AMF shall ensure that the 10 Least Significant Bits of the 5G-TMSI are evenly distributed.

As specified in TS 38.331 [28] and TS 36.331 [51] for 3GPP access, the NG-RAN's RRC Connection Establishment's contention resolution process assumes that there is a low probability of the same 5G-TMSI being allocated by different AMFs to different UEs. The AMFs' process for allocating the 5G-TMSI should take this account.

NOTE 4: To achieve this, the AMF could, for example, use a random seed number for any process it uses when choosing the UE's 5G-TMSI.

5.9.5 AMF Name

An AMF is identified by an AMF Name. AMF Name is a globally unique FQDN, the structure of AMF Name FQDN is defined in TS 23.003 [19]. An AMF can be configured with one or more GUAMIs. At a given time, GUAMI with distinct AMF Pointer value is associated to one AMF name only.

5.9.6 Data Network Name (DNN)

A DNN is equivalent to an APN as defined in TS 23.003 [19]. Both identifiers have an equivalent meaning and carry the same information.

The DNN may be used e.g. to:

- Select a SMF and UPF(s) for a PDU Session.
- Select N6 interface(s) for a PDU Session.
- Determine policies to apply to this PDU Session.

The wildcard DNN is a value that can be used for the DNN field of Subscribed DNN list of Session Management Subscription data defined in clause 5.2.3.3 of TS 23.502 [3].

The wildcard DNN can be used with an S-NSSAI for operator to allow the subscriber to access any Data Network supported within the Network Slice associated with the S-NSSAI.

5.9.7 Internal-Group Identifier

The subscription data for an UE in UDR may associate the subscriber with groups. A group is identified by an Internal-Group Identifier.

NOTE 1: A UE can belong to a limited number of groups, the exact number is defined in stage 3 specifications.

NOTE 2: In this Release of the specification, the support of groups is only defined in non-roaming case.

The Internal-Group Identifier(s) corresponding to an UE are provided by the UDM to the SMF as part Session Management Subscription data and (when PCC applies to a PDU Session) by the SMF to the PCF. The SMF may use this information to apply local policies and to store this information in CDR. The PCF may use this information to enforce AF requests as described in clause 5.6.7.

The Internal-Group Identifier(s) corresponding to an UE are provided by the UDM to the AMF as part of Access and Mobility Subscription data. The AMF may use this information to apply local policies (such as Group specific NAS level congestion control defined in clause 5.19.7.5).

5.9.8 Generic Public Subscription Identifier

Generic Public Subscription Identifier (GPSI) is needed for addressing a 3GPP subscription in different data networks outside of the 3GPP system. The 3GPP system stores within the subscription data the association between the GPSI and the corresponding SUPI.

GPSIs are public identifiers used both inside and outside of the 3GPP system.

The GPSI is either an MSISDN or an External Identifier, see TS 23.003 [19]. If MSISDN is included in the subscription data, it shall be possible that the same MSISDN value is supported in both 5GS and EPS.

NOTE: There is no implied 1-to-1 relationship between GPSI and SUPI.

5.9.9 AMF UE NGAP ID

An AMF UE NGAP ID is an identifier used to identify the UE in AMF on N2 reference point. AMF allocates the AMF UE NGAP ID and send it to the 5G-AN. For the following N2 signalling interaction sent from 5G-AN to AMF, AMF UE NGAP ID is used to identify the UE at the AMF. AMF UE NGAP ID is unique per AMF set. AMF UE NGAP ID may be updated without AMF change, or with AMF change as specified at clause 5.21.2.2.

5.9.10 UE Radio Capability ID

The UE Radio Capability ID is a short pointer with format defined in TS 23.003 [19] that is used to uniquely identify a set of UE radio capabilities (i.e. UE Radio Capability information). The UE Radio Capability ID is assigned either by the serving PLMN or by the UE manufacturer, as follows:

- UE manufacturer-assigned: The UE Radio Capability ID may be assigned by the UE manufacturer in which case it includes a UE manufacturer identification (i.e. a Vendor ID). In this case, the UE Radio Capability ID uniquely identifies a set of UE radio capabilities for a UE by this manufacturer in any PLMN.

- PLMN-assigned: If a UE manufacturer-assigned UE Radio Capability ID is not used by the UE or the serving network, or it is not recognised by the serving PLMN UCMF, the UCMF may allocate UE Radio Capability IDs for the UE corresponding to each different set of UE radio capabilities the PLMN may receive from the UE at different times. In this case, the UE Radio Capability IDs the UE receives are applicable to the serving PLMN and uniquely identify the corresponding sets of UE radio capabilities in this PLMN. The PLMN assigned UE Radio Capability ID includes a Version ID in its format. The value of the Version ID is the one configured in the UCMF, at time the UE Radio Capability ID value is assigned. The Version ID value makes it possible to detect whether a UE Radio Capability ID is current or outdated.

NOTE: For the case the PLMN is configured to store PLMN assigned IDs in the UE manufacturer-assigned operation requested list defined in clause 5.4.4.1a, then the algorithm for assignment of PLMN-assigned UE Radio Capability ID shall assign different UE Radio Capability IDs for UEs with different TAC value.

The type of UE Radio Capability ID (UE manufacturer-assigned or PLMN-assigned) is distinguished when a UE Radio Capability ID is signalled.

5.10 Security aspects

5.10.1 General

The security features in the 5G System include:

- Authentication of the UE by the network and vice versa (mutual authentication between UE and network).

- Security context generation and distribution.

- User Plane data confidentiality and integrity protection.
- Control Plane signalling confidentiality and integrity protection.
- User identity confidentiality.
- Support of LI requirements as specified in TS 33.126 [35] subject to regional/national regulatory requirements, including protection of LI data (e.g., target list) that may be stored or transferred by an NF.

Detailed security related network functions for 5G are described in TS 33.501 [29].

5.10.2 Security Model for non-3GPP access

5.10.2.1 Signalling Security

When a UE is connected via a NG-RAN and via a standalone non-3GPP accesses, the multiple N1 instances are secured using independent NAS security contexts, each created based on the security context in the corresponding SEAF (e.g. in the common AMF when the UE is served by the same AMF) derived from the UE authentication.

5.10.3 PDU Session User Plane Security

The User Plane Security Enforcement information provides the NG-RAN with User Plane security policies for a PDU session. It indicates:

- whether UP integrity protection is:
  - Required: for all the traffic on the PDU Session UP integrity protection shall apply.
  - Preferred: for all the traffic on the PDU Session UP integrity protection should apply.
  - Not Needed: UP integrity protection shall not apply on the PDU Session.
- whether UP confidentiality protection is:
  - Required: for all the traffic on the PDU Session UP confidentiality protection shall apply.
  - Preferred: for all the traffic on the PDU Session UP confidentiality protection should apply.
  - Not Needed: UP confidentiality shall not apply on the PDU Session.

User Plane Security Enforcement information applies only over 3GPP access. Once determined at the establishment of the PDU Session the User Plane Security Enforcement information applies for the life time of the PDU Session.

The SMF determines at PDU session establishment a User Plane Security Enforcement information for the user plane of a PDU session based on:

- subscribed User Plane Security Policy which is part of SM subscription information received from UDM; and
- User Plane Security Policy locally configured per (DNN, S-NSSAI) in the SMF that is used when the UDM does not provide User Plane Security Policy information.
- The maximum supported data rate per UE for integrity protection for the DRBs, provided by the UE in the Integrity protection maximum data rate IE during PDU Session Establishment.

The SMF may, based on local configuration, reject the PDU Session Establishment request depending on the value of the maximum supported data rate per UE for integrity protection.

NOTE 1: Reasons to reject a PDU Session Establishment request can e.g. be that the UP Integrity Protection is determined to be "Required" while the maximum supported data rate per UE for integrity protection is less than the expected required data rate for the DN.

NOTE 2: The operator can take care to reduce the risk of such rejections when configuring the subscribed User Plane Security Policy for a DNN. For example, the operator may apply integrity protection "Required" only in scenarios where it can be assumed that the UE maximum supported data rate per UE for integrity protection is likely to be adequate for the DN.

The User Plane Security Policy provide the same level of information than User Plane Security Enforcement information.

User Plane Security Policy from UDM takes precedence over locally configured User Plane Security Policy.

The User Plane Security Enforcement information, including the maximum supported data rate for integrity protection provided by the UE, is communicated from SMF to the NG-RAN for enforcement as part of PDU session related information. If the UP Integrity Protection is determined to be "Required" or "Preferred", the SMF also provides the maximum supported data rate per UE for integrity protection as received in the Integrity protection maximum data rate IE. This takes place at establishment of a PDU Session or at activation of the user plane of a PDU Session. The NG-RAN rejects the establishment of UP resources for the PDU Session when it cannot fulfil User Plane Security Enforcement information with a value of Required. The NG-RAN may also take the maximum supported data rate per UE for integrity protection into account in its decision on whether to accept or reject the establishment of UP resources. In this case the SMF releases the PDU Session. The NG-RAN notifies the SMF when it cannot fulfil a User Plane Security Enforcement with a value of Preferred.

NOTE 3: For example, the NG-RAN cannot fulfil requirements in User Plane Security Enforcement information with UP integrity protection set to "Required" when it cannot negotiate UP integrity protection with the UE.

It is responsibility of the NG-RAN to enforce that the maximum UP integrity protection data rate delivered to the UE in downlink is not exceeding the maximum supported data rate for integrity protection.

It is expected that generally the UP integrity protection data rate applied by the UE in uplink will not exceed the indicated maximum supported data rate, but the UE is not required to perform strict rate enforcement.

User Plane Security Enforcement information and the maximum supported data rate per UE for integrity protection is communicated from source to target NG-RAN node at handover. If the target RAN node cannot support requirements in User Plane Security Enforcement information, the target RAN node rejects the request to setup resources for the PDU Session. In this case the PDU Session is not handed over to the target RAN node and the PDU Session is released.

PDU Sessions with UP integrity protection of the User Plane Security Enforcement information set to Required are not handed over to EPS:

- In the case of mobility without N26, the PGW-C+SMF shall reject a PDN connectivity request in EPS with handover indication if the UP integrity protection of the User Plane Security Enforcement is set to Required.

NOTE 4: As described in clause 5.17.2.3.3, the UE does not know before trying to move a given PDU Session to EPC, whether that PDU session can be transferred to EPC.

- In the case of mobility with N26 to EPS, the source NG-RAN ensures that a PDU Session with UP integrity protection of the User Plane Security Enforcement information set to Required is not handed over to EPS.

PDU Sessions with UP confidentiality protection of the User Plane Security Enforcement information set to Required and UP integrity protection of the User Plane Security Enforcement information not set to Required, are allowed to be handed over to EPS regardless of how UP confidentiality protection applies in EPS.

In the case of dual connectivity, the Integrity Protection is set to "Preferred", the Master NG-RAN node may notify the SMF when it cannot fulfil a User Plane Security Enforcement with a value of Preferred. The SMF handling of the PDU session with respect to the Integrity Protection status is up to SMF implementation decision.

5.11 Support for Dual Connectivity, Multi-Connectivity

5.11.1 Support for Dual Connectivity

Dual Connectivity involves two radio network nodes in providing radio resources to a given UE (with active radio bearers), while a single N2 termination point exists for the UE between an AMF and the RAN. The RAN architecture and related functions to support Dual Connectivity is further described in RAN specifications (e.g. TS 37.340 [31]).

The RAN node at which the N2 terminates, performs all necessary N2 related functions such as mobility management, relaying of NAS signalling, etc. and manages the handling of user plane connection (e.g. transfer over N3). It is called the Master RAN Node. It may use resources of another RAN node, the Secondary RAN node, to exchange User Plane traffic of an UE. Master RAN node takes into account the RSN to determine if dual connectivity shall be set up and ensure appropriate PDU session handling ensures fully redundant user plane path as described in clause 5.33.2.1.

If the UE has Mobility Restriction (either signalled from the UDM, or, locally generated by the Serving PLMN policy in the AMF) the AMF signals these restrictions to the Master RAN Node as Mobility Restriction List; This may prevent the Master RAN node from setting up a Dual Connectivity for an UE.

NOTE 1: Subject to policies in the NG-RAN, configuration of Dual Connectivity for a Data Radio Bearer can also be based on the Network Slice that the PDU Session belongs to.

Dual Connectivity provides the possibility for the Master node RAN to request SMF:

- For some or all PDU Sessions of an UE: Direct all the DL User Plane traffic of the PDU Session to the either the Master RAN Node or to the Secondary RAN Node. In this case, there is a single N3 tunnel termination at the RAN for such PDU Session.

NOTE 2: The terminating RAN Node, can decide to keep traffic for specific QFI(s) in a PDU Session for a UE on a single RAT, or split them across the two RATs.

- For some other PDU Sessions of an UE: Direct the DL User Plane traffic of some QoS Flows of the PDU Session to the Secondary (respectively Master) RAN Node while the remaining QoS Flows of the PDU Session are directed to the Master (respectively Secondary) RAN Node. In this case there are, irrespective of the number of QoS Flows, two N3 tunnel terminations at the RAN for such PDU Session.

The Master RAN may create and change this assignment for the user plane of a PDU Session at any time during the life time of the PDU Session;

In both cases, a single PDU Session Id is used to identify the PDU Session.

Additional functional characteristics are:

- User location information reporting is based on the identity of the cell that is serving the UE in the Master RAN node.

- Path update signalling related with Dual Connectivity and UPF re-allocation cannot occur at the same time.

5.12 Charging

5.12.1 General

The 5GC charging supports collection and reporting of charging information for network resource usage, as defined in TS 32.240 [41]. The CHF and the interfaces of the CHF are defined in TS 32.240 [41].

The SMF supports the interactions towards the charging system, as defined in TS 32.240 [41]. The UPF supports functionality to collect and report usage data to SMF. The N4 reference point supports the SMF control of the UPF collection and reporting of usage data. The AMF supports interactions towards the charging system, as defined in TS 32.256 [114]. The SMSF supports interactions towards the charging system, as defined in TS 32.274 [118].

5.12.2 Usage Data Reporting for Secondary RAT

When NG-RAN is deployed in dual connectivity configuration, the HPLMN or VPLMN operator may wish to record the data volume sent and received on the Secondary RAT.

In order to reduce the complexity of this procedure, the following principles are used in this release:

a) The PLMN locally activates the Secondary RAT Usage Data Reporting by NG-RAN OAM. The activation is based on configuration in NG-RAN and NG-RAN determines whether the data volume report will contain data volumes consumed for the whole PDU Session or for selected QoS flows or both as described in TS 38.413 [34].

The activation can happen separately for Data Volume Reporting of NR in licensed or unlicensed spectrum and E-UTRA in licensed or unlicensed spectrum. If the PLMN uses this feature, it should ensure that this functionality is supported by all NG-RAN nodes that support NR or E-UTRA as a Secondary RAT.

b) Depending on its configuration the NG-RAN reports uplink and downlink data volumes to the 5GC for the Secondary RAT (including the using of unlicensed spectrum for NR or E-UTRA) for the PDU Session or for selected QoS flows or both and per time interval.

c) During Xn handover and N2 handover, the source NG-RAN node reports the data volume to the 5GC. The reported data volume excludes data forwarded to the target RAN node.

d) At the time of NG connection release, Secondary Node change/release, deactivation of UP connection for a PDU Session, the NG-RAN node reports the data volumes to the 5GC.

e) To assist "partial CDR" generation, NG-RAN OAM can instruct the NG-RAN to also make periodic reports (as described in clause 5.12.3) if no event has triggered a report before the period expires.

NOTE 2: The timing of these periodic NG-RAN reports is not expected to align with the timing of partial CDR generation. Hence the frequency of NG-RAN reports might be greater than that of partial CDR generation.

NOTE 3: RAN needs to be able to partition the measurements in a report to indicate usage that occurred before and after an absolute time. An example of the absolute time is that RAN is configured to partition data usage reports that occurred before and after midnight.

5.12.3 Secondary RAT Periodic Usage Data Reporting Procedure

Periodic reporting of the Secondary RAT usage data is an optional function. When NG-RAN, as defined in bullet e) of clause 5.12.12, is configured with a "time interval for Secondary RAT usage data reporting", the NG-RAN shall send a RAN Usage Data Report message for periodic reporting purposes to the SMF only when the timer expires for a UE for which Secondary RAT usage data reporting is ongoing. The timer runs from the last usage reporting for the UE.

5.13 Support for Edge Computing

Edge computing enables operator and 3rd party services to be hosted close to the UE's access point of attachment, so as to achieve an efficient service delivery through the reduced end-to-end latency and load on the transport network.

NOTE: Edge Computing typically applies to non-roaming and LBO roaming scenarios.

The 5G Core Network selects a UPF close to the UE and executes the traffic steering from the UPF to the local Data Network via a N6 interface. This may be based on the UE's subscription data, UE location, the information from Application Function (AF) as defined in clause 5.6.7, policy or other related traffic rules.

Due to user or Application Function mobility, the service or session continuity may be required based on the requirements of the service or the 5G network.

The 5G Core Network may expose network information and capabilities to an Edge Computing Application Function.

NOTE: Depending on the operator deployment, certain Application Functions can be allowed to interact directly with the Control Plane Network Functions with which they need to interact, while the other Application Functions need to use the external exposure framework via the NEF (see clause 6.2.10 for details).

Edge computing can be supported by one or a combination of the following enablers:

- User plane (re)selection: the 5G Core Network (re)selects UPF to route the user traffic to the local Data Network as described in clause 6.3.3;

- Local Routing and Traffic Steering: the 5G Core Network selects the traffic to be routed to the applications in the local Data Network;

  - this includes the use of a single PDU Session with multiple PDU Session Anchor(s) (UL CL / IP v6 multi-homing) as described in clause 5.6.4.

- Session and service continuity to enable UE and application mobility as described in clause 5.6.9;

- An Application Function may influence UPF (re)selection and traffic routing via PCF or NEF as described in clause 5.6.7;
- Network capability exposure: 5G Core Network and Application Function to provide information to each other via NEF as described in clause 5.20 or directly as described in TS 23.502 [3] clause 4.15;
- QoS and Charging: PCF provides rules for QoS Control and Charging for the traffic routed to the local Data Network;
- Support of Local Area Data Network: 5G Core Network provides support to connect to the LADN in a certain area where the applications are deployed as described in clause 5.6.5.

5.14 Policy Control

The policy and charging control framework for the 5G System is defined in TS 23.503 [45].

5.15 Network slicing

5.15.1 General

A Network Slice instance is defined within a PLMN and shall include:

- the Core Network Control Plane and User Plane Network Functions, as described in clause 4.2,

and, in the serving PLMN, at least one of the following:

- the NG-RAN described in TS 38.300 [27];
- the N3IWF or TNGF functions to the non-3GPP Access Network described in clause 4.2.8.2 or the TWIF functions to the trusted WLAN in the case of support of N5CW devices described in clause 4.2.8.5;
- the W-AGF function to the Wireline Access Network described in clause 4.2.8.4.

The 5G System deployed in a PLMN shall always support the procedures, information and configurations specified to support Network Slice instance selection in the present document, TS 23.502 [3] and TS 23.503 [45].

Network slicing support for roaming is described in clause 5.15.6.

Network slices may differ for supported features and network functions optimisations, in which case such Network Slices may have e.g. different S-NSSAIs with different Slice/Service Types (see clause 5.15.2.1). The operator can deploy multiple Network Slices delivering exactly the same features but for different groups of UEs, e.g. as they deliver a different committed service and/or because they are dedicated to a customer, in which case such Network Slices may have e.g. different S-NSSAIs with the same Slice/Service Type but different Slice Differentiators (see clause 5.15.2.1).

The network may serve a single UE with one or more Network Slice instances simultaneously via a 5G-AN regardless of the access type(s) over which the UE is registered (i.e. 3GPP Access and/or N3GPP Access). The AMF instance serving the UE logically belongs to each of the Network Slice instances serving the UE, i.e. this AMF instance is common to the Network Slice instances serving a UE.

NOTE 1: Number of simultaneous connection of Network Slice instances per UE is limited by the number of S-NSSAIs in the Requested/Allowed NSSAI as described in clause 5.15.2.1.

NOTE 2: In this Release of the specification it is assumed that in any (home or visited) PLMN it is always possible to select an AMF that can serve any combination of S-NSSAIs that will be provided as an Allowed NSSAI.

The selection of the set of Network Slice instances for a UE is triggered by the first contacted AMF in a Registration procedure normally by interacting with the NSSF, and can lead to a change of AMF. This is further described in clause 5.15.5.

A PDU Session belongs to one and only one specific Network Slice instance per PLMN. Different Network Slice instances do not share a PDU Session, though different Network Slice instances may have slice-specific PDU Sessions using the same DNN.

During the Handover procedure the source AMF selects a target AMF by interacting with the NRF as specified in clause 6.3.5.

5.15.2 Identification and selection of a Network Slice: the S-NSSAI and the NSSAI

5.15.2.1 General

An S-NSSAI identifies a Network Slice.

An S-NSSAI is comprised of:

- A Slice/Service type (SST), which refers to the expected Network Slice behaviour in terms of features and services;
- A Slice Differentiator (SD), which is optional information that complements the Slice/Service type(s) to differentiate amongst multiple Network Slices of the same Slice/Service type.

An S-NSSAI can have standard values (i.e. such S-NSSAI is only comprised of an SST with a standardised SST value, see clause 5.15.2.2, and no SD) or non-standard values (i.e. such S-NSSAI is comprised of either both an SST and an SD or only an SST without a standardised SST value and no SD). An S-NSSAI with a non-standard value identifies a single Network Slice within the PLMN with which it is associated. An S-NSSAI with a non-standard value shall not be used by the UE in access stratum procedures in any PLMN other than the one to which the S-NSSAI is associated.

The S-NSSAIs in the NSSP of the URSP rules (see TS 23.503 [45] clause 6.6.2) and in the Subscribed S-NSSAIs (see clause 5.15.3) contain only HPLMN S-NSSAI values.

The S-NSSAIs in the Configured NSSAI, the Allowed NSSAI (see clause 5.15.4.1), the Requested NSSAI (see clause 5.15.5.2.1), the Rejected S-NSSAIs contain only values from the Serving PLMN. The Serving PLMN can be the HPLMN or a VPLMN.

The S-NSSAI(s) in the PDU Session Establishment contain one Serving PLMN S-NSSAI value and in addition may contain a corresponding HPLMN S-NSSAI value to which this first value is mapped (see clause 5.15.5.3).

The optional mapping of Serving PLMN S-NSSAIs to HPLMN S-NSSAIs contains Serving PLMN S-NSSAI values and corresponding mapped HPLMN S-NSSAI values.

The NSSAI is a collection of S-NSSAIs. An NSSAI may be a Configured NSSAI, a Requested NSSAI or an Allowed NSSAI. There can be at most eight S-NSSAIs in Allowed and Requested NSSAIs sent in signalling messages between the UE and the Network. The Requested NSSAI signalled by the UE to the network allows the network to select the Serving AMF, Network Slice(s) and Network Slice instance(s) for this UE, as specified in clause 5.15.5.

Based on the operator's operational or deployment needs, a Network Slice instance can be associated with one or more S-NSSAIs, and an S-NSSAI can be associated with one or more Network Slice instances. Multiple Network Slice instances associated with the same S-NSSAI may be deployed in the same or in different Tracking Areas. When multiple Network Slice instances associated with the same S-NSSAI are deployed in the same Tracking Areas, the AMF instance serving the UE may logically belong to (i.e. be common to) more than one Network Slice instance associated with this S-NSSAI.

In a PLMN, when an S-NSSAI is associated with more than one Network Slice instance, one of these Network Slice instances, as a result of the Network Slice instance selection procedure defined in clause 5.15.5, serves a UE that is allowed to use this S-NSSAI. For any S-NSSAI, the network may at any one time serve the UE with only one Network Slice instance associated with this S-NSSAI until cases occur where e.g. this Network Slice instance is no longer valid in a given Registration Area, or a change in UE's Allowed NSSAI occurs, etc. In such cases, procedures mentioned in clause 5.15.5.2.2 or clause 5.15.5.2.3 apply.

Based on the Requested NSSAI (if any) and the Subscription Information, the 5GC is responsible for selection of a Network Slice instance(s) to serve a UE including the 5GC Control Plane and User Plane Network Functions corresponding to this Network Slice instance(s).

The (R)AN may use Requested NSSAI in access stratum signalling to handle the UE Control Plane connection before the 5GC informs the (R)AN of the Allowed NSSAI. The Requested NSSAI is used by the RAN for AMF selection, as

described in clause 6.3.5. The UE shall not include the Requested NSSAI in the RRC Resume when the UE asks to resume the RRC connection and is CM-CONNECTED with RRC Inactive state.

When a UE is successfully registered over an Access Type, the CN informs the (R)AN by providing the Allowed NSSAI for the corresponding Access Type.

NOTE: The details of how the RAN uses NSSAI information are described in TS 38.300 [27].

5.15.2.2 Standardised SST values

Standardized SST values provide a way for establishing global interoperability for slicing so that PLMNs can support the roaming use case more efficiently for the most commonly used Slice/Service Types.

The SSTs which are standardised are in the following Table 5.15.2.2-1.

Table 5.15.2.2-1 - Standardised SST values

Slice/Service type	SST value	Characteristics
eMBB	1	Slice suitable for the handling of 5G enhanced Mobile Broadband.
URLLC	2	Slice suitable for the handling of ultra- reliable low latency communications.
MIoT	3	Slice suitable for the handling of massive IoT.
V2X	4	Slice suitable for the handling of V2X services.

NOTE: The support of all standardised SST values is not required in a PLMN. Services indicated in this table for each SST value can also be supported by means of other SSTs.

5.15.3 Subscription aspects

The Subscription Information shall contain one or more S-NSSAIs i.e. Subscribed S-NSSAIs. Based on operator's policy, one or more Subscribed S-NSSAIs can be marked as a default S-NSSAI. If an S-NSSAI is marked as default, then the network is expected to serve the UE with a related applicable Network Slice instance when the UE does not send any permitted S-NSSAI to the network in a Registration Request message as part of the Requested NSSAI.

The Subscription Information for each S-NSSAI may contain:

- a Subscribed DNN list and one default DNN; and
- the indication whether the S-NSSAI is marked as default Subscribed S-NSSAI; and
- the indication whether the S-NSSAI is subject to Network Slice-Specific Authentication and Authorization and associated AAA Server Address.

The network verifies the Requested NSSAI the UE provides in the Registration Request against the Subscription Information. For the S-NSSAIs subject to Network Slice-Specific Authentication and Authorization the clause 5.15.10 applies.

NOTE 1: It is recommended that at least one of the Subscribed S-NSSAIs marked as default S-NSSAI is not subject to Network Slice-specific Authentication and Authorization, in order to ensure access to services even when Network Slice-specific Authentication and Authorization fails.

NOTE 2: It is recommended to minimize the number of Subscribed S-NSSAIs in subscriptions for NB-IoT capable UEs to minimize overhead for signalling a large number of S-NSSAIs in Requested NSSAI in RRC and NAS via NB-IoT.

In roaming case, the UDM shall provide to the VPLMN only the S-NSSAIs from the Subscribed S-NSSAIs the HPLMN allows for the UE in the VPLMN.

NOTE 3: Network slice instances supporting an S-NSSAI subject to Network Slice-Specific Authentication and Authorization need to be deployed with AMFs supporting Network Slice-Specific Authentication and Authorization, otherwise S-NSSAIs requiring Network Slice-Specific Authentication and Authorization would be incorrectly allowed without execution of Network Slice-Specific Authentication and Authorization.

When the UDM updates the Subscribed S-NSSAI(s) to the serving AMF, based on configuration in this AMF, the AMF itself or the NSSF determines the mapping of the Configured NSSAI for the Serving PLMN and/or Allowed NSSAI to the Subscribed S-NSSAI(s). The serving AMF then updates the UE with the above information as described in clause 5.15.4.

5.15.4 UE NSSAI configuration and NSSAI storage aspects

5.15.4.1 General

5.15.4.1.1 UE Network Slice configuration

The Network Slice configuration information contains one or more Configured NSSAI(s). A Configured NSSAI may either be configured by a Serving PLMN and apply to the Serving PLMN, or may be a Default Configured NSSAI configured by the HPLMN and that applies to any PLMNs for which no specific Configured NSSAI has been provided to the UE. There is at most one Configured NSSAI per PLMN.

NOTE 1: The value(s) used in the Default Configured NSSAI are expected to be commonly decided by all roaming partners, e.g. by the use of values standardized by 3GPP or other bodies.

The Default Configured NSSAI, if it is configured in the UE, is used by the UE in a Serving PLMN only if the UE has no Configured NSSAI for the Serving PLMN.

The Configured NSSAI of a PLMN may include S-NSSAIs that have standard values or PLMN-specific values.

The Configured NSSAI for the Serving PLMN includes the S-NSSAI values which can be used in the Serving PLMN and may be associated with mapping of each S-NSSAI of the Configured NSSAI to one or more corresponding HPLMN S-NSSAI values.

The UE may be pre-configured with the Default Configured NSSAI. The UE may be provisioned/updated with the Default Configured NSSAI, determined by the UDM in the HPLMN, using the UE Parameters Update via UDM Control Plane procedure defined in clause 4.20 of TS 23.502 [3]. Each S-NSSAI in the Default Configured NSSAI may have a corresponding S-NSSAI as part of the Subscribed S-NSSAI(s). Consequently, if the Subscribed S-NSSAI(s) which are also present in the Default Configured NSSAI are updated the UDM should update the Default Configured NSSAI in the UE.

In the HPLMN, the S-NSSAIs in the Configured NSSAI provided as described in clause 5.15.4.2, at the time when they are provided to the UE, shall match the Subscribed S-NSSAIs for the UE. When the Subscribed S-NSSAI(s) are updated (i.e. some existing S-NSSAIs are removed and/or some new S-NSSAIs are added) and one or more are applicable to the Serving PLMN the UE is registered in, as described in clause 5.15.3, or when the associated mapping is updated the AMF shall update the UE with the Configured NSSAI for the Serving PLMN and/or Allowed NSSAI and/or the associated mapping to HPLMN S-NSSAIs (see clause 5.15.4.2). When there is the need to update the Allowed NSSAI, the AMF shall provide the UE with the new Allowed NSSAI and the associated mapping to HPLMN S-NSSAIs, unless the AMF cannot determine the new Allowed NSSAI (e.g. all S-NSSAIs in the old Allowed NSSAI have been removed from the Subscribed S-NSSAIs), in which case the AMF shall not send any Allowed NSSAI to the UE but indicate to the UE to perform a Registration procedure. If the UE is in a CM-IDLE state, the AMF may trigger Network Triggered Service Request or wait until the UE is in a CM-CONNECTED state as described in clause 4.2.4.2, TS 23.502 [3].

When providing a Requested NSSAI to the network upon registration, the UE in a given PLMN only includes and uses S-NSSAIs applying to this PLMN. The mapping of S-NSSAIs of the Requested NSSAI to HPLMN S-NSSAIs may also be provided (see clause 5.15.4.1.2 for when this is needed). The S-NSSAIs in the Requested NSSAI are part of the Configured and/or Allowed NSSAIs applicable for this PLMN, when they are available. If no Configured NSSAI and Allowed NSSAI for the PLMN are available, the S-NSSAIs in the Requested NSSAI correspond to the Default Configured NSSAI, if configured in the UE. Upon successful completion of a UE's Registration procedure over an Access Type, the UE obtains from the AMF an Allowed NSSAI for this Access Type, which includes one or more S-NSSAIs and, if needed (see clause 5.15.4.1.2 for when this is needed), their mapping to the HPLMN S-NSSAIs. These

S-NSSAIs are valid for the current Registration Area and Access Type provided by the AMF the UE has registered with and can be used simultaneously by the UE (up to the maximum number of simultaneous Network Slice instances or PDU Sessions).

The UE might also obtain one or more rejected S-NSSAIs with cause and validity of rejection from the AMF. An S-NSSAI may be rejected:

- for the entire PLMN; or
- for the current Registration Area.

While it remains RM-REGISTERED in the PLMN and regardless of the Access Type, the UE shall not re-attempt to register to an S-NSSAI rejected for the entire PLMN until this rejected S-NSSAI is deleted as specified below.

While it remains RM-REGISTERED in the PLMN, the UE shall not re-attempt to register to an S-NSSAI rejected in the current Registration Area until it moves out of the current Registration Area.

NOTE 2: The details and more cases of S-NSSAI rejection are described in TS 24.501 [47].

S-NSSAIs that the UE provides in the Requested NSSAI which are neither in the Allowed NSSAI nor provided as a rejected S-NSSAI, shall, by the UE, not be regarded as rejected, i.e. the UE may request to register these S-NSSAIs again next time the UE sends a Requested NSSAI.

The UE stores (S-)NSSAIs as follows:

- When provisioned with a Configured NSSAI for a PLMN and/or a mapping of Configured NSSAI to HPLMN S-NSSAIs, or when requested to remove the configuration due to network slicing subscription change, the UE shall:
  - replace any stored (old) Configured NSSAI for this PLMN with the new Configured NSSAI for this PLMN (if applicable); and
  - delete any stored associated mapping of this old Configured NSSAI for this PLMN to HPLMN S-NSSAIs and, if present and applicable, store the mapping of Configured NSSAI to HPLMN S-NSSAIs; and
  - delete any stored rejected S-NSSAI for this PLMN;
  - keep the received Configured NSSAI for a PLMN (if applicable) and associated mapping to HPLMN S-NSSAIs (if applicable) stored in the UE, even when registering in another PLMN, until a new Configured NSSAI for this PLMN and/or associated mapping are provisioned in the UE, or until the network slicing subscription changes, as described in clause 5.15.4.2. The number of Configured NSSAIs and associated mapping to be kept stored in the UE for PLMNs other than the HPLMN is up to UE implementation. A UE shall at least be capable of storing a Configured NSSAI for the serving PLMN including any necessary mapping of the Configured NSSAI for the Serving PLMN to HPLMN S-NSSAIs and the Default Configured NSSAI.
- The Allowed NSSAI received in a Registration Accept message or a UE Configuration Update Command applies to a PLMN when at least a TAI of this PLMN is included in the RA/TAI list included in this Registration Accept message or UE Configuration Update Command. If the UE Configuration Update Command contains an Allowed NSSAI but not a TAI List, then the last received RA/TAI list applies for the decision on which PLMN(s) the Allowed NSSAI is applicable. If received, the Allowed NSSAI for a PLMN and Access Type and any associated mapping of this Allowed NSSAI to HPLMN S-NSSAIs shall be stored in the UE. The UE should store this Allowed NSSAI and any associated mapping of this Allowed NSSAI to HPLMN S-NSSAIs also when the UE is turned off, or until the network slicing subscription changes, as described in clause 5.15.4.2:

NOTE 3: Whether the UE stores the Allowed NSSAI and any associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs also when the UE is turned off is left to UE implementation.

- When a new Allowed NSSAI for a PLMN and any associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs are received over an Access Type, the UE shall:
  - replace any stored (old) Allowed NSSAI and any associated mapping for these PLMN and Access Type with this new Allowed NSSAI; and
  - delete any stored associated mapping of this old Allowed NSSAI for this PLMN to HPLMN S-NSSAIs and, if present, store the associated mapping of this new Allowed NSSAI to HPLMN S-NSSAIs;

- If received, an S-NSSAI rejected for the entire PLMN shall be stored in the UE while RM-REGISTERED in this PLMN regardless of the Access Type or until it is deleted.

- If received, an S-NSSAI rejected for the current Registration Area shall be stored in the UE while RM-REGISTERED until the UE moves out of the current Registration Area or until the S-NSSAI is deleted.

NOTE 4: The storage aspects of rejected S-NSSAIs are described in TS 24.501 [47].

- If received, the Pending NSSAI shall be stored in the UE as described in TS 24.501 [47].

5.15.4.1.2 Mapping of S-NSSAIs values in the Allowed NSSAI and in the Requested NSSAI to the S-NSSAIs values used in the HPLMN

One or more S-NSSAIs in an Allowed NSSAI provided to the UE can have values which are not part of the UE's current Network Slice configuration information for the Serving PLMN. In this case, the network provides the Allowed NSSAI together with the mapping of each S-NSSAI of the Allowed NSSAI to the corresponding S-NSSAI of the HPLMN. This mapping information allows the UE to associate Applications to S-NSSAIs of the HPLMN as per NSSP of the URSP rules or as per the UE Local Configuration (if available), as defined in clause 6.1.2.2.1 of TS 23.503 [45] and to the corresponding S-NSSAI from the Allowed NSSAI.

In roaming case, the UE may need to provide the mapping of S-NSSAIs values in the Requested NSSAI to the corresponding S-NSSAI values used in the HPLMN. These values are found in the mapping previously received from the Serving PLMN of the S-NSSAIs of the Configured NSSAI for the Serving PLMN or of the S-NSSAIs of the Allowed NSSAI for the Serving PLMN and Access Type to the corresponding S-NSSAIs values used in the HPLMN.

5.15.4.2 Update of UE Network Slice configuration

At any time, the AMF may provide the UE with a new Configured NSSAI for the Serving PLMN, associated with mapping of the Configured NSSAI to HPLMN S-NSSAIs as specified in clause 5.15.4.1. The Configured NSSAI for the Serving PLMN and the mapping information is either determined in the AMF (if based on configuration, the AMF is allowed to determine the Network Slice configuration for the whole PLMN) or by the NSSF. The AMF provides an updated Configured NSSAI as specified in TS 23.502 [3], clause 4.2.4 UE Configuration Update procedure.

If the HPLMN performs the configuration update of a UE registered in the HPLMN (e.g. due to a change in the Subscribed S-NSSAI(s)), this results in updates to the Configured NSSAI for the HPLMN. Updates to the Allowed NSSAI and/or, if present, to the associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs are also possible if the configuration update affects S-NSSAI(s) in the current Allowed NSSAI.

If the VPLMN performs the configuration update of a UE registered in the VPLMN (e.g. due to a change in the Subscribed S-NSSAI(s), the associated mapping is updated), this results in updates to the Configured NSSAI for the Serving PLMN and/or to the associated mapping of the Configured NSSAI for the Serving PLMN to HPLMN S-NSSAIs. Updates to the Allowed NSSAI and/or to the associated mapping of the Allowed NSSAI to HPLMN S-NSSAIs are also possible if the configuration update affects S-NSSAI(s) in the current Allowed NSSAI.

A UE for which the Configured NSSAI for the Serving PLMN has been updated as described in clause 5.15.4.1 and has been requested to perform a Registration procedure, shall initiate a Registration procedure to receive a new valid Allowed NSSAI (see clause 5.15.5.2.2).

When the subscribed S-NSSAIs change, a UDR flag is set in the HPLMN to make sure the current PLMN (or, if the UE was not reachable, the next serving PLMN) is informed by the UDM that the subscription data for network slicing has changed. The AMF, when it receives the indication from the UDM subscription has changed, indicates the UE that subscription has changed and uses any updated subscription information from the UDM to update the UE. Once the AMF updates the UE and obtains an acknowledgment from the UE, the AMF informs the UDM that the configuration update was successful and the UDM clears the flag in the UDR. If the UE is in a CM-IDLE state, the AMF may trigger Network Triggered Service Request or wait until the UE is in a CM-CONNECTED state as described in clause 4.2.4.2, TS 23.502 [3].

If the UE receives indication from the AMF that Network Slicing subscription has changed, the UE locally deletes the network slicing information it has for all PLMNs, except the Default Configured NSSAI (if present). It also updates the current PLMN network slicing configuration information with any received values from the AMF.

The update of URSP rules (which include the NSSP), if necessary at any time, is described in TS 23.503 [45].

5.15.5 Detailed Operation Overview

5.15.5.1 General

The establishment of User Plane connectivity to a Data Network via a Network Slice instance(s) comprises two steps:

- performing a RM procedure to select an AMF that supports the required Network Slices.
- establishing one or more PDU Session to the required Data network via the Network Slice instance(s).

5.15.5.2 Selection of a Serving AMF supporting the Network Slices

5.15.5.2.1 Registration to a set of Network Slices

When a UE registers over an Access Type with a PLMN, if the UE has either or both of:

- a Configured NSSAI for this PLMN;
- an Allowed NSSAI for this PLMN and Access Type;

the UE shall provide to the network, in AS layer under the conditions described in clause 5.15.9 and in NAS layer, a Requested NSSAI containing the S-NSSAI(s) corresponding to the Network Slice(s) to which the UE wishes to register, unless they are stored in the UE in the Pending NSSAI.

The Requested NSSAI shall be one of:

- the Default Configured NSSAI, i.e. if the UE has no Configured NSSAI nor an Allowed NSSAI for the serving PLMN;
- the Configured-NSSAI, or a subset thereof as described below, e.g. if the UE has no Allowed NSSAI for the Access Type for the serving PLMN;
- the Allowed-NSSAI for the Access Type over which the Requested NSSAI is sent, or a subset thereof; or
- the Allowed-NSSAI for the Access Type over which the Requested NSSAI is sent, or a subset thereof, plus one or more S-NSSAIs from the Configured-NSSAI not yet in the Allowed NSSAI for the Access Type as described below.

NOTE 1: If the UE wishes to register only a subset of the S-NSSAIs from the Configured NSSAI or the Allowed NSSAI, to be able to register with some Network Slices e.g. to establish PDU Sessions for some application(s), and the UE uses the URSP rules (which includes the NSSP) or the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45], then the UE uses applicable the URSP rules or the UE Local Configuration to ensure that the S-NSSAIs included in the Requested NSSAI are not in conflict with the URSP rules or with the UE Local Configuration.

The subset of S-NSSAIs in the Configured-NSSAI provided in the Requested NSSAI consists of one or more S-NSSAI(s) in the Configured NSSAI applicable to this PLMN, if one is present, and for which no corresponding S-NSSAI is already present in the Allowed NSSAI for the access type for this PLMN. The UE shall not include in the Requested NSSAI any S-NSSAI that is currently rejected by the network (i.e. rejected in the current registration area or rejected in the PLMN). For the registration to a PLMN for which neither a Configured NSSAI applicable to this PLMN or an Allowed NSSAI are present, the S-NSSAIs provided in the Requested NSSAI correspond to the S-NSSAI(s) in the Default Configured NSSAI unless the UE has HPLMN S-NSSAI for established PDU Session(s) in which case the HPLMN S-NSSAI(s) shall be provided in the mapping of Requested NSSAI in the NAS Registration Request message, with no corresponding VPLMN S-NSSAI in the Requested NSSAI.

NOTE 2: In this release of the specifications the support of the continuation of PDU sessions upon mobility to a target 5GS PLMN or from EPS to the 5GS when neither the Configured NSSAI nor the Allowed NSSAI are available for the target PLMN, is not guaranteed.

When a UE registers over an Access Type with a PLMN, the UE shall also indicate in the Registration Request message when the Requested NSSAI is based on the Default Configured NSSAI.

The UE shall include the Requested NSSAI in the RRC Connection Establishment and in the establishment of the connection to the N3IWF/TNGF (as applicable) and in the NAS Registration procedure messages subject to conditions

set out in clause 5.15.9. However, the UE shall not indicate any NSSAI in RRC Connection Establishment or Initial NAS message unless it has either a Configured NSSAI for the corresponding PLMN, an Allowed NSSAI for the corresponding PLMN and Access Type, or the Default Configured NSSAI. If the UE has HPLMN S-NSSAI(s) for established PDU Session(s), the HPLMN S-NSSAI(s) shall be provided in the mapping of Requested NSSAI in the NAS Registration Request message, independent of whether the UE has the corresponding VPLMN S-NSSAI. The (R)AN shall route the NAS signalling between this UE and an AMF selected using the Requested NSSAI obtained during RRC Connection Establishment or connection to N3IWF/TNGF respectively. If the (R)AN is unable to select an AMF based on the Requested NSSAI, it routes the NAS signalling to an AMF from a set of default AMFs. In the NAS signalling, if available, the UE provides the mapping of each S-NSSAI of the Requested NSSAI to a corresponding HPLMN S-NSSAI.

When a UE registers with a PLMN, if for this PLMN the UE has not included a Requested NSSAI nor a GUAMI while establishing the connection to the (R)AN, the (R)AN shall route all NAS signalling from/to this UE to/from a default AMF. When receiving from the UE a Requested NSSAI and a 5G-S-TMSI or a GUAMI in RRC Connection Establishment or in the establishment of connection to N3IWF/TNGF, if the 5G-AN can reach an AMF corresponding to the 5G-S-TMSI or GUAMI, then 5G-AN forwards the request to this AMF. Otherwise, the 5G-AN selects a suitable AMF based on the Requested NSSAI provided by the UE and forwards the request to the selected AMF. If the 5G-AN is not able to select an AMF based on the Requested NSSAI, then the request is sent to a default AMF.

When the AMF selected by the AN during Registration Procedure receives the UE Registration request, or after an AMF selection by MME (i.e. during EPS to 5GS handover) the AMF receives S-NSSAI(s) from PGW-C+SMF in 5GC:

- As part of the Registration procedure described in TS 23.502 [3], clause 4.2.2.2.2, or as part of the EPS to 5GS handover using N26 interface procedure described in clause 4.11.1.2.2 in TS 23.502 [3], the AMF may query the UDM to retrieve UE subscription information including the Subscribed S-NSSAIs.

- The AMF verifies whether the S-NSSAI(s) in the Requested NSSAI or the S-NSSAI(s) received from PGW-C+SMF are permitted based on the Subscribed S-NSSAIs (to identify the Subscribed S-NSSAIs the AMF may use the mapping to HPLMN S-NSSAIs provided by the UE, in the NAS message, for each S-NSSAI of the Requested NSSAI).

- When the UE context in the AMF does not yet include an Allowed NSSAI for the corresponding Access Type, the AMF queries the NSSF (see (B) below for subsequent handling), except in the case when, based on configuration in this AMF, the AMF is allowed to determine whether it can serve the UE (see (A) below for subsequent handling). The IP address or FQDN of the NSSF is locally configured in the AMF.

NOTE 3: The configuration in the AMF depends on operator's policy.

- When the UE context in the AMF already includes an Allowed NSSAI for the corresponding Access Type, based on the configuration for this AMF, the AMF may be allowed to determine whether it can serve the UE (see (A) below for subsequent handling).

NOTE 4: The configuration in the AMF depends on the operator's policy.

(A) Depending on fulfilling the configuration as described above, the AMF may be allowed to determine whether it can serve the UE, and the following is performed:

- For the mobility from EPS to 5GS, the AMF first derives the serving PLMN value(s) of S-NSSAI(s) based on the HPLMN S-NSSAI(s) in the mapping of Requested NSSAI (in CM-IDLE state) or the HPLMN S-NSSAI(s) received from PGW-C+SMF (in CM-CONNECTED state). After that the AMF regards the derived value(s) as the Requested NSSAI.

- AMF checks whether it can serve all the S-NSSAI(s) from the Requested NSSAI present in the Subscribed S-NSSAIs (potentially using configuration for mapping S-NSSAI values between HPLMN and Serving PLMN), or all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in the case that no Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI are permitted, i.e. do not match any of the Subscribed S-NSSAIs or not available at the current UE's Tracking Area (see clause 5.15.3).

    - If the AMF can serve the S-NSSAIs in the Requested NSSAI, the AMF remains the serving AMF for the UE. The Allowed NSSAI is then composed of the list of S-NSSAI(s) in the Requested NSSAI permitted based on the Subscribed S-NSSAIs and/or the list of S-NSSAI(s) for the Serving PLMN which are mapped to the HPLMN S-NSSAI(s) provided in the mapping of Requested NSSAI permitted based on the Subscribed S-NSSAIs, or, if neither Requested NSSAI nor the mapping of Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI are permitted, all the S-NSSAI(s) marked as default in the Subscribed S-

NSSAIs and taking also into account the availability of the Network Slice instances as described in clause 5.15.8 that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's Tracking Areas. It also determines the mapping if the S-NSSAI(s) included in the Allowed NSSAI needs to be mapped to Subscribed S-NSSAI(s) values. If no Requested NSSAI is provided, or the mapping of the S-NSSAIs in Requested NSSAI to HPLMN S-NSSAIs is incorrect, or the Requested NSSAI includes an S-NSSAI that is not valid in the Serving PLMN, or the UE indicated that the Requested NSSAI is based on the Default Configured NSSAI, the AMF, based on the Subscribed S-NSSAI(s) and operator's configuration, may also determine the Configured NSSAI for the Serving PLMN and, if applicable, the associated mapping of the Configured NSSAI to HPLMN S-NSSAIs, so these can be configured in the UE. Then Step (C) is executed.

- Else, the AMF queries the NSSF (see (B) below).

(B) When required as described above, the AMF needs to query the NSSF, and the following is performed:

- The AMF queries the NSSF, with Requested NSSAI (excluding S-NSSAIs subject to NSSA which are in "Pending" state and are not yet in the Allowed NSSAI, if any), Default Configured NSSAI Indication, mapping of Requested NSSAI to HPLMN S-NSSAIs, the Subscribed S-NSSAIs (with an indication if marked as default S-NSSAI), any Allowed NSSAI it might have for the other Access Type (including its mapping to HPLMN S-NSSAIs), PLMN ID of the SUPI and UE's current Tracking Area.

- Based on this information, local configuration, and other locally available information including RAN capabilities in the current Tracking Area for the UE or load level information for a Network Slice instance provided by the NWDAF, the NSSF does the following:

  - It verifies which S-NSSAI(s) in the Requested NSSAI are permitted based on comparing the Subscribed S-NSSAIs with the S-NSSAIs in the mapping of Requested NSSAI to HPLMN S-NSSAIs. It considers the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs in the case that no Requested NSSAI was provided or no S-NSSAI from the Requested NSSAI are permitted i.e. are not present in the Subscribed S-NSSAIs or not available e.g. at the current UE's Tracking Area.

  - It selects the Network Slice instance(s) to serve the UE. When multiple Network Slice instances in the UE's Tracking Area are able to serve a given S-NSSAI, based on operator's configuration, the NSSF may select one of them to serve the UE, or the NSSF may defer the selection of the Network Slice instance until a NF/service within the Network Slice instance needs to be selected.

  - It determines the target AMF Set to be used to serve the UE, or, based on configuration, the list of candidate AMF(s), possibly after querying the NRF.

  NOTE 5: If the target AMF(s) returned from the NSSF is the list of candidate AMF(s), the Registration Request message can only be redirected via the direct signalling between the initial AMF and the selected target AMF as described in clause 5.15.5.2.3.

  - It determines the Allowed NSSAI(s) for the applicable Access Type, composed of the list of S-NSSAI(s) in the Requested NSSAI permitted based on the Subscribed S-NSSAIs and/or the list of S-NSSAI(s) for the Serving PLMN which are mapped to the HPLMN S-NSSAIs provided in the mapping of Requested NSSAI permitted based on the Subscribed S-NSSAIs, or, if neither Requested NSSAI nor the mapping of Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI are permitted, all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs, and taking also into account the availability of the Network Slice instances as described in clause 5.15.8 that are able to serve the S-NSSAI(s) in the Allowed NSSAI in the current UE's Tracking Areas.

  - It also determines the mapping of each S-NSSAI of the Allowed NSSAI(s) to the Subscribed S-NSSAIs if necessary.

  - Based on operator configuration, the NSSF may determine the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s).

  - Additional processing to determine the Allowed NSSAI(s) in roaming scenarios and the mapping to the Subscribed S-NSSAIs, as described in clause 5.15.6.

  - If no Requested NSSAI is provided or the Requested NSSAI includes an S-NSSAI that is not valid in the Serving PLMN, or the mapping of the S-NSSAIs in Requested NSSAI to HPLMN S-NSSAIs is incorrect, or the Default Configured NSSAI Indication is received from AMF, the NSSF based on the Subscribed S-NSSAI(s) and operator configuration may also determine the Configured NSSAI for the Serving PLMN and,

if applicable, the associated mapping of the Configured NSSAI to HPLMN S-NSSAIs, so these can be configured in the UE.

- The NSSF returns to the current AMF the Allowed NSSAI for the applicable Access Type, the mapping of each S-NSSAI of the Allowed NSSAI to the Subscribed S-NSSAIs if determined and the target AMF Set, or, based on configuration, the list of candidate AMF(s). The NSSF may return the NRF(s) to be used to select NFs/services within the selected Network Slice instance(s), and the NRF to be used to determine the list of candidate AMF(s) from the AMF Set. The NSSF may return NSI ID(s) to be associated to the Network Slice instance(s) corresponding to certain S-NSSAIs. NSSF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1. The NSSF may return the Configured NSSAI for the Serving PLMN and the associated mapping of the Configured NSSAI to HPLMN S-NSSAIs.

- Depending on the available information and based on configuration, the AMF may query the appropriate NRF (e.g. locally pre-configured or provided by the NSSF) with the target AMF Set. The NRF returns a list of candidate AMFs.

- If AMF Re-allocation is necessary, the current AMF reroutes the Registration Request or forwards the UE context to a target serving AMF as described in clause 5.15.5.2.3.

- Step (C) is executed.

(C) The serving AMF shall determine a Registration Area such that all S-NSSAIs of the Allowed NSSAI for this Registration Area are available in all Tracking Areas of the Registration Area (and also considering other aspects as described in clause 5.3.2.3) and then return to the UE this Allowed NSSAI and the mapping of the Allowed NSSAI to the Subscribed S-NSSAIs if provided. The AMF may return the rejected S-NSSAI(s) as described in clause 5.15.4.1.

NOTE 6: As there is a single distinct Registration Area for Non-3GPP access in a PLMN, the S-NSSAIs in the Allowed NSSAI for this Registration Area (i.e. for Non-3GPP access) are available homogeneously in the PLMN.

When either no Requested NSSAI was included, or the mapping of the S-NSSAIs in Requested NSSAI to HPLMN S-NSSAIs is incorrect, or a Requested NSSAI is not considered valid in the PLMN and as such at least one S-NSSAI in the Requested NSSAI was rejected as not usable by the UE in the PLMN, or the UE indicated that the Requested NSSAI is based on the Default Configured NSSAI, the AMF may update the UE slice configuration information for the PLMN as described in clause 5.15.4.2.

If the Requested NSSAI does not include S-NSSAIs which map to S-NSSAIs of the HPLMN subject to Network Slice-Specific Authentication and Authorization and the AMF determines that no S-NSSAI can be provided in the Allowed NSSAI for the UE in the current UE's Tracking Area and if no default S-NSSAI(s) could be added as described in step (A), the AMF shall reject the UE Registration and shall include in the rejection message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

If the Requested NSSAI includes S-NSSAIs which map to S-NSSAIs of the HPLMN subject to Network Slice-Specific Authentication and Authorization, the AMF shall include in the Registration Accept message an Allowed NSSAI containing only those S-NSSAIs that are not to be subject to Network Slice-Specific Authentication and Authorization and, based on the UE Context in AMF, those S-NSSAIs for which Network Slice-Specific Authentication and Authorization for at least one of the corresponding HPLMN S-NSSAIs succeeded previously regardless the Access Type, if any.

The AMF shall also provide the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

The S-NSSAIs which map to S-NSSAIs of the HPLMN subject to Network Slice-Specific Authentication and Authorization is ongoing are in "pending" state in the AMF and shall be included in the Pending NSSAI. The Pending NSSAI may contain a mapping of the S-NSSAI(s) for the Serving PLMN to the HPLMN S-NSSAIs, if applicable. The UE shall not include in the Requested NSSAI any of the S-NSSAIs from the Pending NSSAI the UE stores, regardless of the Access Type.

If:

- all the S-NSSAI(s) in the Requested NSSAI are still to be subject to Network Slice-Specific Authentication and Authorization; or

- no Requested NSSAI was provided or none of the S-NSSAIs in the Requested NSSAI matches any of the Subscribed S-NSSAIs, and all the S-NSSAI(s) marked as default in the Subscribed S-NSSAIs are to be subject to Network Slice-Specific Authentication and Authorization;

the AMF shall provide an empty Allowed NSSAI to the UE in the Registration Accept message. Upon receiving an empty Allowed NSSAI, the UE is registered in the PLMN but shall wait for the completion of the Network Slice-Specific Authentication and Authorization without attempting to use any service provided by the PLMN on any access, except e.g. emergency services (see TS 24.501 [47]), until the UE receives an allowed NSSAI.

Editor's note: Mechanisms to prevent the UE from waiting indefinitely for the completion of Slice-Specific Authentication and Authorization are defined in Stage 3 specifications.

Then, the AMF shall initiate the Network Slice-Specific Authentication and Authorization procedure as described in clause 5.15.10 for each S-NSSAI that requires it, except, based on Network policies, for those S-NSSAIs for which Network Slice-Specific Authentication and Authorization have been already initiated on another Access Type for the same S-NSSAI(s). At the end of the Network Slice-Specific Authentication and Authorization steps, the AMF by means of the UE Configuration Update procedure shall provide a new Allowed NSSAI to the UE which also contains the S-NSSAIs subject to Network Slice-Specific Authentication and Authorization for which the authentication and authorization is successful. The AMF may perform AMF selection when NSSAA completes for the S-NSSAIs subject to S-NSSAI in "pending" status. If an AMF change is required, this shall be triggered by the AMF using the UE Configuration Update procedure indicating a UE re-registration is required. The S-NSSAIs which were not successfully authenticated and authorized are not included in the Allowed NSSAI and are included in the list of Rejected S-NSSAIs with a rejection cause value indicating Network Slice-Specific Authentication and Authorization failure. The AMF shall remove the mobility restriction if the Tracking Areas of the Registration Area were previously assigned as a Non-Allowed Area due to pending Network Slice-Specific Authentication and Authorization.

Once completed the Network Slice-Specific Authentication and Authorization procedure, if the AMF determines that no S-NSSAI can be provided in the Allowed NSSAI for the UE, which is already authenticated and authorized successfully by a PLMN, and if no default S-NSSAI(s) could be added as described in step (A), the AMF shall execute the Network-initiated Deregistration procedure described in TS 23.502 [3], clause 4.2.2.3.3, and shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

If an S-NSSAI is rejected with a rejection cause value indicating Network Slice-Specific Authentication and Authorization failure or revocation, the UE can re-attempt to request the S-NSSAI based on policy, local in the UE.

5.15.5.2.2 Modification of the Set of Network Slice(s) for a UE

The set of Network Slices for a UE can be changed at any time while the UE is registered with a network, and may be initiated by the network, or by the UE, under certain conditions as described below.

The network, based on local policies, subscription changes and/or UE mobility, operational reasons (e.g. a Network Slice instance is no longer available or load level information for a network slice instance provided by the NWDAF), may change the set of Network Slice(s) to which the UE is registered and provide the UE with a new Registration Area and/or Allowed NSSAI and the mapping of this Allowed NSSAI to HPLMN S-NSSAIs, for each Access Type over which the UE is registered. In addition, the network may provide the Configured NSSAI for the Serving PLMN, the associated mapping information, and the rejected S-NSSAIs. The network may perform such a change over each Access Type during a Registration procedure or trigger a notification towards the UE of the change of the Network Slices using a UE Configuration Update procedure as specified in TS 23.502 [3], clause 4.2.4. The new Allowed NSSAI(s) and the mapping to HPLMN S-NSSAIs are determined as described in clause 5.15.5.2.1 (an AMF Re-allocation may be needed). The AMF provides the UE with:

- an indication that the acknowledgement from UE is required;
- Configured NSSAI for the Serving PLMN (if required), rejected S-NSSAI(s) (if required) and TAI list, and
- the new Allowed NSSAI with the associated mapping of Allowed NSSAI for each Access Type (as applicable) unless the AMF cannot determine the new Allowed NSSAI (e.g. all S-NSSAIs in the old Allowed NSSAI have been removed from the Subscribed S-NSSAIs).

  Furthermore:

- If the changes to the Allowed NSSAI require the UE to perform immediately a Registration procedure because they affect the existing connectivity to Network Slices (e.g. the new S-NSSAIs require a separate AMF that cannot be determined by the current serving AMF, or the AMF cannot determine the Allowed NSSAI) or due to AMF local policies also when the changes does not affect the existing connectivity to Network Slices:
  - The serving AMF indicates to the UE the need for the UE to perform a Registration procedure without including the GUAMI or 5G-S-TMSI in the access stratum signalling after entering CM-IDLE state. The

AMF shall release the NAS signalling connection to the UE to allow to enter CM-IDLE after receiving the acknowledgement from UE.

- When the UE receives indications to perform a Registration procedure without including the GUAMI or 5G-S-TMSI in the access stratum signalling after entering CM-IDLE state, then:

  - The UE deletes any stored (old) Allowed NSSAI and associated mapping as well as any (old) rejected S-NSSAI.

  - The UE shall initiate a Registration procedure with the registration type Mobility Registration Update after the UE enters CM-IDLE state as specified in as described in TS 23.502 [3] step 4 of clause 4.2.4.2. The UE shall include a Requested NSSAI (as described in clause 5.15.5.2.1) with the associated mapping of Requested NSSAI in the Registration Request message. Also, the UE shall include, subject to the conditions set out in clause 5.15.9, a Requested NSSAI in access stratum signalling but no GUAMI.

If there are established PDU Session(s) associated with emergency services, then the serving AMF indicates to the UE the need for the UE to perform a Registration procedure but does not release the NAS signalling connection to the UE. The UE performs the Registration procedure only after the release of the PDU Session(s) used for the emergency services.

In addition to sending the new Allowed NSSAI to the UE, when a Network Slice used for a one or multiple PDU Sessions is no longer available for a UE, the following applies:

- If the Network Slice becomes no longer available under the same AMF (e.g. due to UE subscription change), the AMF indicates to the SMF(s) which PDU Session ID(s) corresponding to the relevant S-NSSAI shall be released. SMF releases the PDU Session according to clause 4.3.4.2 in TS 23.502 [3].

- If the Network Slice becomes no longer available upon a change of AMF (e.g. due to Registration Area change), the new AMF indicates to the old AMF that the PDU Session(s) corresponding to the relevant S-NSSAI shall be released. The old AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the new AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status in the Registration Accept message.

The UE uses either the URSP rules (which includes the NSSP) or the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45] to determine whether ongoing traffic can be routed over existing PDU Sessions belonging to other Network Slices or establish new PDU Session(s) associated with same/other Network Slice.

In order to change the set of S-NSSAIs the UE is registered to over an Access Type, the UE shall initiate a Registration procedure over this Access Type as specified in clause 5.15.5.2.1.

If, for an established PDU Session:

- none of the values of the S-NSSAIs of the HPLMN in the mapping of the Requested NSSAI to S-NSSAIs of the HPLMN included in the Registration Request matches the S-NSSAI of the HPLMN associated with the PDU Session; or

- none of the values of the S-NSSAIs in the Requested NSSAI matches the value of the S-NSSAI of HPLMN associated with the PDU Session and the mapping of the Requested NSSAI to S-NSSAIs of the HPLMN is not included in the Registration Request,

the network shall release this PDU Session as follows.

- the AMF informs the corresponding SMF(s) to release the indicated PDU Session(s). The SMF(s) release the PDU Session(s) as described in clause 4.3.4 of TS 23.502 [3]. Then the AMF modifies the PDU Session Status correspondingly. The PDU Session(s) context is locally released in the UE after receiving the PDU Session Status from the AMF.

A change of the set of S-NSSAIs (whether UE or Network initiated) to which the UE is registered may, subject to operator policy, lead to AMF change, as described in clause 5.15.5.2.1.

5.15.5.2.3 AMF Re-allocation due to Network Slice(s) Support

During a Registration procedure in a PLMN, if the network decides that the UE should be served by a different AMF based on Network Slice(s) aspects, then the AMF that first received the Registration Request shall redirect the

Registration request to target AMF via the 5G-AN or via direct signalling between the initial AMF and the target AMF. If the target AMF(s) are returned from the NSSF and identified by a list of candidate AMF(s), the redirection message shall only be sent via the direct signalling between the initial AMF and the target AMF. If the redirection message is sent by the AMF via the 5G-AN, the message shall include information for selection of a new AMF to serve the UE.

During a EPS to 5GS handover using N26 interface procedure, if the network decides that the UE should be served by a different AMF based on Network Slice(s) aspects, then the AMF, which received the Forward Relocation Request from MME, shall forward the UE context to target AMF via direct signalling between the initial AMF and the target AMF as described in clause 4.11.1.2.2 in TS 23.502 [3].

For a UE that is already registered, the system shall support a redirection initiated by the network of a UE from its serving AMF to a target AMF due to Network Slice(s) considerations (e.g. the operator has changed the mapping between the Network Slice instances and their respective serving AMF(s)). Operator policy determines whether redirection between AMFs is allowed.

5.15.5.3 Establishing a PDU Session in a Network Slice

The PDU Session Establishment in a Network Slice instance to a DN allows data transmission in a Network Slice instance. A PDU Session is associated to an S-NSSAI and a DNN. A UE that is registered in a PLMN over an Access Type and has obtained a corresponding Allowed NSSAI, shall indicate in the PDU Session Establishment procedure the S-NSSAI according to the NSSP in the URSP rules or according to the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45], and, if available, the DNN the PDU Session is related to. The UE includes the appropriate S-NSSAI from this Allowed NSSAI and, if mapping of the Allowed NSSAI to HPLMN S-NSSAIs was provided, an S-NSSAI with the corresponding value from this mapping.

If the UE cannot determine any S-NSSAI after performing the association of the application to a PDU Session according to clause 6.1.2.2.1 of TS 23.503 [45], the UE shall not indicate any S-NSSAI in the PDU Session Establishment procedure.

The network (HPLMN) may provision the UE with Network Slice selection policy (NSSP) as part of the URSP rules, see TS 23.503 [45], clause 6.6.2. When the Subscription Information contains more than one S-NSSAI and the network wants to control/modify the UE usage of those S-NSSAIs, then the network provisions/updates the UE with NSSP as part of the URSP rules. When the Subscription Information contains only one S-NSSAI, the network needs not provision the UE with NSSP as part of the URSP rules. The NSSP rules associate an application with one or more HPLMN S-NSSAIs. A default rule which matches all applications to a HPLMN S-NSSAI may also be included.

The UE shall store and use the URSP rules, including the NSSP, as described in TS 23.503 [45]. When a UE application associated with a specific S-NSSAI requests data transmission:

- if the UE has one or more PDU Sessions established corresponding to the specific S-NSSAI, the UE routes the user data of this application in one of these PDU Sessions, unless other conditions in the UE prohibit the use of these PDU Sessions. If the application provides a DNN, then the UE considers also this DNN to determine which PDU Session to use. This is further described in TS 23.503 [45], clause 6.6.2.

- If the UE does not have a PDU Session established with this specific S-NSSAI, the UE requests a new PDU Session corresponding to this S-NSSAI and with the DNN that may be provided by the application. In order for the RAN to select a proper resource for supporting network slicing in the RAN, RAN needs to be aware of the Network Slices used by the UE. This is further described in TS 23.503 [45], clause 6.6.2.

If the AMF is not able to determine the appropriate NRF to query for the S-NSSAI provided by the UE, the AMF may query the NSSF with this specific S-NSSAI, location information, PLMN ID of the SUPI. The NSSF determines and returns the appropriate NRF to be used to select NFs/services within the selected Network Slice instance. The NSSF may also return an NSI ID to be used to select NFs within the selected Network Slice instance to use for this S-NSSAI. The IP address or FQDN of the NSSF is locally configured in the AMF.

SMF discovery and selection within the selected Network Slice instance is initiated by the AMF when a SM message to establish a PDU Session is received from the UE. The appropriate NRF is used to assist the discovery and selection tasks of the required network functions for the selected Network Slice instance.

The AMF queries the appropriate NRF to select an SMF in a Network Slice instance based on S-NSSAI, DNN, NSI-ID (if available) and other information e.g. UE subscription and local operator policies, when the UE triggers PDU Session Establishment. The selected SMF establishes a PDU Session based on S-NSSAI and DNN.

When the AMF belongs to multiple Network Slice instances, based on configuration, the AMF may use an NRF at the appropriate level for the SMF selection.

For further details on the SMF selection, refer to clause 4.3.2.2.3 in TS 23.502 [3].

When a PDU Session for a given S-NSSAI is established using a specific Network Slice instance, the CN provides to the (R)AN the S-NSSAI corresponding to this Network Slice instance to enable the RAN to perform access specific functions.

The UE shall not perform PDU Session handover from one Access Type to another if the S-NSSAI of the PDU Session is not included in the Allowed NSSAI of the target Access Type.

5.15.6 Network Slicing Support for Roaming

For roaming scenarios:

- If the UE only uses standard S-NSSAI values, then the same S-NSSAI values can be used in VPLMN as in the HPLMN.

- If the VPLMN and HPLMN have an SLA to support non-standard S-NSSAI values in the VPLMN, the NSSF of the VPLMN maps the Subscribed S-NSSAIs values to the respective S-NSSAI values to be used in the VPLMN. The S-NSSAI values to be used in the VPLMN are determined by the NSSF of the VPLMN based on the SLA. The NSSF of the VPLMN need not inform the HPLMN of which values are used in the VPLMN.

  Depending on operator's policy and the configuration in the AMF, the AMF may decide the S-NSSAI values to be used in the VPLMN and the mapping to the Subscribed S-NSSAIs.

- The UE constructs Requested NSSAI and provides the mapping of S-NSSAIs of the Requested NSSAI to HPLMN S-NSSAIs if the mapping is stored in the UE, as described in clause 5.15.5.2.1.

- The NSSF in the VPLMN determines the Allowed NSSAI without interacting with the HPLMN.

- The Allowed NSSAI in the Registration Accept includes S-NSSAI values used in the VPLMN. The mapping information described above is also provided to the UE with the Allowed NSSAI as described in clause 5.15.4.

- In PDU Session Establishment procedure, the UE includes both:

  (a) the S-NSSAI that matches the application (that is triggering the PDU Session Request) within the NSSP in the URSP rules or within the UE Local Configuration as defined in clause 6.1.2.2.1 of TS 23.503 [45]; the value of this S NSSAI is used in the HPLMN; and

  (b) an S-NSSAI belonging to the Allowed NSSAI that maps to (a) using the mapping of the Allowed NSSAI to HPLMN S-NSSAIs; the value of this S-NSSAI is used in the VPLMN.

  For the home routed case, the V-SMF sends the PDU Session Establishment Request message to the H-SMF along with the S-NSSAI with the value used in the HPLMN (a).

- When a PDU Session is established, the CN provides to the AN the S-NSSAI with the value from the VPLMN corresponding to this PDU Session, as described in clause 5.15.5.3.

- The Network Slice instance specific network functions in the VPLMN are selected by the VPLMN by using the S-NSSAI with the value used in the VPLMN and querying an NRF that has either been pre-configured, or provided by the NSSF in the VPLMN. The Network Slice specific functions of the HPLMN (if applicable) are selected by the VPLMN by using the related S-NSSAI with the value used in the HPLMN via the support from an appropriate NRF in the HPLMN, identified as specified in clause 4.17.5 of TS 23.502 [3] and, for SMF in clause 4.3.2.2.3.3 of TS 23.502 [3].

5.15.7 Network slicing and Interworking with EPS

5.15.7.1 General

A 5GS supports Network Slicing and might need to interwork with the EPS in its PLMN or in other PLMNs as specified in clause 5.17.2. The EPC may support the Dedicated Core Networks (DCN). In some deployments, the MME selection may be assisted by a DCN-ID provided by the UE to the RAN (see TS 23.401 [26]).

Mobility between 5GC to EPC does not guarantee all active PDU Session(s) can be transferred to the EPC.

During PDN connection establishment in the EPC, the UE allocates the PDU Session ID and sends it to the PGW-C+SMF via PCO. An S-NSSAI associated with the PDN connection is determined based on the operator policy by the PGW-C+SMF, e.g. based on a combination of PGW-C+SMF address and APN, and is sent to the UE in PCO together with a PLMN ID that the S-NSSAI relates to. In Home Routed roaming case, the UE receives a HPLMN S-NSSAI value from the PGW-C+SMF. If the PGW-C+SMF supports more than one S-NSSAI and the APN is valid for more than one S-NSSAI, the PGW-C+SMF should only select an S-NSSAI that is mapped to the subscribed S-NSSAIs of the UE. The UE stores this S-NSSAI and the PLMN ID associated with the PDN connection. The UE derives Requested NSSAI by taking into account of the received PLMN ID. The Requested NSSAI is included in the NAS Registration Request message and, subject to the conditions in clause 5.15.9, the RRC message carrying this Registration Request when the UE registers in 5GC if the UE is non-roaming or the UE has Configured NSSAI for the VPLMN in roaming case. If the UE has no Configured NSSAI of the VPLMN, the UE includes the HPLMN S-NSSAIs in the NAS Registration Request message as described in clause 5.15.5.2.1.

5.15.7.2 Idle mode aspects

In addition to the interworking principles documented in clause 5.17.2 the following applies for interworking with N26:

- When UE moves from 5GS to EPS, the UE context information sent by AMF to MME includes the UE Usage type, which is retrieved from UDM by AMF as part of subscription data.

- When UE moves from EPS to 5GS, then the UE includes the S-NSSAIs (with values for the Serving PLMN of the target 5GS, if available) associated with the established PDN connections in the Requested NSSAI in RRC Connection Establishment (subject to the conditions set out in clause 5.15.9) and NAS. The UE also provides to the AMF in the Registration Request message the mapping information as described in clause 5.15.6. The UE derives the S-NSSAIs values for the Serving PLMN by using the latest available information from EPS (if received in PCO) and from 5GS (e.g. based on URSP, Configured NSSAI, Allowed NSSAI). In the home-routed roaming case, the AMF selects default V-SMFs. The PGW-C+SMF sends PDU Session IDs and related S-NSSAIs to AMF. The AMF derives S-NSSAI values for the Serving PLMN as described in clause 5.15.5.2.1 and determines whether the AMF is the appropriate AMF to serve the UE. If not, the AMF reallocation may need be triggered. For each PDU Session the AMF determines whether the V-SMF need be reselected based on the associated S-NSSAI value for the Serving PLMN. If the V-SMF need be reallocated, i.e. change from the default V-SMF to another V-SMF, the AMF trigger the V-SMF reallocation as described in TS 23.502 [3] clause 4.23.3.

In addition to the interworking principles documented in clause 5.17.2 the following applies for interworking without N26:

- When the UE initiates the Registration procedure, and subject to the conditions set out in clause 5.15.9, the UE includes the S-NSSAI (with values for the Serving PLMN of the target 5GS) associated with the established PDN connections in the Requested NSSAI in the RRC Connection Establishment.

- The UE includes the S-NSSAIs (with values for the Serving PLMN of the target 5GS, if available) and the HPLMN S-NSSAI received in the PCO for the PDN connections as mapping information when moving PDN connections to 5GC using PDU Session Establishment Request message. The UE derives the S-NSSAIs values for the Serving PLMN by using, the latest available information from EPS (if received in PCO) and from 5GS (e.g. based on URSP, Configured NSSAI, Allowed NSSAI).

5.15.7.3 Connected mode aspects

In addition to the interworking principles documented in clause 5.17.2 the following applies for interworking with N26:

- When a UE is CM-CONNECTED in 5GC and a handover to EPS occur, the AMF selects the target MME based on the source AMF Region ID, AMF Set ID and target location information. The AMF forwards the UE context

to the selected MME over the N26 Interface. In the UE context, the AMF also includes the UE Usage type, if it is received as part of subscription data. The Handover procedure is executed as documented in TS 23.502 [3]. When the Handover procedure completes successfully the UE performs a Tracking Area Update. This completes the UE registration in the target EPS. As part of this the UE obtains a DCN-ID if the target EPS uses it.

- When a UE is ECM-CONNECTED in EPC, and performs a handover to 5GS, the MME selects the target AMF based on target location information, e.g. TAI and any other available local information (including the UE Usage Type if one is available for the UE in the subscription data) and forwards the UE context to the selected AMF over the N26 interface. In the home-routed roaming case, the AMF selects default V-SMFs. The Handover procedure is executed as documented in TS 23.502 [3]. The PGW-C+SMF sends PDU Session IDs and related S-NSSAIs to AMF. Based on the received S-NSSAIs values the target AMF derives the S-NSSAI values for the Serving PLMN, the target AMF reselects a final target AMF if necessary as described in clause 5.15.5.2.1, the AMF reallocation procedure is triggered. For each PDU Session based on the associated derived S-NSSAI values if the V-SMF need be reallocated, the final target AMF triggers the V-SMF reallocation as described in TS 23.502 [3] clause 4.23.2. When the Handover procedure completes successfully the UE performs a Registration procedure. This completes the UE registration in the target 5GS and as part of this the UE obtains an Allowed NSSAI.

5.15.8 Configuration of Network Slice availability in a PLMN

A Network Slice may be available in the whole PLMN or in one or more Tracking Areas of the PLMN.

The availability of a Network Slice refers to the support of the S-NSSAI in the involved NFs. In addition, policies in the NSSF may further restrict from using certain Network Slices in a particular TA, e.g. depending on the HPLMN of the UE.

The availability of a Network Slice in a TA is established end-to-end using a combination of OAM and signalling among network functions. It is derived by using the S-NSSAIs supported per TA in 5G-AN, the S-NSSAIs supported in the AMF and operator policies per TA in the NSSF.

The AMF learns the S-NSSAIs supported per TA by the 5G-AN when the 5G-AN nodes establish or update the N2 connection with the AMF (see TS 38.413 [34]) and TS 38.300 [27]). One or all AMF per AMF Set provides and updates the NSSF with the S-NSSAIs support per TA. The 5G-AN learns the S-NSSAIs per PLMN ID the AMFs it connects to support when the 5G-AN nodes establishes the N2 connection with the AMF or when the AMF updates the N2 connection with the 5G-AN (see TS 38.413 [34] and TS 38.300 [27]).

The NSSF may be configured with operator policies specifying under what conditions the S-NSSAIs can be restricted per TA and per HPLMN of the UE.

The per TA restricted S-NSSAIs may be provided to the AMFs of the AMF Sets at setup of the network and whenever changed.

The AMF may be configured for the S-NSSAIs it supports with operator policies specifying any restriction per TA and per HPLMN of the UE.

5.15.9 Operator-controlled inclusion of NSSAI in Access Stratum Connection Establishment

The Serving PLMN can control per Access Type which (if any) NSSAI the UE includes in the Access Stratum when establishing a connection caused by Service Request, Periodic Registration Update or Registration procedure used to update the UE capabilities. In addition, the Home and Visited PLMNs can also instruct the UE to never include NSSAI in the Access Stratum, regardless of the procedure that causes a RRC Connection to be established, i.e. to always enable privacy for the NSSAI).

During the Registration procedure, the AMF may provide to the UE in the Registration Accept message, an Access Stratum Connection Establishment NSSAI Inclusion Mode parameter, indicating whether and when the UE shall include NSSAI information in the Access Stratum Connection Establishment -e.g. an RRC connection Establishment defined in TS 38.331 [28]) according to one of these modes:

a) The UE shall include an NSSAI set to the Allowed NSSAI, if available, in the Access Stratum Connection Establishment caused by a Service Request, Periodic Registration Update or Registration procedure used to update the UE capabilities;

b) The UE shall include a NSSAI with the following content:

- for the case of Access Stratum Connection Establishment caused by a Service Request: an NSSAI including the S-NSSAI(s) of the Network Slice(s) that trigger the Access Stratum Connection Establishment; i.e. all the S-NSSAIs of the PDU sessions that have the User Plane reactivated by the Service Request, or the S-NSSAIs of the Network Slices a Control Plane interaction triggering the Service Request is related to, e.g. for SM it would be the S-NSSAI of the PDU Session the SM message is about;

- for the case of Access Stratum Connection Establishment caused by a Periodic Registration Update or Registration procedure used to update the UE capabilities, an NSSAI set to the Allowed NSSAI;

c) The UE shall not include any NSSAI in the Access Stratum Connection Establishment caused by Service Request, Periodic Registration Update or Registration procedure used to update the UE capabilities; or

d) The UE shall not provide NSSAI in the Access stratum.

For the case of Access Stratum Connection Establishment caused by Mobility Registration Update or Initial Registration in modes a), b) or c) the UE shall include the Requested NSSAI provided by the NAS layer and defined in clause 5.15.5.2.1.

For all UEs that are allowed to use modes a), b) or c), the Access Stratum Connection Establishment NSSAI Inclusion Mode should be the same over the same Registration Areas.The UE shall store and comply to the required behaviour for a PLMN per Access Type as part of the network slicing configuration. The Serving PLMN AMF shall not instruct the UE to operate in any other mode than mode d) in 3GPP Access Type unless the HPLMN provides an indication that it is allowed to do so -i.e. if a PLMN allows behaviours a,b,c, then its UDM sends to the serving AMF an explicit indication that the NSSAI can be included in RRC as part of the subscription data).

The UE default mode of operation is the following:

- For 3GPP access the UE shall by default operate in mode d) unless it has been provided with an indication to operate in mode a), b) or c).

- For untrusted non-3GPP access the UE shall operate by default in mode b) unless it has been provided with an indication to operate in mode a), c) or d).

- For trusted non-3GPP access the UE shall operate by default in mode d) unless it has been provided with an indication to operate in mode a), b) or c).

- For W-AGF access the 5G-RG shall operate by default in mode b) unless it has been provided with an indication to operate in mode a), c) or d).

An operator may pre-configure the UE to operate by default according to mode c) in the HPLMN (i.e. the UE by default includes NSSAI in the access stratum when it performs an Initial Registration and Mobility Registration Update with the HPLMN until the HPLMN changes the mode as described above).

5.15.10 Network Slice-Specific Authentication and Authorization

A serving PLMN shall perform Network Slice-Specific Authentication and Authorization for the S-NSSAIs of the HPLMN which are subject to it based on subscription information. The UE shall indicate in the Registration Request message in the UE 5GMM Core Network Capability whether it supports NSSAA feature. If the UE does not support NSSAA feature and if the UE requests any of these S-NSSAIs that are subject to Network Slice-Specific Authentication and Authorization, the AMF shall not trigger this procedure for the UE and they are rejected for the PLMN. If the UE supports NSSAA feature and if the UE requests any of these S-NSSAIs that are subject to Network Slice-Specific Authentication and Authorization, they are included in the list of Pending NSSAI for the PLMN, as described in clause 5.15.5.2.1.

If a UE is configured with S-NSSAIs, which are subject to Network Slice-Specific Authentication and Authorization, the UE stores an association between the S-NSSAI and corresponding credentials for the Network Slice-Specific Authentication and Authorization.

NOTE: The credentials for Network Slice-Specific Authentication and Authorization and how to provision them in the UE are not specified.

To perform the Network Slice-Specific Authentication and Authorization for an S-NSSAI, the AMF invokes an EAP-based Network Slice-Specific authorization procedure documented in TS 23.502 [3] clause 4.2.9 (see also TS 33.501 [29]) for the S-NSSAI. When an NSSAA procedure is started and is ongoing for an S-NSSAI, the AMF stores the NSSAA status of the S-NSSAI as pending and when the NSSAA is completed the S-NSSAI becomes either part of the Allowed NSSAI or a Rejected S-NSSAI. The NSSAA status of each S-NSSAI, if any is stored, is transferred when the AMF changes.

This procedure can be invoked for a supporting UE by an AMF at any time, e.g. when:

a. The UE registers with the AMF and one of the S-NSSAIs of the HPLMN which maps to an S-NSSAI in the Requested NSSAI is requiring Network Slice-Specific Authentication and Authorization (see clause 5.15.5.2.1 for details), and the S-NSSAI in the Requested NSSAI can be added to the Allowed NSSAI by the AMF once the Network Slice-Specific Authentication and Authorization for the HPLMN S-NSSAI succeeds; or

b. The Network Slice-Specific AAA Server triggers a UE re-authentication and re-authorization for an S-NSSAI; or

c. The AMF, based on operator policy or a subscription change, decides to initiate the Network Slice-Specific Authentication and Authorization procedure for a certain S-NSSAI which was previously authorized.

   In the case of re-authentication and re-authorization (b. and c. above) the following applies:

   - If S-NSSAIs that are requiring Network Slice-Specific Authentication and Authorization map to S-NSSAIs that are included in the Allowed NSSAI for each Access Type, AMF selects an Access Type to be used to perform the Network Slice Specific Authentication and Authorization procedure based on network policies.

   - If the Network Slice-Specific Authentication and Authorization for some S-NSSAIs mapped to some S-NSSAIs in the Allowed NSSAI is unsuccessful, the AMF shall update the Allowed NSSAI for each Access Type to the UE via UE Configuration Update procedure.

   - If the Network Slice-Specific Authentication and Authorization fails for all S-NSSAIs mapped to all S-NSSAIs in the Allowed NSSAI, the AMF shall execute the Network-initiated Deregistration procedure described in TS 23.502 [3], clause 4.2.2.3.3, and shall include in the explicit De-Registration Request message the list of Rejected S-NSSAIs, each of them with the appropriate rejection cause value.

After a successful or unsuccessful UE Network Slice-Specific Authentication and Authorization, the UE context in the AMF shall retain the authentication and authorization status for the UE for the related specific S-NSSAI of the HPLMN while the UE remains RM-REGISTERED in the PLMN, so that the AMF is not required to execute a Network Slice-Specific Authentication and Authorization for a UE at every Periodic Registration Update or Mobility Registration procedure with the PLMN.

A Network Slice-Specific AAA server may revoke the authorization or challenge the authentication and authorization of a UE at any time. When authorization is revoked for an S-NSSAI that maps to an S-NSSAI in the current Allowed NSSAI for an Access Type, the AMF shall provide a new Allowed NSSAI to the UE and trigger the release of all PDU sessions associated with the S-NSSAI, for this Access Type.

The AMF provides the GPSI of the UE related to the S-NSSAI to the AAA Server to allow the AAA server to initiate the Network Slice-Specific Authentication and Authorization, or the Authorization revocation procedure, where the current AMF serving the UE needs to be identified by the system, so the UE authorization status can be challenged or revoked.

The Network Slice-Specific Authentication and Authorization requires that the UE Primary Authentication and Authorization of the SUPI has successfully completed. If the SUPI authorization is revoked, then also the Network Slice-Specific authorization is revoked.

5.16 Support for specific services

5.16.1 Public Warning System

The functional description for supporting Public Warning System for 5G System can be found in TS 23.041 [46].

5.16.2 SMS over NAS

5.16.2.1 General

This clause includes feature description for supporting SMS over NAS in 5G System. Support for SMS incurs the following functionality:

- Support for SMS over NAS transport between UE and AMF. This applies to both 3GPP and Non 3GPP accesses.
- Support for AMF determining the SMSF for a given UE.
- Support for subscription checking and actual transmission of MO/MT-SMS transfer by the SMSF.
- Support for MO/MT-SMS transmission for both roaming and non-roaming scenarios.
- Support for selecting proper domains for MT SMS message delivery including initial delivery and re-attempting in other domains.

5.16.2.2 SMS over NAS transport

5G System supports SMS over NAS via both 3GPP access and non-3GPP access.

During Registration procedure, a UE that wants to use SMS provides an "SMS supported" indication over NAS signalling indicating the UE's capability for SMS over NAS transport. "SMS supported" indication indicates whether UE can support SMS delivery over NAS. If the core network supports SMS functionality, the AMF includes "SMS allowed" indication to the UE, and whether SMS delivery over NAS is accepted by the network.

SMS is transported via NAS transport message, which can carry SMS messages as payload.

5.16.3 IMS support

5.16.3.1 General

IP-Connectivity Access Network specific concepts when using 5GS to access IMS can be found in TS 23.228 [15].

5GS supports IMS with the following functionality:

- Indication toward the UE if IMS voice over PS session is supported.
- Capability to transport the P-CSCF address(es) to UE.
- Paging Policy Differentiation for IMS as defined in TS 23.228 [15].
- IMS emergency service as defined in TS 23.167 [18].
- Domain selection for UE originating sessions.
- Terminating domain selection for IMS voice.
- Support of P-CSCF restoration procedure (clause 5.16.3.9).
- NRF based P-CSCF discovery (clause 5.16.3.11).

NOTE: The NRF based P-CSCF discovery has no impact on the UE, i.e. the UE does not need to know how P-CSCF IP address(es) is discovered in the network.

- NRF based HSS discovery (clause 5.16.3.12).

5.16.3.2 IMS voice over PS Session Supported Indication over 3GPP access

The serving PLMN AMF shall send an indication toward the UE during the Registration procedure over 3GPP access to indicate if an IMS voice over PS session is supported or not supported in 3GPP access and non-3GPP access. A UE

with "IMS voice over PS" voice capability over 3GPP access should take this indication into account when performing voice domain selection, as described in clause 5.16.3.5.

The serving PLMN AMF may only indicate IMS voice over PS session supported over 3GPP access in one of the following cases:

- If the network and the UE are able to support IMS voice over PS session in the current Registration Area with a 5G QoS Flow that supports voice as specified in clause 5.7.
- If the network or the UE are not able to support IMS voice over PS session over NR connected to 5GC, but is able for one of the following:
  - If the network and the UE are able to support IMS voice over PS session over E-UTRA connected to 5GC, and the NG-RAN supports a handover or redirection to E-UTRA connected to 5GC for this UE at QoS Flow establishment for IMS voice;
  - If the UE supports handover to EPS, the EPS supports IMS voice, and the NG-RAN supports a handover to EPS for this UE at QoS Flow establishment for IMS voice; or
  - If the UE supports redirection to EPS, the EPS supports IMS voice, and the NG-RAN supports redirection to EPS for this UE at QoS Flow establishment for IMS voice.
- If the network is not able to provide a successful IMS voice over PS session over E-UTRA connected to 5GC, but is able for one of the following:
  - If the UE supports handover to EPS, the EPS supports IMS voice, and the NG-RAN supports a handover to EPS for this UE at QoS Flow establishment for IMS voice; or
  - If the UE supports redirection to EPS, the EPS supports IMS voice, and the NG-RAN supports redirection to EPS for this UE at QoS Flow establishment for IMS voice.

The serving PLMN provides this indication based e.g. on local policy, UE capabilities, HPLMN, whether IP address preservation is possible, whether NG-RAN to UTRAN SRVCC is supported and how extended NG-RAN coverage is, and the Voice Support Match Indicator from the NG-RAN (see TS 23.502 [3] clause 4.2.8a). The AMF in serving PLMN shall indicate that IMS voice over PS is supported only if the serving PLMN has a roaming agreement that covers support of IMS voice with the HPLMN. This indication is per Registration Area.

NOTE: If the network supports EPS fallback for voice the 5GC can be configured not to perform the Voice Support Match Indicator procedure in order to set the IMS voice over PS session Supported Indication.

5.16.3.2a IMS voice over PS Session Supported Indication over non-3GPP access

The serving PLMN AMF shall send an indication toward the UE during the Registration procedure over non-3GPP access to indicate whether an IMS voice over PS session is supported or not supported via non-3GPP access. A UE with "IMS voice over PS" voice capability over non-3GPP access should take this indication (received in the Registration procedure performed over either 3GPP access or Non-3GPP access) into account when performing the selection between N3IWF/TNGF and ePDG described in clause 6.3.6.

The serving PLMN AMF may only indicate IMS voice over PS session supported over non-3GPP access if the network is able to provide a successful IMS voice over PS session over N3IWF/TNGF connected to 5GC with a 5G QoS Flow that supports voice as specified in clause 5.7.

5.16.3.3 Homogeneous support for IMS voice over PS Session supported indication

5GC shall support the usage of "Homogeneous Support of IMS Voice over PS Sessions" indication between AMF and UDM.

When the AMF initiates Nudm_UECM_Registration operation to the UDM, it shall:

- if "IMS Voice over PS Sessions" is supported homogeneously in all TAs in the serving AMF for the UE, include the "Homogeneous Support of IMS Voice over PS Sessions" indication set to "Supported";
- if none of the TAs of the serving AMF supports "IMS Voice over PS Sessions" for the UE, include the "Homogeneous Support of IMS Voice over PS Sessions" indication set to "Not supported";

- if "IMS Voice over PS Sessions" support is either non-homogeneous or unknown, not include the "Homogeneous Support of IMS Voice over PS Sessions" indication.

The AMF shall be able to provide the "Homogeneous Support of IMS Voice over PS Sessions" indication as described above to the UDM using Nudm_UECM_Update operation as specified in clause 4.2.2.2.2 of TS 23.502 [3].

The UDM shall take this indication into account when doing Terminating Access Domain Selection (T-ADS) procedure for IMS voice.

NOTE: A TA supports "IMS Voice over PS Sessions" if the serving AMF indicates IMS voice over PS Session Supported Indication over 3GPP access to the UE, as described in clause 5.16.3.2. In order to support routing of incoming IMS voice calls to the correct domain, the network-based T-ADS (see TS 23.292 [63] and TS 23.221 [23]) requires that the "Homogeneous Support of IMS Voice over PS Sessions" indication is set to "Supported" for all registered TAs of the UE or "Not supported" for all registered TAs of the UE.

5.16.3.4 P-CSCF address delivery

At PDU Session Establishment procedure related to IMS, SMF shall support the capability to send the P-CSCF address(es) to UE. The SMF is located in VPLMN if LBO is used. This is sent by visited SMF if LBO is used. For Home routed, this information is sent by the SMF in HPLMN. P-CSCF address(es) shall be sent transparently through AMF, and in the case of Home Routed also through the SMF in VPLMN. The P-CSCF IP address(es) may be locally configured in the SMF, or discovered using NRF as described in clause 5.16.3.11.

NOTE 1: Other options to provide P-CSCF to the UE as defined in TS 23.228 [15] is not excluded.

NOTE 2: PDU Session for IMS is identified by "APN" or "DNN".

5.16.3.5 Domain selection for UE originating sessions / calls

For UE originating calls, the 5GC capable UE performs access domain selection. The UE shall be able to take following factors into account for access domain selection decision:

- The state of the UE in the IMS. The state information shall include: Registered, Unregistered.
- The "IMS voice over PS session supported indication" as defined in clause 5.16.3.2.
- Whether the UE is expected to behave in a "voice centric" or "data centric" way for 5GS.
- UE capability of supporting IMS PS voice.
- UE capability for operating in dual-registration mode with selective PDU Session transfer as defined in clause 5.17.2.3.3.
- Whether 3GPP PS Data Off is active or not and whether IMS voice is included in 3GPP PS Data Off Exempt Services or not as defined in clause 5.24.

NOTE 1: In this release of the specification, the exact logic of which PDU sessions are kept in which system for Dual Registration UE with selective transfer of certain PDU Sessions as defined in clause 5.17.2.3.3, is left up to UE implementation. The voice centric UE will keep the PDU Session used for IMS services to a system that supports voice over IMS. The voice centric UE can re-register with the IMS (if needed) when the IMS PDU session is transferred between 5GS and EPS.

To allow for appropriate domain selection for originating voice calls, the UE shall attempt Initial Registration in 5GC. If the UE fails to use IMS for voice, e.g. due to "IMS voice over PS session supported indication" indicates voice is not supported in 5G System, the UE behaves as described below for "voice centric" for 5GS or "data centric" for 5GS:

- A UE set to "voice centric" for 5GS shall always try to ensure that Voice service is possible. A voice centric 5GC capable and EPC capable UE unable to obtain voice service in 5GS shall not select a cell connected only to 5GC. By disabling capabilities to access 5GS, the UE re-selects to E-UTRAN connected to EPC first (if available). When the UE selects E-UTRAN connected to EPC, the UE performs Voice Domain Selection procedures as defined in TS 23.221 [23].
- A UE set to "data centric" for 5GS does not need to perform any reselection if voice services cannot be obtained.

NOTE 2: The related radio capabilities in order for the voice centric UE to not reselect to NR or E-UTRA cell connected to 5GC (i.e. avoid ping pong) will be defined by RAN WGs.

5.16.3.6 Terminating domain selection for IMS voice

When requested by IMS, the UDM/HSS shall be able to query the serving AMF for T-ADS related information. T-ADS is a functionality located in the IMS and is performed as specified in TS 23.221 [23].

The AMF shall respond to the query with the following information unless the UE is detached:

- whether or not IMS voice over PS Session is supported in the registration area (s) where the UE is currently registered;
- whether or not IMS voice over PS Session Supported Indication over non-3GPP access is supported in the WLAN where the UE is currently registered;
- the time of the last radio contact with the UE; and
- the current Access Type and RAT type.

5.16.3.7 UE's usage setting

If the UE is configured to support IMS voice, the UE shall include the information element "UE's usage setting" in Registration Request messages. The UE's usage setting indicates whether the UE behaves in a "voice centric" or "data centric" way (as defined in clause 5.16.3.5).

A UE supporting IMS voice over 3GPP access connected to 5GC and that is EPS capable shall also support IMS voice over E-UTRA connected to EPC.

NOTE: Depending on operator's configuration, the UE's usage setting can be used by the network to choose the RFSP Index in use (see clause 5.3.4.3). As an example, this enables the enforcement of selective idle mode camping over E-UTRA for voice centric UEs.

5.16.3.8 Domain and Access Selection for UE originating SMS

5.16.3.8.1 UE originating SMS for IMS Capable UEs supporting SMS over IP

To allow for appropriate domain selection for SMS delivery, it should be possible to provision UEs with the following HPLMN operator preferences on how an IMS enabled UE is supposed to handle SMS services:

- SMS is not to be invoked over IP networks: the UE does not attempt to deliver SMS over IP networks. The UE attempts to deliver SMS over NAS signalling.
- SMS is preferred to be invoked over IP networks: the UE attempts to deliver SMS over IP networks. If delivery of SMS over IP networks is not available, the UE attempts to deliver SMS over NAS signalling.

5.16.3.8.2 Access Selection for SMS over NAS

It should be possible to provision UEs with the HPLMN SMS over NAS operator preferences on access selection for delivering SMS over NAS signalling.

Based on the SMS over NAS preference:

- SMS is preferred to be invoked over 3GPP access for NAS transport: the UE attempts to deliver MO SMS over NAS via 3GPP access if the UE is both registered in 3GPP access and non-3GPP access.
- SMS is preferred to be invoked over non-3GPP access for NAS transport: the UE attempts to deliver MO SMS over NAS via non-3GPP access if the UE is both registered in 3GPP access and non-3GPP access. If delivery of SMS over NAS via non-3GPP access is not available, the UE attempts to deliver SMS over NAS via 3GPP access.

5.16.3.9 SMF support for P-CSCF restoration procedure

For the support of P-CSCF restoration the SMF behaves as described in TS 23.380 [61].

5.16.3.10 IMS Voice Service via EPS Fallback or RAT fallback in 5GS

In order to support various deployment scenarios for obtaining IMS voice service, the UE and NG-RAN may support the mechanism to direct or redirect the UE from NG-RAN either towards E-UTRA connected to 5GC (RAT fallback) or towards EPS (E-UTRAN connected to EPC System fallback).

Following principles apply for IMS Voice Service:

- The serving AMF indicates toward the UE during the Registration procedure that IMS voice over PS session is supported.
- If a request for establishing the QoS flow for IMS voice reaches the NG-RAN, the NG-RAN responds indicating rejection of the establishment request and the NG-RAN may trigger one of the following procedures depending on UE capabilities, N26 availability, network configuration and radio conditions:
  - Redirection to EPS;
  - Handover procedure to EPS;
  - Redirection to E-UTRA connected to 5GC; or
  - Handover to E-UTRA connected to 5GC.
- If needed, Network Provided Location Information is provided as described in clauses 4.13.6.1 and 4.13.6.2 of TS 23.502 [3].
- The ongoing IMS voice session is not impacted by a change of the IMS voice over PS session indicator from supported to unsupported (e.g. the UE receives during RAT Fallback or EPS Fallback the IMS voice over PS session indicator indicating that IMS voice over PS sessions are not supported).

NOTE: Any change in IMS voice over PS session indicator applies to new IMS sessions initiated only after the ongoing IMS voice session is terminated.

During any release of RRC connection including after EPS/RAT fallback is performed, the eNB or NG-RAN node may provide to the UE dedicated idle mode priorities for NR as defined in TS 36.331 [51] taking into account RFSP, PLMNs contained in Handover Restriction List and local operator policy. If the UE remains ECM/CM connected after the voice call has ended, the eNB or NG-RAN node may trigger handover to NR connected to 5GC, if configured to do so, taking into account local operator policy and Handover Restriction List.

5.16.3.11 P-CSCF discovery and selection

P-CSCF selection functionality may be used by the SMF to select the P-CSCF for an IMS PDU Session of the UE.

The SMF can utilize the Network Repository Function to discover the P-CSCF instance(s). The NRF provides the IP address or the FQDN of P-CSCF instance(s) to the SMF. The P-CSCF selection function in the SMF selects the P-CSCF instance(s) based on the available P-CSCF instances obtained from NRF or based on the configured P-CSCF information in the SMF. If the SMF receives FQDN(s) from the NRF or is configured with FQDN(s) the SMF shall resolve these to IP addresses for sending to the UE in the PDU session response.

The following factors may be considered during the P-CSCF discovery and selection:

- S-NSSAI of the PDU Session.
- UE location information.
- Local operator policies.
- Availability of candidate P-CSCFs.
- UE IP address.

- Access Type.
- Proximity to location of selected UPF.
- Selected Data Network Name (DNN).

5.16.3.12 HSS discovery and selection

HSS discovery and selection functionality is used by the I-CSCF/S-CSCF/IMS-AS to select an HSS that manages the user's IMS subscriptions and has the ability to serve the IMS services for the UE, see clause AA.3.3 in TS 23.228 [15] and clause 6.3.1 for details.

5.16.4 Emergency Services

5.16.4.1 Introduction

Emergency Services are provided to support IMS emergency sessions. "Emergency Services" refers to functionalities provided by the serving network when the network is configured to support Emergency Services. Emergency Services are provided to normally registered UEs and to Emergency Registered UEs, that can be either normally registered or in limited service state. Depending on local regulation, receiving Emergency Services in limited service state does not require a valid subscription. Depending on local regulation and on operator's policy, the network may allow or reject a registration request for Emergency Services (i.e. Emergency Registration) from UEs that have been identified to be in limited service state. Four different behaviours of Emergency Services as defined in TS 23.401 [26] clause 4.3.12.1 are supported.

Emergency Services shall not be provided to a UE over 3GPP access and untrusted non-3GPP access concurrently, except for the following case:

- a UE may be Emergency Registered and have an emergency PDU session over non-3GPP access or may be attached for emergency session to ePDG over untrusted WLAN (as defined in TS 23.402 [43]) when 3GPP access becomes available. In which case the UE may have to register over 3GPP access and check first the support for Emergency Services over the 3GPP RAT it has selected (e.g. based on Emergency Services Support indication, Emergency Services Fallback, AS broadcast indicator). If there is native support for Emergency Services in the selected 3GPP RAT the UE will attempt to transfer the emergency PDU session from non-3GPP access to 3GPP access (see TS 23.502 [3] clause 4.9.2). If there is no native support for Emergency Services in the selected RAT, but Emergency Services Fallback to another RAT in 5GS or to another System where Emergency Services may be supported (based on the conditions defined in clause 5.16.4.11), the UE may trigger first Emergency Services Fallback (see TS 23.502 [3] clause 4.13.4.2) and then attempt to transfer the emergency PDU session from non-3GPP access to 3GPP access (see TS 23.502 [3] clause 4.9.2). In these cases the UE may thus briefly be emergency registered and receive emergency services over both 3GPP access and non-3GPP access concurrently.

A UE may only attempt to use Emergency Services over untrusted non-3GPP access if it is unable to use Emergency Services over 3GPP access as specified in TS 23.167 [18].

To provide Emergency Services, the AMF is configured with Emergency Configuration Data that are applied to Emergency Services that are established by an AMF based on request from the UE. The AMF Emergency Configuration Data contains the S-NSSAI and Emergency DNN which is used to derive an SMF. In addition, the AMF Emergency Configuration Data may contain the statically configured SMF for the Emergency DNN. The SMF may also store Emergency Configuration Data that contains statically configured UPF information for the Emergency DNN.

When the UE is camped normally in the cell, i.e. not in limited service state, during Registration procedure described in TS 23.502 [3] clause 4.2.2.2, the serving AMF includes an indication for Emergency Services Support within the Registration Accept to the UE. For 3GPP access, the Emergency Services Support indication is valid within the current Registration Area per RAT (i.e. this is to cover cases when the same registration area supports multiple RATs and they have different capability).

The Emergency Services Support is configured in the AMF according to local regulations and network capabilities. AMF includes Emergency Services Support indicator in the Registration Accept message to indicate that the UE can setup emergency PDU Session to obtain emergency services. The AMF may include additional local emergency numbers associated with the serving network for the UE, further defined in TS 24.501 [47].

During Registration procedures over 3GPP access, the 5GC includes the Emergency Services Support indicator, valid for the current Registration Area and indicating per RAT that Emergency Services are supported if any of the following conditions is true within the current Registration Area:

- the Network is able to support Emergency Services natively over 5GS;
- E-UTRA connected to 5GC supports IMS Emergency Services (e.g. voice), and the NG-RAN is able to trigger handover or redirection from NR to E-UTRA connected to 5GC at QoS Flow establishment for IMS Emergency Services (e.g. voice);
- NG-RAN is able to trigger handover to EPS at QoS Flow establishment for IMS Emergency Services (e.g. voice);
- NG-RAN is able to trigger redirection to EPS at QoS Flow establishment for IMS Emergency Services (e.g. voice); or
- NG-RAN is able to trigger 5G SRVCC handover to UTRAN for IMS Emergency Services (i.e. voice).

During Registration procedures over non-3GPP access, the 5GC indicates that Emergency Services are supported if the Network is able to support Emergency Services natively over 5GS.

The 5GC includes an indication per RAT whether it supports Emergency Services Fallback (as defined in clause 5.16.4.11) to another RAT in 5GS or to another System where Emergency Services are supported natively. The Emergency Services Fallback support indicator is valid within the current Registration Area per RAT.

If a certain RAT is restricted for Emergency Services, AMF signals that the corresponding RAT is restricted for Emergency Services Support to the Master RAN Node. This helps assist the Master RAN node determine whether to set up Dual Connectivity for Emergency Services.

UEs that are in limited service state, as specified in TS 23.122 [17], or that camp normally on a cell but failed to register successfully to the network under conditions specified in TS 24.501 [47], initiate the Registration procedure by indicating that the registration is to receive Emergency Services, referred to as Emergency Registration, and a Follow-on request is included in the Registration Request to initiate PDU Session Establishment procedure with a Request Type indicating "Emergency Request". UEs that had registered for normal services and do not have emergency PDU Sessions established and that are subject to Mobility Restriction in the present area or RAT (e.g. because of restricted tracking area) shall initiate the UE Requested PDU Session Establishment procedure to receive Emergency Services, i.e. with a Request Type indicating "Emergency Request". Based on local regulation, the network supporting Emergency Services for UEs in limited service state provides Emergency Services to these UE, regardless whether the UE can be authenticated, has roaming or Mobility Restrictions or a valid subscription.

For Emergency Services over 3GPP access, other than eCall over IMS, the UEs in limited service state determine that the cell supports Emergency Services over NG-RAN from a broadcast indicator in AS. The cell connected to EPC and 5GC broadcasts separate broadcast indicator for EPC and 5GC to indicate support of emergency services by the EPC and 5GC. For Emergency Services over untrusted non-3GPP access, other than eCall over IMS, the UE in limited service state selects any N3IWF as specified in clause 6.3.6. Emergency calls for eCall Over IMS may only be performed if the UE has a USIM.

A serving network shall provide an Access Stratum broadcast indication from NG-RAN (NR or E-UTRA connected to 5GC) to UEs indicating whether eCall Over IMS is supported:

- When an E-UTRA cell is connected to EPC and 5GC, the cell broadcasts separate Access stratum broadcast indication for 5GC and EPC to indicate support of eCall over IMS by 5GC and EPC.
- A UE that is not in limited service state determines that the NG-RAN cell supports eCall Over IMS via 5GC using the broadcast indicator for eCall over IMS. Emergency calls for eCall over IMS are not supported over non-3GPP access.

NOTE 1: The Access Stratum broadcast indicator is determined according to operator policies and minimally indicates that the PLMN, or all of the PLMNs in the case of network sharing, and at least one emergency center or PSAP to which an eCall Over IMS can be routed, support eCall Over IMS.

- A UE in limited service state determines that the cell supports eCall Over IMS using both the broadcast indicator for support of Emergency Services over NG-RAN and the broadcast indicator of NG-RAN for eCall over IMS. Emergency calls for eCall Over IMS are not supported over Non-3GPP access.

NOTE 2: The broadcast indicator for eCall Over IMS does not indicate whether UEs in limited service state are supported. So, the broadcast indicator for support of Emergency Services over NG-RAN that indicates limited service state support needs to be applied in addition.

For a UE that is Emergency Registered, if it is unauthenticated the security context is not set up on UE.

In order to receive Emergency Services, UEs that camp on a suitable cell in RM-DEREGISTERED state (i.e. without any conditions that result in limited service state), or that decide to access 5GC via untrusted non-3GPP access (and not in limited service state over untrusted non-3GPP access), initiate the Initial Registration procedure for normal service instead of Emergency Registration. Upon successful registration, such UEs shall initiate the UE Requested PDU Session Establishment procedure with a Request Type indicating "Emergency Request" to receive Emergency Services if the AMF indicated support for Emergency Services in 5GC (for the RAT the UE is currently camped on when UE is camping on 3GPP access). The UEs that camp normally on a cell or that are connected via untrusted Non-3GPP access are informed that the PLMN supports Emergency Services over 5G-AN from the Emergency Services Support indicator in the Registration procedure. This applies to both 3GPP and non-3GPP Access Types.

NOTE 3: The Emergency Services Support indicator in the Registration procedures does not indicate support for eCall Over IMS.

For a UE that is Emergency Registered, normal PLMN selection principles apply after the end of the IMS emergency session.

NOTE 4: For Emergency Services, there is no support for inter PLMN mobility thus there is a risk of service disruption due to failed inter PLMN mobility attempts.

The UE shall set the RRC establishment cause to emergency as defined in TS 38.331 [28] when it requests an RRC Connection in relation to an emergency session.

In the case of Limited Service state, UE shall not include any Network Slice related parameters when communicating with the network.

When a PLMN supports IMS and Emergency Services:

- all AMFs in that PLMN shall have the capability to support Emergency Services.
- at least one SMF shall have this capability.

For other emergency scenarios (e.g. UE autonomous selection for initiating Emergency Services), refer to TS 23.167 [18] for domain selection principles.

For emergency service support in Public network integrated NPNs, refer to clause 5.30.3.5.

5.16.4.2 Architecture Reference Model for Emergency Services

According to clause 4.2, the non-roaming architectures (Figure 4.2.3-1 and Figure 4.2.3-2) and roaming architecture with the visited operator's application function (Figure 4.2.4-1 and Figure 4.2.4-4) apply for Emergency Services. The other non-roaming and roaming architectures with services provided by the home network do not apply for Emergency Services.

5.16.4.3 Mobility Restrictions and Access Restrictions for Emergency Services

When Emergency Services are supported and local regulation requires IMS Emergency Sessions to be provided regardless of the Mobility Restrictions (see clause 5.3.4.1), or access should not be applied to UEs receiving Emergency Services. When the (R)AN resources for Emergency Services are established, the ARP value for Emergency Services indicates the usage for Emergency Services to the 5G-AN.

During handover, the source NG-RAN and source AMF ignore any UE related restrictions during handover evaluation when there is an active PDU Session associated with emergency service.

During Mobility Registration Update procedures, including a Mobility Registration Update as part of a handover, the target AMF ignores any Mobility Restrictions or access restrictions for UE with emergency services where required by local regulation. Any non-emergency services are not allowed, by the target network when not allowed by the subscription for the target location. To allow the UE in limited service state (either Emergency Registered or registered for normal service) over a given Access Type to get access to normal services over this Access Type after the

Emergency Session has ended and when it has moved to a new area that is not stored by the UE as a forbidden area, after allowing a period of time for subsequent Emergency Services, the UE may explicitly deregister and register for normal services over this Access Type without waiting for the emergency PDU Session Release by the SMF.

This functionality applies to all mobility procedures.

5.16.4.4 Reachability Management

Over 3GPP access, an Emergency Registered UE when its Periodic Registration Update timer expires shall not initiate a Periodic Registration Update procedure but shall enter the RM-DEREGISTERED state. For such UEs, the AMF runs a mobile reachable timer with a similar value to the UE's Periodic Registration Update timer. After expiry of this timer the AMF may change the UE RM state for 3GPP Access in the AMF to RM-DEREGISTERED. The AMF assigns the Periodic Registration Update timer value to Emergency Registered UEs. This timer keeps the Emergency Registered UE registered for Emergency Services after change to CM-IDLE state to allow for a subsequent Emergency Service without a need for a new Emergency Registration.

Over untrusted non-3GPP access, an Emergency Registered UE is only reachable in CM-CONNECTED state: since the UE may only use Emergency Services over untrusted Non-3GPP access when it is not possible over 3GPP access, 3GPP access is assumed to be unavailable for paging the UE.

5.16.4.5 SMF and UPF selection function for Emergency Services

When a SMF is selected for Emergency Services, the SMF selection function described in clause 6.3.2 for normal services is applied to the Emergency DNN or the AMF selects the SMF directly from the AMF Emergency Configuration Data. If the SMF selection function described in clause 6.3.2 is used it shall always derive a SMF in the Serving PLMN, which guarantees that the IP address is also allocated by the Serving PLMN. When a UPF is selected for Emergency Services, the UPF selection function described in clause 6.3.3 for normal services is applied to the Emergency DNN or the SMF selects the UPF directly from the SMF Emergency Configuration Data. The information in the AMF Emergency Configuration Data and the SMF Emergency Configuration Data is specified in clause 5.16.4.1.

5.16.4.6 QoS for Emergency Services

Local regulation may require supporting emergency calls from an unauthorised UE. In such a case, the SMF may not have subscription data. Additionally, the local network may want to provide Emergency Services support differently than what is allowed by a UE subscription. Therefore, the initial QoS parameters used for establishing Emergency Services are configured in the V-SMF (local network) in the SMF Emergency Configuration Data.

This functionality is used by the UE Requested PDU Session Establishment procedure when establishing Emergency Services.

5.16.4.7 PCC for Emergency Services

Dynamic PCC is used for UEs establishing emergency service and shall be used to manage IMS emergency sessions when an operator allows IMS emergency sessions. When establishing Emergency Services with a SMF, the PCF provides the SMF with the QoS parameters, including an ARP value reserved for the Emergency Services to prioritize the QoS Flows when performing admission control, as defined in TS 23.503 [45].

The PCF rejects an IMS session established via the emergency PDU Session if the AF (i.e. P-CSCF) does not provide an emergency indication to the PCF.

5.16.4.8 IP Address Allocation

Emergency service is provided by the serving PLMN. The UE and serving PLMN must have compatible IP address versions in order for the UE to obtain a local emergency PDU Session.

5.16.4.9 Handling of PDU Sessions for Emergency Services

The QoS Flows of a PDU Session associated with the emergency DNN shall be dedicated for IMS emergency sessions and shall not allow any other type of traffic. The emergency contexts shall not be changed to non-emergency contexts and vice versa. The UPF shall block any traffic that is not from or to addresses of network functions (e.g. P-CSCF) providing Emergency Services. If there is already an emergency PDU Session over a given Access Type (3GPP access

or untrusted non-3GPP access), the UE shall not request another emergency PDU Session over the other Access Type except for handing over the emergency PDU Session to this other Access Type. The network shall reject any emergency PDU Session requests over a given Access Type (3GPP access or untrusted non-3GPP access) if it knows the UE already has an emergency PDU Session over the other Access Type. The ARP reserved for emergency service shall only be assigned to QoS Flows associated with an emergency PDU Session. If the UE is Emergency Registered over a given access, it shall not request a PDU Session to any other DNN over this access.

5.16.4.9a Handling of PDU Sessions for normal services for Emergency Registered UEs

For an Emergency Registered UE over a given Access Type:

- the UE shall not initiate the UE Requested PDU Session Establishment procedure for normal service over this Access Type; and
- the network shall reject any PDU Session Establishment request for normal service from the UE on this Access Type;
- the UE may attempt to receive normal service over another Access Type if not otherwise prevented by the present document.

5.16.4.10 Support of eCall Only Mode

For service requirements for eCall only mode, refer to TS 22.101 [33].

A UE configured for eCall Only Mode shall remain in RM-DEREGISTERED state, shall camp on a network cell when available but shall refrain from any Registration Management, Connection Management or other signalling with the network. The UE may instigate Registration Management and Connection Management procedures in order to establish, maintain and release an eCall Over IMS session or a session to any non-emergency MSISDN(s) or URI(s) configured in the USIM for test and/or terminal reconfiguration services. Following the release of either session, the UE starts a timer whose value depends on the type of session (i.e. whether eCall or a session to a non-emergency MSISDN or URI for test/reconfiguration). While the timer is running, the UE shall perform normal RM/CM procedures and is permitted to respond to paging to accept and establish an incoming session (e.g. from an emergency centre, PSAP or HPLMN operator). When the timer expires, the UE shall perform a UE-initiated Deregistration procedure if still registered and enter RM-DEREGISTERED state.

NOTE 1: An HPLMN operator can change the eCall Only Mode configuration state of a UE in the USIM. An HPLMN operator can also instead add, modify or remove a non-emergency MSISDN or URI in the USIM for test and/or terminal reconfiguration services. This can occur following a UE call to a non-emergency MSISDN or URI configured for reconfiguration. When the eCall Only Mode configuration is removed, the UE operates as a normal UE that can support eCall over IMS.

NOTE 2: A test call and a reconfiguration call can be seen as normal (non-emergency) call by a serving PLMN and normal charging rules can apply depending on operator policy.

NOTE 3: An MSISDN configured in the USIM for test and/or terminal reconfiguration services for eCall Over IMS can differ from an MSISDN configured in the USIM for test services for eCall over the CS domain.

5.16.4.11 Emergency Services Fallback

In order to support various deployment scenarios for obtaining Emergency Services, the UE and 5GC may support the mechanism to direct or redirect the UE either towards E-UTRA connected to 5GC (RAT fallback) when only NR does not support Emergency Services or towards EPS (E-UTRAN connected to EPC System fallback) when the 5GC does not support Emergency Services. Emergency Services fallback may be used when the 5GS does not indicate support for Emergency Services (see clause 5.16.4.1) and indicates support for Emergency Services fallback.

Following principles apply for Emergency Services Fallback:

- If the AMF indicates support for Emergency Services fallback in the Registration Accept message, then in order to initiate Emergency Service, normally registered UE supporting Emergency Services fallback shall initiate a Service Request with Service Type set to Emergency Services fallback as defined in TS 23.502 [3] clause 4.13.4.1.

- AMF uses the Service Type Indication within the Service Request to redirect the UE towards the appropriate RAT/System. The 5GS may, for Emergency Services, trigger one of the following procedures:
  - Handover or redirection to EPS.
  - Handover or redirection to E-UTRA connected to 5GC.
- After receiving the Service Request for Emergency Fallback, the AMF triggers N2 procedure resulting in either CONNECTED state mobility (Handover procedure) or IDLE state mobility (redirection) to either E-UTRA/5GC or to E-UTRAN/EPC depending on factors such as N26 availability, network configuration and radio conditions. In the N2 procedure, the AMF based on support for Emergency Services in 5GC or EPC may indicate the target CN for the RAN node to know whether inter-RAT fallback or inter-system fallback is to be performed. The target CN indicated in the N2 procedure is also conveyed to the UE in order to be able to perform the appropriate NAS procedures (S1 or N1 Mode).

NOTE: Emergency Services Fallback to EPS can be followed by an onward movement to GERAN or UTRAN via CSFB procedures if the PLMN does not support IMS emergency services.

5.16.5 Multimedia Priority Services

TS 22.153 [24] specifies the service requirements for Multimedia Priority Service (MPS). MPS allows Service Users (as per TS 22.153 [24]) priority access to system resources in situations such as during congestion, creating the ability to deliver or complete sessions of a high priority nature. Service Users are government-authorized personnel, emergency management officials and/or other authorized users. MPS supports priority sessions on an "end-to-end" priority basis.

MPS is based on the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions. MPS is supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

NOTE 1: If a session terminates on a server in the Internet (e.g. web-based service), then the remote end and the Internet transport are out of scope for this specification.

A Service User may use an MPS-subscribed UE or any other UE to obtain MPS. An MPS-subscribed UE obtains priority access to the Radio Access Network by using the Unified Access Control mechanism according to TS 22.261 [2]. This mechanism provides preferential access to UEs based on its assigned Access Identity. If an MPS-subscribed UE belongs to the special Access Identity as defined in TS 22.261 [2], the UE has preferential access to the network compared to ordinary UEs in periods of congestion.

MPS subscription allows users to receive priority services, if the network supports MPS. MPS subscription entitles a USIM with special Access Identity. MPS subscription includes indication for support of priority PDU connectivity service and IMS priority service support for the end user. Priority level regarding QoS Flows and IMS are also part of the MPS subscription information. The usage of priority level is defined in TS 22.153 [24], TS 23.503 [45] and TS 23.228 [15].

NOTE 2: The term "Priority PDU connectivity services" is used to refer to 5G System functionality that corresponds to the functionality as provided by LTE/EPC Priority EPS bearer services in clause 4.3.18.3 of TS 23.401 [26].

MPS includes signalling priority and media priority. All MPS-subscribed UEs get priority for QoS Flows (e.g., used for IMS signalling) when established to the DN that is configured to have priority for a given Service User by setting MPS-appropriate values in the QoS profile in the UDM. Service Users are treated as On Demand MPS subscribers or not, based on regional/national regulatory requirements. On Demand service is based on Service User invocation/revocation explicitly and applied to the media QoS Flows being established. When not On Demand MPS service does not require invocation, and provides priority treatment for all QoS Flows only to the DN that is configured to have priority for a given Service User after attachment to the 5G network.

NOTE 3: According to regional/national regulatory requirements and operator policy, On-Demand MPS Service Users can be assigned the highest priority.

Priority treatment is applicable to IMS based multimedia services and priority PDU connectivity service.

Priority treatment for MPS includes priority message handling, including priority treatment during authentication, security, and Mobility Management procedures.

Priority treatment for MPS session requires appropriate ARP and 5QI (plus 5G QoS characteristics) setting for QoS Flows according to the operator's policy.

NOTE 4: Use of QoS Flows for MPS with QoS characteristics signalled as part of QoS profile enables the flexible assignment of 5G QoS characteristics (e.g. priority level) for MPS.

When an MPS session is requested by a Service User, the following principles apply in the network:

- QoS Flows employed in an MPS session shall be assigned ARP value settings appropriate for the priority level of the Service User.
- Setting ARP pre-emption capability and vulnerability for MPS QoS Flows, subject to operator policies and depending on national/regional regulatory requirements.
- Pre-emption of non-Service Users over Service Users during network congestion situation, subject to operator policy and national/regional regulations.

The terminating network identifies the priority of the MPS session and applies priority treatment, including paging with priority, to ensure that the MPS session can be established with priority to the terminating user (either a Service User or normal user).

MPS priority mechanisms can be classified as subscription-related, invocation-related, and those applied to existing QoS Flows. Subscription related mechanisms, as described in clause 5.22.2, are further divided into two groups: those which are always applied and those which are conditionally applied. Invocation-related mechanisms, as described in clause 5.22.3, are further divided into three groups: those that apply for mobile originated SIP call/sessions, those that apply for mobile terminated SIP call/sessions, and those that apply for the Priority PDU connectivity services. Methods applied to existing QoS Flows focus on handover and congestion control and are described in clause 5.22.4.

5.16.6 Mission Critical Services

According to TS 22.280 [37], a Mission Critical Service (MCX Service) is a communication service reflecting enabling capabilities Mission Critical Applications and provided to end users from Mission Critical Organizations and mission critical applications for other businesses and organizations (e.g. utilities, railways). An MCX Service is either Mission Critical Push To Talk (MCPTT) as defined in TS 23.379 [38], Mission Critical Video (MCVideo) as defined in TS 23.281 [39], or Mission Critical Data (MCData) as defined in TS 23.282 [40] and represents a shared underlying set of requirements between two or more MCX Service types. MCX Services are not restricted only to the ones defined in this sub clause and such services can also have priority treatment, if defined via operator's policy and/or local regulation.

MCX Services are based on the ability to invoke, modify, maintain and release sessions with priority, and deliver the priority media packets under network congestion conditions. As specified in TS 22.261 [2] clause 6.8, MCX Users require 5GS functionality that allows for real-time, dynamic, secure and limited interaction with the QoS and policy framework for modification of the QoS and policy framework by authorized users. The limited interaction is based on operator policy, and provides specific limitations on what aspects of the QoS and policy framework an authorized MCX User can modify. MCX Services are supported in a roaming environment when roaming agreements are in place and where regulatory requirements apply.

An MCX-subscribed UE obtains priority access to the Radio Access Network by using the Unified Access Control mechanism according to TS 22.261 [2]. This mechanism provides preferential access to UEs based on its assigned Access Identity. If an MCX-subscribed UE belongs to the special Access Identity as defined in TS 22.261 [2], the UE has preferential access to the network compared to ordinary UEs in periods of congestion. MCX subscription allows users to receive priority services, if the network supports MCX. MCX subscription entitles a USIM with special Access Identity.

MCX Services leverage the foundation of the 5G QoS Model as defined in clause 5.7, and 5G Policy Control as defined in clause 5.14. It requires that the necessary subscriptions are in place for both the 5G QoS Profile and the necessary Policies. In addition, MCX Services leverage priority mechanism as defined in clause 5.22.

The terminating network identifies the priority of the MCX Service session and applies priority treatment, including paging with priority, to ensure that the MCX Service session can be established with priority to the terminating user (either an MCX User or normal user).

Priority treatment for MCX Service includes priority message handling, including priority treatment during authentication, security, and Mobility Management procedures.

Priority treatment for MCX Service sessions require appropriate ARP and 5QI (plus 5G QoS characteristics) setting for QoS Flows according to the operator's policy.

NOTE: Use of QoS Flows for MCX Service sessions with non-standardized 5QI values enables the flexible assignment of 5G QoS characteristics (e.g. priority level).

When a MCX Service session is requested by an MCX User, the following principles apply in the network:

- QoS Flows employed in a MCX Service session shall be assigned ARP value settings appropriate for the priority level of the MCX User.
- Setting ARP pre-emption capability and vulnerability of QoS Flows related to a MCX Service session, subject to operator policies and depending on national/regional regulatory requirements.
- Pre-emption of non-MCX Users over MCX Users during network congestion situations, subject to operator policy and national/regional regulations.

Priority treatment is applicable to IMS based multimedia services and priority PDU connectivity services.

Relative PDU priority decisions for MCX Service sessions are based on real-time data of the state of the network and/or based on modification of the QoS and policy framework by authorized users as described in clause 6.8 of TS 22.261 [2].

5.17 Interworking and Migration

5.17.1 Support for Migration from EPC to 5GC

5.17.1.1 General

Clause 5.17.1 describes the UE and network behaviour for the migration from EPC to 5GC.

Deployments based on different 3GPP architecture options (i.e. EPC based or 5GC based) and UEs with different capabilities (EPC NAS and 5GC NAS) may coexist at the same time within one PLMN.

It is assumed that a UE that is capable of supporting 5GC NAS procedures may also be capable of supporting EPC NAS (i.e. the NAS procedures defined in TS 24.301 [13]) to operate in legacy networks e.g. in the case of roaming.

The UE will use EPC NAS or 5GC NAS procedures depending on the core network by which it is served.

In order to support smooth migration, it is assumed that the EPC and the 5GC have access to a common subscriber database, that is HSS in the case of EPC and the UDM in the case of 5GC, acting as the master data base for a given user as defined in TS 23.002 [21]. The PCF has access to the UDR that acts as a common subscriber database for a given user identified by a SUPI using the Nudr services defined in TS 23.502 [3].

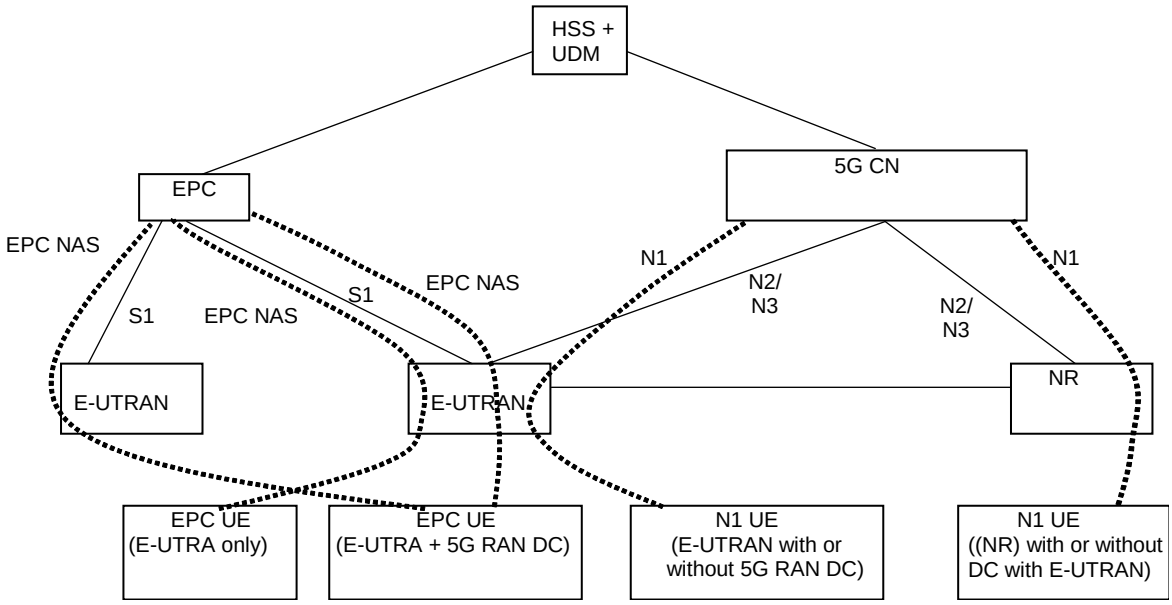


Figure 5.17.1.1-1: Architecture for migration scenario for EPC and 5G CN

A UE that supports only EPC based Dual Connectivity with secondary RAT NR:

- always performs initial access through E-UTRA (LTE-Uu) but never through NR;
- performs EPC NAS procedures over E-UTRA (i.e. Mobility Management, Session Management etc) as defined in TS 24.301 [13].

A UE that supports camping on 5G Systems with 5GC NAS:

- performs initial access either through E-UTRAN that connects to 5GC or NR towards 5GC;
- performs initial access through E-UTRAN towards EPC, if supported and needed;
- performs EPC NAS or 5GC NAS procedures over E-UTRAN or NR respectively (i.e. Mobility Management, Session Management etc) depending on whether the UE requests 5GC access or EPC access, if the UE also supports EPC NAS.

When camping on an E-UTRA cell connected to both EPC and 5GC, a UE supporting EPC NAS and 5GC NAS shall select a core network type (EPC or 5GC) and initiate the corresponding NAS procedure as specified in TS 23.122 [17].

In order to support different UEs with different capabilities in the same network, i.e. both UEs that are capable of only EPC NAS (possibly including EPC based Dual Connectivity with secondary NR) and UEs that support 5GC NAS procedures in the same network:

- eNB that supports access to 5GC shall broadcast that it can connect to 5GC. Based on that, the UE AS layer indicates "E-UTRA connected to 5GC" capability to the UE NAS layer. In addition the eNB broadcasts the supported CIoT 5GS Optimisations that the UE uses for selecting a core network type.
- It is also expected that the UE AS layer is made aware by the UE NAS layer whether a NAS signalling connection is to be initiated to the 5GC. Based on that, UE AS layer indicates to the RAN whether it is requesting 5GC access (i.e. "5GC requested" indication). The RAN uses this indication to determine whether a UE is requesting 5GC access or an EPC access. RAN routes NAS signalling to the applicable AMF or MME accordingly.

NOTE: The UE that supports EPC based Dual Connectivity with secondary RAT only does not provide this "5GC requested" indication at Access Stratum when it performs initial access and therefore eNB uses the "default" CN selection mechanism to direct this UE to an MME

The 5GC network may steer the UE from 5GC based on:

- Core Network type restriction (e.g. due to lack of roaming agreements) described in clause 5.3.4.1.1;

- Availability of EPC connectivity;
- UE indication of EPC Preferred Network Behaviour; and
- Supported Network Behaviour.

In this Release of the specification there is no support in 5G System for some functionalities supported in EPS such as ProSe, MBMS, etc. The UE that wants to use one or more of these functionalities not supported by 5G System, when in CM-IDLE may disable all the related radio capabilities that allow the UE to access 5G System. The triggers to disable and re-enable the 5GS capabilities to access 5G System in this case are left up to UE implementation.

5.17.1.2 User Plane management to support interworking with EPS

In order to support the interworking with EPC, the SMF+PGW-C provides information over N4 to the UPF+PGW-U related to the handling of traffic over S5-U. Functionality defined in TS 23.503 [45] for traffic steering control on SGi-LAN/N6 can be activated in UPF+PGW-U under consideration of whether the UE is connected to EPC or 5GC.

When the UE is connected to EPC and establishes/releases PDN connections, the following differences apply to N4 compared to when the UE is connected to 5GC:

- The CN Tunnel Info is allocated for each EPS Bearer.
- In addition to the Service Data Flow related information, the SMF+PGW-C shall be able to provide the GBR and MBR values for each GBR bearer of the PDN connection to the UPF+PGW-U.

If the UE does not have preconfigured rules for associating an application to a PDN connection (i.e. the UE does not have rules in UE local configuration and is not provisioned with ANDSF rules), the UE should use a matching URSP rule as defined in TS 23.503 [45], if available, to derive the parameters, e.g. APN, for the PDN connection establishment and associating an application to the PDN connection.

NOTE: The mapping between the parameters in the URSP rules and the parameters used for PDN connection establishment is defined in TS 24.526 [110].

5.17.2 Interworking with EPC

5.17.2.1 General

Interworking with EPC in this clause refers to mobility procedures between 5GC and EPC/E-UTRAN, except for clause 5.17.2.4. Network slicing aspects for EPS Interworking are specified in clause 5.15.7

In order to interwork with EPC, the UE that supports both 5GC and EPC NAS can operate in single-registration mode or dual-registration mode:

- In single-registration mode, UE has only one active MM state (either RM state in 5GC or EMM state in EPC) and it is either in 5GC NAS mode or in EPC NAS mode (when connected to 5GC or EPC, respectively). UE maintains a single coordinated registration for 5GC and EPC. Accordingly, the UE maps the EPS-GUTI to 5G GUTI during mobility between EPC and 5GC and vice versa following the mapping rules in Annex B. To enable re-use of a previously established 5G security context when returning to 5GC, the UE also keeps the native 5G-GUTI and the native 5G security context when moving from 5GC to EPC.
- In dual-registration mode, UE handles independent registrations for 5GC and EPC using separate RRC connections. In this mode, UE maintains 5G-GUTI and EPS-GUTI independently. In this mode, UE provides native 5G-GUTI, if previously allocated by 5GC, for registrations towards 5GC and it provides native EPS-GUTI, if previously allocated by EPC, for Attach/TAU towards EPC. In this mode, the UE may be registered to 5GC only, EPC only, or to both 5GC and EPC.

  Dual-registration mode is intended for interworking between EPS/E-UTRAN and 5GS/NR. A dual-registered UE should not send its E-UTRA connected to 5GC and E-UTRAN radio capabilities to NR access when connected to 5GS/NR to avoid being handed over to 5GC-connected E-UTRA or to E-UTRAN.

NOTE 1: This is to prevent the dual registered UE from being connected to the same E-UTRA cell either connected to EPC or 5GC simultaneously using separate RRC connections via single RAN node as a result of handover. If a dual- registered UE implementation chooses to send its E-UTRA capability when connected to 5GS/NR, the UE and the network behaviour when UE enters a 5GC-connected E-UTRA is not further specified. If however the UE is registered with 5GS/NR only, the UE can send its E-UTRA capability in order to allow inter-RAT handover to E-UTRA/5GC and Dual Connectivity with multiple RATs.

If a dual-registered UE had not sent its E-UTRA connected to 5GC and E-UTRAN radio capabilities to 5GS and the UE needs to initiate emergency services, it shall locally re-enable its E-UTRA connected to 5GC and E-UTRAN radio capabilities in order to perform domain selection for emergency services as defined in TS 23.167 [18].

NOTE 2: However even in this case, the UE is still not expected to connect to E-UTRAN/EPC and E-UTRA/5GC simultaneously using separate RRC connection via single RAN node as a result of the domain selection for emergency services.

The support of single registration mode is mandatory for UEs that support both 5GC and EPC NAS.

During E-UTRAN Initial Attach, UE supporting both 5GC and EPC NAS shall indicate its support of 5G NAS in UE Network Capability described in clause 5.11.3 of TS 23.401 [26].

During registration to 5GC, UE supporting both 5GC and EPC NAS shall indicate its support of EPC NAS.

NOTE 3: This indication may be used to give the priority towards selection of PGW-C + SMF for UEs that support both EPC and 5GC NAS.

If the EPC supports "Ethernet" PDU Session Type, and the 5GSM Capabilities indicate that the UE supports Ethernet PDN type in EPC, then PDU Session type "Ethernet" is transferred to EPC as "Ethernet". Otherwise, PDU Session types "Ethernet" and "Unstructured" are transferred to EPC as "non-IP" PDN type (when supported by UE and network). If the UE or EPC does not support Ethernet PDN type in EPC, the UE sets the PDN type to non-IP when it moves from 5GS to EPS and after the transfer to EPS, and the UE and the SMF shall maintain information about the PDU Session type used in 5GS, i.e. information indicating that the PDN Connection with "non-IP" PDN type corresponds to PDU Session type Ethernet or Unstructured respectively. This is done to ensure that the appropriate PDU Session type will be used if the UE transfers to 5GS.

PDN type "non-IP" is transferred to 5GS as "Unstructured" PDU Session type if it is successfully transferred.

It is assumed that if a UE supports Ethernet PDU Session type and/or Unstructured PDU Session type in 5GS it will also support non-IP PDN type in EPS. If this is not the case, the UE shall locally delete any EBI(s) corresponding to the Ethernet/Unstructured PDU Session(s) to avoid that the Ethernet/Unstructured PDU Session(s) are transferred to EPS.

MTU size consideration for PDU Sessions and PDN Connections towards a PGW-C+SMF follows the requirements in clause 5.6.10.4.

Networks that support interworking with EPC, may support interworking procedures that use the N26 interface or interworking procedures that do not use the N26 interface. Interworking procedures with N26 support provides IP address continuity on inter-system mobility to UEs that support 5GC NAS and EPC NAS and that operate in single registration mode. Networks that support interworking procedures without N26 shall support procedures to provide IP address continuity on inter-system mobility to UEs operating in both single-registration mode and dual-registration mode. In such networks, AMF shall provide the indication that interworking without N26 is supported to UEs during initial Registration in 5GC or MME may optionally provide the indication that interworking without N26 is supported in the Attach procedure in EPC as defined in TS 23.401 [26].

If the network does not support interworking with EPC, network shall not indicate support for "interworking without N26" to the UE.

When the HSS+UDM is required to provide the subscription data to the MME, for each APN, only one PGW-C+SMF FQDN and associated APN is provided to the MME according to TS 23.401 [26].

For interworking without N26 interface:

- if the PDU session supports interworking, the PGW-C+SMF stores the PGW-C+SMF FQDN to SMF context in HSS+UDM when the SMF is registered to HSS+UDM.

- For an APN, the HSS+UDM selects one of the stored PGW-C+SMF FQDN based on operator's policy.

For interworking with N26 interface:

- For a DNN, AMF determines PDU session(s) associated with 3GPP access in only one PGW-C+SMF supporting EPS interworking via EBI allocation procedure as described in clause 4.11.1.4.1 of TS 23.502 [3].

- If the network supports EPS interworking of non-3GPP access connected to 5GC, the AMF serving 3GPP access notifies the UDM to store the association between DNN and PGW-C+SMF FQDN which supports EPS interworking as Intersystem continuity context, to avoid MME receiving inconsistent PGW-C+SMF FQDN from AMF and HSS+UDM.

- The AMF updates Intersystem continuity context if the PGW-C+SMF and DNN association is changed due to the AMF selecting another PGW-C+SMF for EPS interworking for the same DNN.

- If the PGW-C+SMF FQDN and associated DNN exists in Intersystem continuity context, the HSS+UDM provides MME with PGW-C+SMF FQDN and associated APN.

It does not assume that the HSS+UDM is aware of whether N26 is deployed in the serving network. The HSS+UDM check the Intersystem continuity context first. If no PGW-C+SMF FQDN associated with an DNN exists in Intersystem continuity context, the HSS+UDM selects one of the PGW-C+SMF FQDN for the APN from SMF context based on operator's policy.

In entire clause 5.17.2 the terms "initial attach", "handover attach" and "TAU" for the UE procedures in EPC can alternatively be combined EPS/IMSI Attach and combined TA/LA depending on the UE configuration defined in TS 23.221 [23].

If a UE in MICO mode moves to E-UTRAN connected to EPC and any of the triggers defined in clause 5.4.1.3 occur, then the UE shall locally disable MICO mode and perform the TAU or Attach procedure as defined in clause 5.17.2. The UE can renegotiate MICO when it returns to 5GS during (re-)registration procedure.

IP address preservation for IP PDU sessions cannot be ensured on subsequent mobility from EPC/E-UTRAN to GERAN/UTRAN to a UE that had initially registered in 5GS and moved to EPC/E-UTRAN.

NOTE 4: The SMF+PGW-C might not include the GERAN/UTRAN PDP Context anchor functionality. Also, 5GC does not provide GERAN/UTRAN PDP Context parameters to the UE when QoS flows of PDU Session are setup or modified in 5GS. Hence, the UE might not be able to activate the PDP contexts when it transitions to GERAN/UTRAN.

IP address preservation for IP PDU sessions cannot be ensured on subsequent mobility from EPC/E-UTRAN to 5GS to a 5GS NAS capable UE that had initially attached via GERAN/UTRAN and moved to EPC/E-UTRAN.

NOTE 5: The SMF+PGW-C might not include the GERAN/UTRAN PDP Context anchor functionality. Also, 5GS NAS capable UE does not indicate the support of this capability to the network during GPRS attach via GERAN/UTRAN. Hence, SMF+PGW-C might not be selected for the UE's PDP contexts that are setup in GERAN/UTRAN.

When a PDU session is moved from 5GS to EPS, the PGW-C+SMF keeps the registration and subscription in HSS+UDM until the corresponding PDN connection is released. The PGW-C+SMF may receive notification of subscription update regarding the DNN(s) which are associated with the PDN connection(s) connecting via EPS. In this case the PGW-C+SMF shall not trigger any action to those PDN connection(s). Instead, the MME will receive subscription update and trigger corresponding actions according to TS 23.401 [26].

If APN Rate Control is used when the UE moves from EPC to 5GC then the P-GW/SCEF and UE store the current APN Rate Control Status for an APN. If while connected to 5GC the last PDU Session to a DNN that is the same as the APN identified in the APN Rate Control Status is released then the APN Rate Control Status may be stored in the AMF in addition to the Small Data Rate Control Status and the UE discards the APN Rate Control Status. The APN Rate Control Status is stored in the AMF so it can be provided to the MME during mobility to EPC and subsequently applied at establishment of a new first PDN Connection to the same APN, if valid. The APN Rate Control Status is provided to the PGW-U+UPF if a first new PDU Session is established towards the DNN that is the same as the APN identified in the APN Rate Control Status if the UE moves back to EPC, taking into account its validity period.

The UE may be provided with initial APN Rate Control parameters by the SMF when a first new PDU Session is established for a DNN and S-NSSAI that supports interworking with EPS and the DNN matches an APN. The SMF provides the APN Rate Control Status for the APN that matches the DNN, if available at the SMF, otherwise the

configured APN Rate Control parameters for the APN that matches the DNN are provided as the initially applied parameters. If the initially applied parameters differ from the configured APN Rate Control parameters and the first APN Rate Control validity period expires, the UE is updated with the configured APN Rate Control parameters once the UE has moved to EPC.

NOTE 6: If the APN Rate Control Status is provided to a PGW-U+UPF it is not used for Small Data Rate Control while the UE is connected to 5GC, it is only used as the APN Rate Control Status if the UE moves to EPC.

NOTE 7: Encoding of APN and DNN specified in TS 23.003 [19] allows the comparison of EPS APN and 5GS DNN.

If a Service Gap timer is running in the AMF when the UE moves from 5GC to EPC, the AMF stops the running Service Gap timer. If the UE returns to 5GC from EPC the AMF provides the Service Gap Time to the UE as described in clause 5.31.16.

If a Service Gap timer is running in the MME when the UE moves from EPC to 5GC, the MME stops the running Service Gap timer. If the UE returns to E-UTRAN connected to EPC from 5GC the MME provides the Service Gap Time to the UE as described in TS 23.401 [26].

If a Service Gap timer is running in the UE when the UE moves to from 5GC to EPC and if Service Gap Time is received from the MME, the UE stores the received Service Gap Time for later use when the timer needs to be started next time, and the Service Gap timer that was started before the system change is kept running in the UE and applied for EPC. If a Service Gap timer is running in the UE when the UE moves to 5GC and if Service Gap Time is received from the AMF, the UE stores the received Service Gap Time for later use when the timer needs to be started next time, and the Service Gap timer that was started before the system change is kept running in the UE and applied in 5GS.

5.17.2.2 Interworking Procedures with N26 interface

5.17.2.2.1 General

Interworking procedures using the N26 interface, enables the exchange of MM and SM states between the source and target network. The N26 interface may be either intra-PLMN or inter-PLMN (e.g. to enable inter-PLMN mobility). When interworking procedures with N26 is used, the UE operates in single-registration mode. For the 3GPP access, the network keeps only one valid MM state for the UE, either in the AMF or MME. For the 3GPP access, either the AMF or the MME is registered in the HSS+UDM.

The support for N26 interface between AMF in 5GC and MME in EPC is required to enable seamless session continuity (e.g. for voice services) for inter-system change.

The UE's subscription may include restriction for Core Network Type (EPC) and RAT restriction for E-UTRA. If so, the UDM provides these restrictions to the AMF. The AMF includes RAT and Core Network type restrictions in the Handover Restriction List to the NR. The AMF and NR use these restrictions to determine if mobility of the UE to EPS or E-UTRA connected to EPS should be permitted. When the UE moves from 5GS to EPS, the SMF determines which PDU Sessions can be relocated to the target EPS, e.g. based on capability of the deployed EPS, operator policies for which PDU Session, seamless session continuity should be supported etc. The SMF can release the PDU Sessions that cannot be transferred as part of the handover or Idle mode mobility. However, whether the PDU Session is successfully moved to the target network is determined by target EPS.

Similarly, the UE's subscription may include restriction for Core Network Type (5GC) and RAT restriction for NR. If so, the HSS provides these restrictions to the MME. The MME includes RAT and Core Network type restrictions in the Handover Restriction List to the E-UTRAN. The MME and E-UTRAN use these restrictions to determine if mobility of the UE to 5GS or NR connected to 5GS should be permitted. When the UE moves from EPS to 5GS, for the case when the MME has selected P-GW+SMF even for PDN connections that cannot be relocated to the target 5GS, the P-GW+SMF determines which PDN Connections can be relocated to the target 5GS, e.g. based on capability of the deployed 5GS, subscription and operator policies for which PDN Connection, seamless session continuity should be supported etc. The P-GW+SMF and NG-RAN can reject the PDN Connections that cannot be transferred as part of the handover or Idle mode mobility.

For the case when the MME has selected standalone P-GW for a PDN connection for which session continuity is not supported and the AMF cannot retrieve the address of the corresponding SMF during EPS to 5GS mobility, the AMF does not move the PDN connection to 5GS.

NOTE 1: When applying the AMF planned removal procedure or the procedure to handle AMF failures (see clause 5.21.2) implementations are expected to update the DNS configuration to enable MMEs to discover alternative AMFs if the MME tries to retrieve a UE context from an AMF that has been taken out of service or has failed. This addresses the scenario of UEs performing 5GS to EPS Idle mode mobility and presenting a mapped GUTI pointing to an AMF that has been taken out of service or has failed.

In the case of mobility from 5GS to EPS, if the MME lacks certain capability, e.g. MME not supporting 15 EPS bearers, the 5GC shall not transfer the UE EPS bearers and/or EPS PDN connections that are not supported by the EPC network. If the MME does not support 15 EPS bearers, the AMF determines which EBIs cannot be transferred to EPS, and retrieves the EPS bearer contexts from the P-GW-C+SMF for the EBIs that can be transferred to EPS.

NOTE 2: How the AMF determines which EBIs can be transferred to EPS is according to local configuration, e.g according to DNN, S-NSSAI, ARP associated with an EBI.

5.17.2.2.2 Mobility for UEs in single-registration mode

When the UE supports single-registration mode and network supports interworking procedure with the N26 interface:

- For idle mode mobility from 5GS to EPS, the UE performs either TAU or Attach procedure with EPS GUTI mapped from 5G-GUTI sent as old Native GUTI, as described in clause 4.11.1.3.2.1 of TS 23.502 [3] and indicates that it is moving from 5GC. The UE includes in the RRC message a GUMMEI mapped from the 5G-GUTI and indicates it as a native GUMMEI and should in addition indicate it as "Mapped from 5G-GUTI". The MME retrieves the UE's MM and SM context from 5GC. For connected mode mobility from 5GS to EPS, either inter-system handover or RRC Connection Release with Redirection to E-UTRAN is performed. At inter-system handover, the AMF selects target MME based on 2 octet TAC format used in the Target ID as specified in TS 38.413 [34]. During the TAU or Attach procedure the HSS+UDM cancels any AMF registration associated with the 3GPP access (but not AMF registration associated with the non-3GPP access): an AMF that was serving the UE over both 3GPP and non-3GPP accesses does not consider the UE as deregistered over non 3GPP access.

- For the first TAU after 5GC initial Registration, the UE and MME for the handling of UE Radio Capabilities follow the procedures as defined in TS 23.401 [26] clause 5.11.2 for first TAU after GERAN/UTRAN Attach.

NOTE 1: MMEs supporting interworking with N26 interface are not required to process the indication from the UE that it is moving from 5GC and will assume that the UE is moving from another MME.

- For idle mode mobility from EPC to 5GC, the UE performs mobility Registration procedure with the 5G GUTI mapped from EPS GUTI and indicates that it is moving from EPC. The UE derives GUAMI from the native 5G-GUTI and includes GUAMI in the RRC message to enable RAN to route to the corresponding AMF (if available). If the UE holds no native 5G-GUTI, then the UE provides in the RRC message a GUAMI mapped from the EPS GUTI and indicates it as "Mapped from EPS". The AMF and SMF retrieve the UE's MM and SM context from EPC. For connected mode mobility from EPC to 5GC, either inter-system handover or RRC Connection Release with Redirection to NG-RAN is performed. At inter-system handover, the MME selects target AMF based on TAC used in the Target ID as specified in TS 38.413 [34]. During the Registration procedure, the HSS+UDM cancels any MME registration.

NOTE 2: During a transition period, the source eNB may be configured via O&M to know that the MME is not upgraded and thus supports only 2 octet TAC. The Target ID for the NG-RAN node is set as "Target eNB ID" in the existing IEs as defined in TS 38.413 [34].

For both idle mode and connected mode mobility from EPC to 5GC:

- The UE includes the native 5G-GUTI as an additional GUTI in the Registration request; the AMF uses the native 5G-GUTI to retrieve MM context identified by the 5G-GUTI from old AMF or from UDSF (if UDSF is deployed and the old AMF is within the same AMF set).

- If this is the first mobility event for a PDU Session that was established while being connected to EPC, the UE shall trigger the PDU Session Modification procedure and:

  - should indicate the support of Reflective QoS to the network (i.e. SMF) if the UE supports Reflective QoS functionality. If the UE indicated support of Reflective QoS, the network may provide a Reflective QoS Timer (RQ Timer) value to the UE;

- shall indicate the number of supported packet filters for signalled QoS rules. The network shall store this information so that subsequent mobility events do not require another signalling of it.

- should indicate the support of Multi-homed IPv6 PDU session to the network -i.e. SMF) if the UE supports Multi-homed IPv6 PDU session. If the UE indicated support of Multi-homed IPv6 PDU session, the network shall consider that this PDU session is supported to use multiple IPv6 prefixes.

- should provide the UE Integrity Protection Maximum Data Rate to the network -i.e. SMF). The network shall consider that the maximum data rate per UE for user-plane integrity protection supported by the UE is valid for the lifetime of the PDU session.

5.17.2.3 Interworking Procedures without N26 interface

5.17.2.3.1 General

For interworking without the N26 interface, IP address preservation is provided to the UEs on inter-system mobility by storing and fetching PGW-C+SMF and corresponding APN/DNN information via the HSS+UDM. In such networks AMF also provides an indication that interworking without N26 is supported to UEs during Initial Registration in 5GC or MME may optionally provide an indication that interworking without N26 is supported in the Attach procedure in EPC as defined in TS 23.502 [3] and TS 23.401 [26]. The UE provides an indication that it supports Request Type flag "handover" for PDN connectivity request during the attach procedure as described in clause 5.3.2.1 of TS 23.401 [26] and during initial Registration and Mobility Registration Update in 5GC.

NOTE 1: The UE support of Request Type flag "handover" for PDN connectivity request during the attach procedure is needed for IP address preservation in the case of interworking without N26.

The indication that interworking without N26 is valid for the entire Registered PLMN and for PLMNs equivalent to the Registered PLMN that are available in the Registration Area. The same indication is provided to all UEs served by the same PLMN. UEs that operate in interworking without N26 may use this indication to decide whether to register early in the target system. UEs that only support single registration mode may use this indication as described in clause 5.17.2.3.2. UE that support dual registration mode uses this indication as described in clause 5.17.2.3.3.

Interworking procedures without N26 interface use the following two features:

1. When UE performs Initial Attach in EPC (with or without "Handover" indication in PDN CONNECTIVITY Request message) and indicates that it is moving from 5GC, the MME indicates to the HSS+UDM not to cancel the registration of AMF, if any.

2. When UE performs Initial Registration in 5GC and indicates that it is moving from EPC, the AMF indicates to the HSS+UDM not to cancel the registration of MME, if any.

To support mobility both for single and dual registration mode UEs, the following also are supported by the network:

3. When PDU Session are created in 5GC, the PGW-C+SMF which supports EPS interworking stores the PGW-C+SMF FQDN along with DNN in the HSS+UDM.

4. The HSS+UDM provides the information about dynamically allocated PGW-C+SMF and APN/DNN information to the target CN network. If there are multiple PGW-C+SMF serving the UE for the same DNN which support EPS interworking in 5GS, the HSS+UDM select one of them according to operator's policy and provides together with the associated APN to the MME.

5. When PDN connections are created in EPC, the MME stores the PGW-C+SMF and APN information in the HSS+UDM.

NOTE 2: Items 3, 4 and 5 are also supported in networks that support interworking with N26 procedures. This enables a VPLMN that does not deploy N26 interface to provide IP address preservation to roamed-in single-registration mode UEs from a HPLMN that only supports interworking with N26 procedures.

When the network serving the UE supports 5GS-EPS interworking procedures without N26 interface, the SMF shall not provide the UEs with mapped target system parameters of the target system when UE is in the source network.

A UE that operates in dual registration mode ignores any received mapped target system parameters (e.g. QoS parameters, bearer IDs/QFI, PDU Session ID, etc.).

5.17.2.3.2 Mobility for UEs in single-registration mode

When the UE supports single-registration mode and network supports interworking procedure without N26 interface:

- For mobility from 5GC to EPC, the UE with at least one PDU Session established in 5GC may either:
  - if supported and if it has received the network indication that interworking without N26 is supported, perform Attach in EPC with a native EPS GUTI, if available, otherwise with IMSI with Request type "Handover" in PDN CONNECTIVITY Request message (TS 23.401 [26], clause 5.3.2.1) and indicating that the UE is moving from 5GC and subsequently moves all its other PDU Session using the UE requested PDN connectivity establishment procedure with Request Type "handover" flag (TS 23.401 [26] clause 5.10.2), or.
  - perform TAU with 4G-GUTI mapped from 5G-GUTI sent as old Native GUTI (TS 23.401 [26], clause 5.3.3) indicating that it is moving from 5GC, in which case the MME instructs the UE to re-attach. IP address preservation is not provided in this case.
  - for the first TAU after 5GC initial Registration, the UE and MME for the handling of UE Radio Capabilities follow the procedures as defined in TS 23.401 [26] clause 5.11.2 for first TAU after GERAN/UTRAN Attach.

NOTE 1: The first PDN connection may be established during the E-UTRAN Initial Attach procedure (see TS 23.401 [26]).

NOTE 2: At inter-PLMN mobility to a PLMN that is not an equivalent PLMN the UE always uses the TAU procedure.

- For mobility from 5GC to EPC, the UE with no PDU Session established in 5GC
  - performs Attach in EPC (TS 23.401 [26], clause 5.3.2.1) indicating that the UE is moving from 5GC.
- For mobility from EPC to 5GC, the UE performs Mobility Registration Update in 5GC with 5G-GUTI mapped from EPS GUTI and a native 5G-GUTI, if available, as Additional GUTI and indicating that the UE is moving from EPC. In this case, the AMF determines that old node is an MME, but proceeds as if the Registration is of type "initial registration". The UE may either:
  - if supported and if it has received the network indication "interworking without N26 supported", move all its PDN connections from EPC using the UE initiated PDU Session Establishment procedure with "Existing PDU Sessions" flag (TS 23.502 [3], clause 4.3.2.2.1), or
  - re-establish PDU Sessions corresponding to the PDN connections that it had in EPS. IP address preservation is not provided in this case.

NOTE 3: The additional native 5G-GUTI enables the AMF to find the UE's 5G security context (if available).

NOTE 4: When single-registration mode UE uses interworking procedures without N26, the registration states during the transition period (e.g. while UE is transferring all PDU Sessions / PDN Connections on the target side) are defined in Stage 3 specifications.

- If the network determines that the UE is changing RAT type, if the UE requests to relocate the PDU session from EPC to 5GC or 5GC to EPC, the SMF/MME uses the "PDU session continuity at inter RAT mobility" or "PDN continuity at inter-RAT mobility" information, respectively, in the subscription to determine whether to maintain the PDU session/PDN connection (if being handed over) or reject the PDU session request, with the relevant cause.
  - If the UE requested to move the PDU session and the "PDN continuity at inter RAT mobility" information indicated "disconnect the PDN connection with a reactivation request" the network should provide a suitable cause code to the UE so that it can request a new PDU session.

5.17.2.3.3 Mobility for UEs in dual-registration mode

To support mobility in dual-registration mode, the support of N26 interface between AMF in 5GC and MME in EPC is not required. A UE that supports dual registration mode may operate in this mode when it receives an indication from the network that interworking without N26 is supported.

For UE operating in dual-registration mode the following principles apply for PDU Session transfer from 5GC to EPC:

- UE operating in Dual Registration mode may register in EPC ahead of any PDU Session transfer using the Attach procedure indicating that the UE is moving from 5GC without establishing a PDN Connection in EPC if the EPC supports EPS Attach without PDN Connectivity as defined in TS 23.401 [26]. Support for EPS Attach without PDN Connectivity is mandatory for UE supporting dual-registration procedures.

NOTE 1: Before attempting early registration in EPC the UE needs to check whether EPC supports EPS Attach without PDN Connectivity by reading the related SIB in the target cell.

- UE performs PDU Session transfer from 5GC to EPC using the UE initiated PDN connection establishment procedure with "handover" indication in the PDN Connection Request message (TS 23.401 [26], clause 5.10.2).

- If the UE has not registered with EPC ahead of the PDU Session transfer, the UE can perform Attach in EPC with "handover" indication in the PDN Connection Request message (TS 23.401 [26], clause 5.3.2.1).

- UE may selectively transfer certain PDU Sessions to EPC, while keeping other PDU Sessions in 5GC.

- UE may maintain the registration up to date in both 5GC and EPC by re-registering periodically in both systems. If the registration in either 5GC or EPC times out (e.g. upon mobile reachable timer expiry), the corresponding network starts an implicit detach timer.

NOTE 2: Whether UE transfers some or all PDU Sessions on the EPC side and whether it maintains the registration up to date in both EPC and 5GC can depend on UE capabilities that are implementation dependent. The information for determining which PDU Sessions are transferred on EPC side and the triggers can be pre-configured in the UE and are not specified in this Release of the specification. The UE does not know before-hand, i.e. before trying to move a given PDU session to EPC, whether that PDU session can be transferred to EPC.

For UE operating in dual-registration mode the following principles apply for PDN connection transfer from EPC to 5GC:

- UE operating in Dual Registration mode may register in 5GC ahead of any PDN connection transfer using the Registration procedure indicating that the UE is moving from EPC (TS 23.502 [3], clause 4.2.2.2.2).

- UE performs PDN connection transfer from EPC to 5GC using the UE initiated PDU Session Establishment procedure with "Existing PDU Session" indication (TS 23.502 [3], clause 4.3.2.2.1).

- UE may selectively transfer certain PDN connections to 5GC, while keeping other PDN Connections in EPC.

- UE may maintain the registration up to date in both EPC and 5GC by re-registering periodically in both systems. If the registration in either EPC or 5GC times out (e.g. upon mobile reachable timer expiry), the corresponding network starts an implicit detach timer.

NOTE 3: Whether UE transfers some or all PDN connections on the 5GC side and whether it maintains the registration up to date in both 5GC and EPC can depend on UE capabilities that are implementation dependent. The information for determining which PDN connections are transferred on 5GC side and the triggers can be pre-configured in the UE and are not specified in this Release of the specification. The UE does not know before-hand, i.e. before trying to move a given PDN connection to 5GC, whether that PDN connection can be transferred to 5GC.

NOTE 4: If EPC does not support EPS Attach without PDN Connectivity the MME detaches the UE when the last PDN connection is released by the PGW as described in TS 23.401 [26] clause 5.4.4.1 (in relation to transfer of the last PDN connection to non-3GPP access).

When sending a control plane request for MT services (e.g. MT SMS) the network routes it via either the EPC or the 5GC. In absence of UE response, the network should attempt routing the control plane request via the other system.

NOTE 5: The choice of the system through which the network attempts to deliver the control plane request first is left to network configuration.

5.17.2.3.4 Redirection for UEs in connected state

When the UE supports single-registration mode or dual-registration mode without N26 interface:

- If the UE is in CM-CONNECTED state in 5GC, the NG-RAN may perform RRC Connection Release with Redirection to E-UTRAN based on certain criteria (e.g. based on local configuration in NG-RAN, or triggered by the AMF upon receiving Handover Request message from NG-RAN).

- If the UE is in ECM-CONNECTED state in EPC, the E-UTRAN may perform RRC Connection release with redirection to NG-RAN based on certain criteria (e.g. based on local configuration in E-UTRAN, or triggered by the MME upon receiving handover request from E-UTRAN).

5.17.2.4 Mobility between 5GS and GERAN/UTRAN

IP address preservation upon mobility between 5GS and GERAN/UTRAN is not supported.

Upon mobility from 5GS to GERAN/UTRAN (e.g. upon leaving NG-RAN coverage) the UE shall perform the A/Gb mode GPRS Attach procedure or Iu mode GPRS Attach procedure (see TS 23.060 [56]).

With regard to interworking between 5GS and the Circuit Switched domain when the GERAN or UTRAN network is operating in NMO II (i.e. no Gs interface between MSC and SGSN): upon mobility from 5GS to GERAN/UTRAN, the UE shall either:

- act as if it is returning after a loss of GERAN/UTRAN coverage (and e.g. only perform a periodic LAU if the periodic LAU timer has expired), or,

- perform a Location Update to the MSC.

Upon mobility from GERAN/UTRAN to 5GS (e.g. upon selecting an NG-RAN cell) the UE shall perform the Registration procedure of "initial registration" type as described in TS 23.502 [3]. The UE shall indicate a 5G-GUTI as UE identity in the Registration procedure if it has a stored valid native 5G-GUTI (e.g. from an earlier registration in the 5G System). Otherwise the UE shall indicate a SUCI.

If a UE in MICO mode moves to GERAN/UTRAN and any of the triggers defined in clause 5.4.1.3 occur, then the UE shall locally disable MICO mode and perform the A/Gb mode GPRS Attach procedure or Iu mode GPRS Attach procedure (see TS 23.060 [56]). The UE can renegotiate MICO when it returns to 5GS during (re-)registration procedure.

In Single Registration mode, expiry of the periodic RAU timer, or, the periodic LAU timer shall not cause the UE to change RAT.

The 5G SRVCC from NG-RAN to UTRAN is specified in the TS 23.216 [88]. After the 5G SRVCC to UTRAN, all the PDU sessions of the UE are released.

5.17.3 Interworking with EPC in presence of Non-3GPP PDU Sessions

When a UE is simultaneously connected to the 5GC over a 3GPP access and a non-3GPP access, it may have PDU Sessions associated with 3GPP access and PDU Sessions associated with non-3GPP access. When inter-system handover from 5GS to EPS is performed for PDU Sessions associated with 3GPP access, the PDU Sessions associated with non-3GPP access are kept anchored by the network in 5GC and the UE may either:

- keep PDU Sessions associated with non-3GPP access in 5GS (5GC+N3IWF or TNGF) (i.e. the UE is then registered both in EPS and, for non-3GPP access, in 5GS); or

- locally or explicitly release PDU Sessions associated with non-3GPP access; or

- once in EPS, transfer PDU Sessions associated with non-3GPP access to E-UTRAN by triggering PDN connection establishment with Request Type "Handover", as specified in TS 23.401 [26].

5.17.4 Network sharing support and interworking between EPS and 5GS

The detailed description for supporting network sharing and interworking between EPS and 5GS is described in clauses 4.11.1.2.1, 4.11.1.2.2, 4.11.1.3.2 and 4.11.1.3.3 of TS 23.502 [3].

5.17.5 Service Exposure in Interworking Scenarios

5.17.5.1 General

Clause 4.3.5 shows the Service Exposure Network Architecture in scenarios where for EPC-5GC Interworking is required.

In scenarios where interworking between 5GS and EPC is possible, the network configuration is expected to associate UEs with SCEF+NEF node(s) for Service Capability Exposure. The SCEF+NEF hides the underlying 3GPP network topology from the AF (e.g. SCS/AS) and hides whether the UE is served by 5GC or EPC.

If the service exposure function that is associated with a given service for a UE is configured in the UE's subscription information, then an SCEF+NEF identity shall be used to identify the exposure function. For example, if a UE is capable of switching between EPC and 5GC, then the SCEF ID that is associated with any of the UE's APN configurations should point to an SCEF+NEF node.

For external exposure of services related to specific UE(s), the SCEF+NEF resides in the HPLMN. Depending on operator agreements, the SCEF+NEF in the HPLMN may have interface(s) with NF(s) in the VPLMN.

The SCEF+NEF exposes over N33 the same API as the SCEF supports over T8. If CAPIF is not supported, the AF is locally configured with the API termination points for each service. If CAPIF is supported, the AF obtains the service API information from the CAPIF core function via the Availability of service APIs event notification or Service Discover Response as specified in TS 23.222 [64].

The common state information shall be maintained by the combined SCEF+NEF node in order to meet the external interface requirements of the combined node. The common state information includes at least the following data that needs to be common for the SCEF and NEF roles of SCEF+NEF:

- SCEF+NEF ID (must be the same towards the AF).
- SCEF+NEF common IP address and port number.
- Monitoring state for any ongoing monitoring request.
- Configured set of APIs supported by SCEF+ NEF.
- PDN Connection/PDU Session State and NIDD Configuration Information, including Reliable Data Service state information.
- Network Parameter Configuration Information (e.g. Maximum Response Time and Maximum Latency).

The SCEF+NEF need not perform the same procedures for the configuration of monitoring events towards the HSS+UDM twice. For example, if the HSS+UDM is deployed as a combined node, a monitoring event only need to be configured by the SCEF+NEF just once.

The SCEF+NEF may configure monitoring events applicable to both EPC and 5GC using only 5GC procedures towards UDM. In this case, the SCEF+NEF shall indicate that the monitoring event is also applicable to EPC (i.e. the event must be reported both by 5GC and EPC) and may include a SCEF address (i.e. if the event needs to be configured in a serving node in the EPC and the corresponding notification needs to be sent directly to the SCEF). If the HSS and UDM are deployed as separate network entities, UDM shall use HSS services to configure the monitoring event in EPC as defined in TS 23.632 [102]. The UDM shall return an indication to SCEF+NEF of whether the configuration of the monitoring event in EPC was successful. In the case that the UDM reports that the configuration of a monitoring event was not possible in EPC, then the SCEF+NEF may configure the monitoring event using EPC procedures via the HSS as defined in TS 23.682 [36].

NOTE 1: The SCEF+NEF uses only 5GC procedures to configure monitoring events in EPC and 5GC.

NOTE 2: In terms of the CAPIF, the SCEF+NEF is considered a single node.

5.17.5.2 Support of interworking for Monitoring Events

5.17.5.2.1 Interworking with N26 interface

In addition to the interworking principles documented in clause 5.17.2.2, the following applies for interworking with N26:

- When UE moves from 5GS to EPS and Monitoring Events are offered via AMF, the UE context information sent by AMF to MME includes the monitoring event configuration information.
- When UE moves from EPS to 5GS and Monitoring Events are offered via MME, the MME's MM context information sent by MME to AMF includes the monitoring event configuration information.

5.17.5.2.2 Interworking without N26 interface

When SCEF+NEF performs the procedure of monitoring via the AMF as described in clause 4.15.3.2.4 ("Exposure with bulk subscription") in TS 23.502 [3], if the AMF determines the interworking without N26 interface is supported, the AMF shall subscribe MME ID in the case of UE's mobility from 5GS to EPS from UDM+HSS on behalf of SCEF+NEF as described in clause 7.1.2. For single-registration mode, when UE's mobility from 5GS to EPS happens and Serving MME sends Update Location Request to the UDM+HSS, the UDM+HSS provides Serving MME ID to the SCEF+NEF which is the notification endpoint based on the subscription request from AMF. Then the SCEF+NEF performs the procedure of configuring monitoring via the MME for the same Monitoring Events as described in clause 5.6.2.1 of TS 23.682 [36].

When SCEF+NEF performs the procedure of monitoring via the UDM+HSS as described in clause 4.15.3.2.2 of TS 23.502 [3], when UE's mobility between 5GS and EPS happens, the UDM+HSS performs the procedure of configuring monitoring at the MME as described in clause 5.6.1.1 of TS 23.682 [36] and at the AMF as described in clause 4.15.3.2.1 of TS 23.502 [3].

5.17.5.3 Availability or expected level of a service API

A service related with common north-bound API may become unavailable due to UE being served by a CN node not supporting the service. If the availability or expected level of support of a service API associated with a UE changes, for example due to a mobility between 5GC and EPC, the AF shall be made aware of the change.

NOTE 1: If CAPIF is supported and the service APIs become (un)available for the 5GC or EPC network, the AF obtains such information from the CAPIF core function.

If the SCEF+NEF receives the subscription request from the AF for the availability or expected level of support of a service API, the SCEF+NEF subscribes a CN Type Change event for the UE or Group of UEs to the HSS+UDM. If the HSS+UDM receives the subscription for CN Type Change event, the HSS+UDM includes the latest CN type for the UE or Group of UEs in the response for the subscription. If the HSS+UDM detects that the UE switches between being served by the MME and the AMF, the CN Type Change event is triggered, and the HSS+UDM notifies the latest CN type for the UE or Group of UEs to the SCEF+NEF. Based on the CN type information, the SCEF+NEF can determine the availability or expected level of support of a given service. The AF will be informed of such information via a subscription/notification service operation. The AF can subscribe for the availability or expected level of support of a service API with report type indicating either One-time report or Continuous report. If there is no CN type information for the UE in the SCEF+NEF, the SCEF+NEF subscribes monitoring event for a new CN Type Change event for the UE or Group of UEs to the HSS+UDM, otherwise, SCEF+NEF determines the CN type locally in the following conditions:

- If the AF subscribes with report type indicating One-time report, the SCEF+NEF may consider the Freshness Timer of the latest CN type information for the UE or Group of UEs. The Freshness Timer is a parameter that is configured based on local SCEF+NEF policy. When a subscription request with One-time report type is received the SCEF+NEF checks if there is the latest CN type information received from the HSS+UDM for the indicated UE ID or External Group ID. If the elapsed time for the CN type information since the last reception is less than the Freshness Timer, then the SCEF+NEF may respond to the AF with the latest CN type information in order to avoid repeated query to HSS+UDM.
- The SCEF+NEF has established a direct connection with MME or AMF or SMF.

When the UE or all members of a Group of UEs are being served by a MME, EPC is determined as CN type. When the UE or all members of a Group of UEs are being served by an AMF, 5GC is determined as CN type. When the UE is

registered both in EPC and 5GC, or some members of a Group of UEs are registered in EPC while some members are registered in 5GC, 5GC+EPC is determined as CN type.

NOTE 2: If 5GC+EPC is determined as the CN type serving the UE or the group of UEs, the SCEF+NEF determines that service APIs for both 5GC and EPC are available to the UE or the group of UEs.

5.17.6 Void

5.17.7 Configuration Transfer Procedure between NG-RAN and E-UTRAN

5.17.7.1 Architecture Principles for Configuration Transfer between NG-RAN and E-UTRAN

The purpose of the Configuration Transfer between NG-RAN and E-UTRAN is to enable the transfer the RAN TNL address information between the gNB and eNodeB via MME and AMF.

In order to make the information transparent for the MME and AMF, the information is included in a transparent container. The source and target RAN node addresses, which allows the Core Network nodes to route the messages. The mechanism depicted in Figure 5.17.7.1-1.

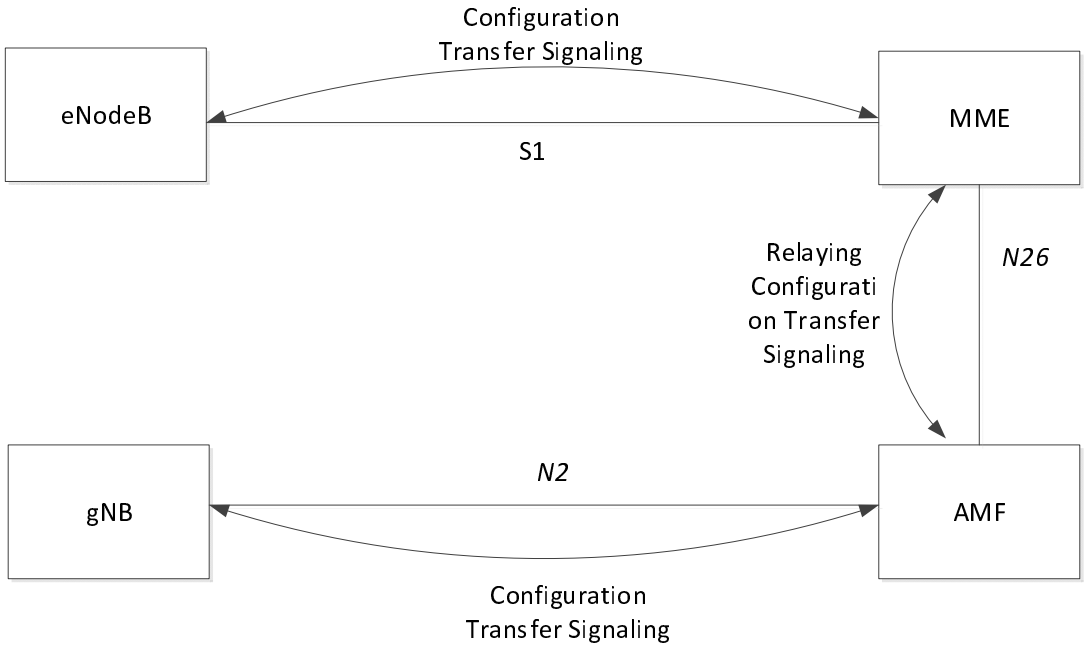


Figure 5.17.7.1-1: Configuration Transfer between gNB and E-UTRAN basic network architecture

The NG-RAN transparent containers are transferred from the source NG-RAN node to the destination E-UTRAN node and vice versa by use of Configuration Transfer messages.

An ENB Configuration Transfer message is used from the E-UTRAN node to the MME over S1 interface as described in TS 36.413 [100], the destination RAN node includes the en-gNB Identifier and may include a TAI associated with the en-gNB. If MME is aware that the en-gNB serves cells which provide access to 5GC, the MME relays the request towards a suitable AMF via inter-system signalling based on a broadcast 5G TAC. An AMF Configuration Transfer message is used from the AMF to the NG-RAN over N2 interface.

A Configuration Transfer message is used by the gNB node to the AMF over N2 interface for the reply, and a Configuration Transfer Tunnel message is used to tunnel the transparent container from AMF to MME over the N26 interface. MME relays this reply to the target eNB using a MME CONFIGURATION TRANSFER message. Transport of the RAN containers in E-UTRAN is specified in TS 23.401 [26].

Each Configuration Transfer message carrying the transparent container is routed and relayed independently by the core network node(s). Any relation between messages is transparent for the AMF and MME, i.e. a request/response exchange between applications, for example SON applications, is routed and relayed as two independent messages by the AMF and MME.

5.17.7.2 Addressing, routing and relaying

5.17.7.2.1 Addressing

All the Configuration Transfer messages contain the addresses of the source and destination RAN nodes.

An gNB node is addressed by the Target NG-RAN node identifier as described in TS 38.413 [34].

An eNodeB is addressed by the Target eNodeB identifier as described in TS 36.413 [100].

5.17.7.2.2 Routing

The source RAN node sends a message to its core network node including the source and destination addresses.

MME uses the destination address to route the message to the correct AMF via N26 interface. AMF uses the destination address to route the message to the correct MME via N26 interface.

The AMF connected to the destination RAN node decides which RAN node to send the message to, based on the destination address.

The MME connected to the destination RAN node decides which RAN node to send the message to, based on the destination address.

5.17.7.2.3 Relaying

The AMF performs relaying between N2 and N26 messages as described in TS 38.413 [34] and TS 29.274 [101].

The MME performs relaying between S1 and N26 message as described in TS 38.413 [34] and TS 29.274 [101].

5.18 Network Sharing

5.18.1 General concepts

A network sharing architecture shall allow multiple participating operators to share resources of a single shared network according to agreed allocation schemes. The shared network includes a radio access network. The shared resources include radio resources.

The shared network operator allocates shared resources to the participating operators based on their planned and current needs and according to service level agreements.

In this Release of the specification, only the 5G Multi-Operator Core Network (5G MOCN) network sharing architecture, in which only the RAN is shared in 5G System, is supported. 5G MOCN for 5G System, including UE, RAN and AMF, shall support operators' ability to use more than one PLMN ID (i.e. with same or different country code (MCC) some of which is specified in TS 23.122 [17] and different network codes (MNC)) or combinations of PLMN ID and NID. 5G MOCN supports NG-RAN Sharing with or without multiple Cell Identity broadcast as described in TS 38.300 [27].

5G MOCN also supports the following sharing scenarios involving non-public networks, i.e.NG-RAN can be shared by any combination of PLMNs, PNI-NPNs (with CAG), and SNPNs (each identified by PLMN ID and NID).

NOTE 1: PNI-NPNs (without CAG) are not explicitly listed above as it does not require additional NG-RAN sharing functionality compared to sharing by one or multiple PLMNs.

In all non-public network sharing scenarios, each Cell Identity is associated with one of the following configuration options:

- one or multiple SNPNs;

- one or multiple PNI-NPNs (with CAG); or
- one or multiple PLMNs only.

NOTE 2: Different PLMN IDs (or combinations of PLMN ID and NID) can also point to the same 5GC. When same 5GC supports multiple SNPNs (identified by PLMN ID and NID), then they are not used as equivalent SNPNs for a UE.

NOTE 3: There is no standardized mechanism to avoid paging collisions if the same 5G-S-TMSI is allocated to different UEs by different PLMNs or SNPNs of the shared network, as the risk of paging collision is assumed to be very low. If such risk is to be eliminated then PLMNs and SNPNs of the shared network needs to coordinate the value space of the 5G-S-TMSI to differentiate the PLMNs and SNPNs of the shared network.

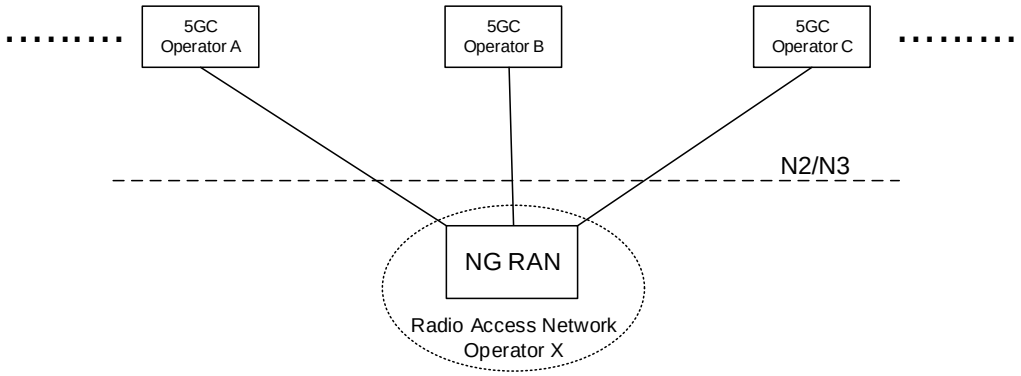


Figure 5.18.1-1: A 5G Multi-Operator Core Network (5G MOCN) in which multiple CNs are connected to the same NG-RAN

5.18.2 Broadcast system information for network sharing

If a shared NG-RAN is configured to indicate available networks (PLMNs and/or SNPNs) for selection by UEs, each cell in the shared radio access network shall in the broadcast system information include available core network operators in the shared network.

The Broadcast System Information broadcasts a set of PLMN IDs and/or PLMN IDs and NIDs and one or more additional set of parameters per PLMN e.g. cell-ID, Tracking Areas, CAG Identifiers. All 5G System capable UEs that connect to NG-RAN support reception of multiple PLMN IDs and per PLMN specific parameters. All SNPN-enabled UEs support reception of multiple combinations of PLMN ID and NID and SNPN-specific parameters.

The available core network operators (PLMNs and/or SNPNs) shall be the same for all cells of a Tracking Area in a shared NG-RAN network.

UEs not set to operate in SNPN access mode decode the broadcast system information and take the information concerning available PLMN IDs into account in PLMN and cell (re-)selection procedures. UEs set to operate in SNPN access mode decode the broadcast system information and take the information concerning available PLMN IDs and NIDs into account in network and cell (re-)selection procedures. Broadcast system information is specified in TS 38.331 [28] for NR, TS 36.331 [51] for E-UTRA and related UE access stratum idle mode procedures in TS 38.304 [50] for NR and TS 36.304 [52] for E-UTRA.

5.18.2a PLMN list handling for network sharing

The AMF prepares lists of PLMN IDs suitable as target PLMNs for use at idle mode cell (re)selection and for use at handover and RRC Connection Release with redirection. The AMF:

- provides the UE with the list of PLMNs that the UE shall consider as Equivalent to the serving PLMN (see TS 23.122 [17]); and

- provides the NG-RAN with a prioritised list of permitted PLMNs. When prioritising these PLMNs, the AMF may consider the following information: HPLMN of the UE, the serving PLMN, a preferred target PLMN (e.g. based on last used EPS PLMN), or the policies of the operator(s).

For a UE registered in an SNPN, the AMF shall not provide a list of equivalent PLMNs to the UE and shall not provide a list of permitted PLMNs to NG-RAN.

5.18.3 Network selection by the UE

NOTE: This clause applies to UEs not operating in SNPN access mode. Network selection for UEs set to operate in SNPN access mode is described in clause 5.30.2.4.

A UE that has a subscription to one of the sharing core network operators shall be able to select this core network operator while within the coverage area of the shared network and to receive subscribed services from that core network operator.

Each cell in shared NG-RAN shall in the broadcast system information include the PLMN-IDs concerning available core network operators in the shared network.

When a UE performs an Initial Registration to a network, one of available PLMNs shall be selected to serve the UE. UE uses all the received broadcast PLMN-IDs in its PLMN (re)selection processes which is specified in TS 23.122 [17]. UE shall inform the NG-RAN of the selected PLMN so that the NG-RAN can route correctly. The NG-RAN shall inform the core network of the selected PLMN.

As per any network, after Initial Registration to the shared network and while remaining served by the shared network, the network selection procedures specified in TS 23.122 [17] may cause the UE to perform a reselection of another available PLMN.

UE uses all of the received broadcast PLMN-IDs in its cell and PLMN (re)selection processes.

5.18.4 Network selection by the network

The NG-RAN uses the selected PLMN (provided by the UE at RRC establishment, or, provided by the AMF/source NG-RAN at N2/Xn handover) to select target cells for future handovers (and radio resources in general) appropriately. The network should not move the UE to another available PLMN, e.g. by handover, as long as the selected PLMN is available to serve the UE's location.

In the case of handover or network controlled release to a shared network:

- When multiple PLMN IDs are broadcasted in a cell selected by NG-RAN, NG-RAN shall select a target PLMN, taking into account the prioritized list of PLMN IDs provided via Mobility Restriction List from AMF.

- For Xn based HO procedure, Source NG-RAN indicates a selected PLMN ID to the target NG-RAN by using target cell ID.

- For N2 based HO procedure, the NG-RAN indicates a selected PLMN ID to the AMF as part of the TAI sent in the HO required message. Source AMF uses the TAI information supplied by the source NG-RAN to select the target AMF/MME. The source AMF should forward the selected PLMN ID to the target AMF/MME. The target AMF/MME indicates the selected PLMN ID to the target NG-RAN/eNB so that the target NG-RAN/eNB can select target cells for future handover appropriately.

- For RRC connection release with redirection to E-UTRAN procedure, NG-RAN decides the target network by using PLMN information as defined in the first bullet.

A change in serving PLMN is indicated to the UE as part of the UE registration with the selected network via 5G-GUTI in 5GS.

5.18.5 Network Sharing and Network Slicing

As defined in clause 5.15.1, a Network Slice is defined within a PLMN or SNPN. Network sharing is performed among different PLMNs and/or SNPNs. In the case of network sharing, each PLMN or SNPN sharing the NG-RAN defines and supports its PLMN- or SNPN- specific set of slices that are supported by the common NG-RAN.

5.19 Control Plane Load Control, Congestion and Overload Control

5.19.1 General

In order to ensure that the network functions within 5G System are operating under nominal capacity for providing connectivity and necessary services to the UE. Thus, it supports various measures to guard itself under various operating conditions (e.g. peak operating hour, extreme situations). It includes support for load (re-)balancing, overload control and NAS level congestion control. A 5GC NF is considered to be in overload when it is operating over its nominal capacity resulting in diminished performance (including impacts to handling of incoming and outgoing traffic).

5.19.2 TNLA Load Balancing and TNLA Load Re-Balancing

AMF can support load balancing and re-balancing of TNL associations between 5G-AN and AMF by using mechanisms specified in clause 5.21.1.

5.19.3 AMF Load Balancing

The AMF Load Balancing functionality permits UEs that are entering into an AMF Region/AMF Set to be directed to an appropriate AMF in a manner that achieves load balancing between AMFs. This is achieved by setting a Weight Factor for each AMF, such that the probability of the 5G-AN selecting an AMF is proportional to Weight Factor of the AMF. The Weight Factor is typically set according to the capacity of an AMF node relative to other AMF nodes. The Weight Factor is sent from the AMF to the 5G-AN via NGAP messages (see TS 38.413 [34]).

NOTE 1: An operator may decide to change the Weight Factor after the establishment of NGAP connectivity as a result of changes in the AMF capacities. E.g., a newly installed AMF may be given a very much higher Weight Factor for an initial period of time making it faster to increase its load.

NOTE 2: It is intended that the Weight Factor is NOT changed frequently. e.g. in a mature network, changes on a monthly basis could be anticipated, e.g. due to the addition of 5G-AN or 5GC nodes.

NOTE 3: Weight Factors for AMF Load Balancing are associated with AMF Names.

Load balancing by 5G-AN node is only performed between AMFs that belong to the same AMF set, i.e. AMFs with the same PLMN, AMF Region ID and AMF Set ID value.

The 5G-AN node may have their Load Balancing parameters adjusted (e.g. the Weight Factor is set to zero if all subscribers are to be removed from the AMF, which will route new entrants to other AMFs within an AMF Set).

5.19.4 AMF Load Re-Balancing

The AMF load re-balancing functionality permits cross-section of its subscribers that are registered on an AMF (within an AMF Set) to be moved to another AMF within the same AMF set with minimal impacts on the network and end users. AMF may request some or all of the 5G-AN node(s) to redirect a cross-section of UE(s) returning from CM-IDLE state to be redirected to another AMF within the same AMF set, if the 5G-AN is configured to support this. The AMF may request some or all of the 5G-AN node(s) to redirect the UEs served by one of its GUAMI(s) to a specific target AMF within the same AMF set or to any different AMF within the same AMF set.

When indicating a specific target AMF, the AMF should ensure that the load re-balancing will not cause overload in the target AMF.

NOTE: This requirement can be fulfilled by the AMF itself or by the OAM.

For UE(s) in CM-IDLE state, when UE subsequently returns from CM-IDLE state and the 5G-AN receives an initial NAS message with a 5G S-TMSI or GUAMI pointing to an AMF that requested for redirection, the 5G-AN should select the specific target AMF (provided by the original AMF) or a different AMF from the same AMF set and forward the initial NAS message.

For UE(s) in CONNECTED mode, similar mechanisms for AMF Management can be used to move the UE to another AMF in the same AMF set as described in clause 5.21.2, except that the old AMF deregisters itself from NRF.

The newly selected/target AMF (which is now the serving AMF) will re-assign the GUTI (using its own GUAMI(s)) to the UE(s). It is not expected that the 5G-AN node rejects any request or enables access control restriction when it receives a request for redirection for load control from the connected AMF(s).

When the AMF wants to stop redirection, the AMF can indicate that it can serve all UE(s) in CM-IDLE state to stop the redirection.

NOTE 1: An example use for the AMF load re-balancing functionality is for the AMF to pro-actively re-balance its load prior to reaching overload i.e. to prevent overload situation.

NOTE 2: Typically, AMF Load Re-Balancing is not needed when the AMF becomes overloaded because the Load Balancing function should have ensured that the other AMFs within the AMF Set are similarly overloaded.

5.19.5 AMF Control Of Overload

5.19.5.1 General

The AMF shall contain mechanisms for avoiding and handling overload situations. This includes the following measures:

- N2 overload control that could result in RRC reject, RRC Connection Release and unified access barring.
- NAS congestion control.

5.19.5.2 AMF Overload Control

Under unusual circumstances, if AMF has reached overload situation, the AMF activates NAS level congestion control as specified in Clause 5.19.7 and AMF restricts the load that the 5G-AN node(s) are generating, if the 5G-AN is configured to support overload control. N2 overload control can be achieved by the AMF invoking the N2 overload procedure (see TS 38.300 [27] and TS 38.413 [34]) to all or to a proportion of the 5G-AN nodes with which the AMF has N2 connections. The AMF may include the S-NSSAI(s) in NGAP OVERLOAD START message sent to 5G-AN node(s) to indicate the Network Slice(s) with which NAS signalling is to be restricted. To reflect the amount of load that the AMF wishes to reduce, the AMF can adjust the proportion of 5G-AN nodes which are sent NGAP OVERLOAD START message, and the content of the overload start procedure.

When NGAP OVERLOAD START is sent by multiple AMFs or from the same AMF set in the same PLMN towards the 5G-AN, it should be ensured that the signalling load is evenly distributed within the PLMN and within each AMF set.

A 5G-AN node supports restricting of 5G-AN signalling connection when a signalling connection establishment are attempted by certain UEs (which are registered or attempting to register with the 5GC), as specified in TS 38.331 [28] and TS 36.331 [51]. Additionally, a 5G-AN node provides support for the barring of UEs as described in TS 22.261 [2]. These mechanisms are further specified in TS 38.331 [28] and TS 36.331 [51]. For 3GPP Access Type, the signalling connection establishment attempt includes a RRC Connection Resume procedure from RRC-Inactive.

By sending the NGAP OVERLOAD START message, the AMF can request the 5G-AN node to apply the following behaviour for UEs that the AMF is serving:

a) Restrict 5G-AN signalling connection requests that are not for emergency, not for exception reporting and not for high priority mobile originated services; or

b) Restrict 5G-AN signalling connection requests for uplink NAS signalling transmission to that AMF;

c) Restrict 5G-AN signalling connection requests where the Requested NSSAI at AS layer only includes the indicated S-NSSAI(s) in the NGAP OVERLOAD START message. This applies also to RRC-Inactive Connection Resume procedure where the Allowed NSSAI in the stored UE context in the RAN only includes S-NSSAIs included in the NGAP OVERLOAD START.

d) only permit 5G-AN signalling connection requests for emergency sessions and mobile terminated services for that AMF; or

e) only permit 5G-AN signalling connection requests for high priority sessions, exception reporting and mobile terminated services for that AMF;

The above applies for RRC Connection Establishment procedure and RRC Connection Resume procedures over 3GPP access, as well as for the UE-N3IWF connection establishment over untrusted Non-3GPP access and for the UE-TNGF connection establishment over trusted Non-3GPP access.

The AMF can provide a value that indicates the percentage of connection requests to be restricted in the NGAP OVERLOAD START, and the 5G-AN node may consider this value for congestion control.

When restricting a 5G-AN signalling connection, the 5G-AN indicates to the UE an appropriate wait timer that limits further 5G-AN signalling connection requests until the wait timer expires.

During an overload situation, the AMF should attempt to maintain support for emergency services and for MPS.

When the AMF is recovering, the AMF can either:

- send a NGAP OVERLOAD START message with a new percentage value that permits more connection requests to be successful, or

- send a NGAP OVERLOAD STOP message.

to the same 5G-AN node(s) the NGAP OVERLOAD START was previously sent.

5.19.6 SMF Overload Control

The SMF shall contain mechanisms for avoiding and handling overload situations. This can include the following measures:

- SMF overload control that could result in rejections of NAS requests.

The SMF overload control may be activated by SMF due to congestion situation at SMF e.g. configuration, by a restart or recovery condition of a UPF, or by a partial failure or recovery of a UPF for a particular UPF(s).

Under unusual circumstances, if the SMF has reached overload situation, the SMF activates NAS level congestion control as specified in clause 5.19.7. The SMF may restrict the load that the AMF(s) are generating, if the AMF is configured to enable the overload restriction.

5.19.7 NAS level congestion control

5.19.7.1 General

NAS level congestion control may be applied in general (i.e. for all NAS messages), per DNN, per S-NSSAI, per DNN and S-NSSAI, or for a specific group of UEs.

NAS level congestion control is achieved by providing the UE a back-off time. To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the 5GC should select each back-off time value so that the deferred requests are not synchronized. When the UE receives a back-off time, the UE shall not initiate any NAS signalling with regards to the applied congestion control until the back-off timer expires or the UE receives a mobile terminated request from the network, or the UE initiates signalling for emergency services or high priority access.

AMFs and SMFs may apply NAS level congestion control, but should not apply NAS level congestion control for procedures not subject to congestion control.

5.19.7.2 General NAS level congestion control

This clause only applies to NAS Mobility Management congestion control.

Under general overload conditions the AMF may reject NAS messages from UEs using any 5G-AN. When a NAS request is rejected, a Mobility Management back-off time may be sent by the AMF to the UE. While the Mobility Management back-off timer is running, the UE shall not initiate any NAS request except for Deregistration procedure and procedures not subject to congestion control (e.g. high priority access, emergency services) and mobile terminated services. After any such Deregistration procedure, the back-off timer continues to run. While the Mobility Management

back-off timer is running, the UE is allowed to perform Mobility Registration Update if the UE is already in CM-CONNECTED state. If the UE receives a paging request or a NAS notification message from the AMF while the Mobility Management back off timer is running, the UE shall stop the Mobility Management back-off timer and initiate the Service Request procedure or the Mobility Registration Update procedure over 3GPP access and/or non-3GPP access as applicable. Over non-3GPP access, if the UE is in CM-IDLE state when the back-off timer is stopped, it shall initiate the UE-triggered Service Request procedure as soon as it switches back to CM-CONNECTED state.

In order to allow the UE to report the PS Data Off status change in PDU Session Modification Request message, the UE behaves as follows while keeping the NAS MM back-off timer running in the UE:

- When the UE is in CM-IDLE state and has not moved out of the Registration Area, the UE is allowed to send a Service Request message with an indication that the message is exempted from NAS congestion control. When the UE is in CM-IDLE mode and has moved out of the Registration Area, the UE is allowed to send a Mobility Registration Update request message, with a Follow-on request, and with an indication that the message is exempted from NAS congestion control.

- When the UE is in CM-CONNECTED state, the UE sends a PDU Session Modification Request with PS Data Off status change carried in UL NAS Transport message with an indication that the message is exempted from NAS congestion control.

When the NAS MM congestion control is activated at AMF, if the UE indicates that the NAS MM message is exempted from NAS congestion control, the AMF shall not reject the NAS MM message and shall forward the NAS SM message to the corresponding SMF with an indication that the NAS SM message was indicated to be exempted from NAS congestion control. The SMF ensures that the NAS SM message is not subject to congestion control otherwise the SMF rejects the message, e.g. the SMF shall reject PDU Session Modification received if it is not for Data Off status reporting.

The Mobility Management back-off timer shall not impact Cell/RAT/Access Type and PLMN change. Cell/RAT/TA/Access Type change does not stop the Mobility Management back-off timer. The Mobility Management back-off timer shall not be a trigger for PLMN reselection. The back-off timer is stopped as defined in TS 24.501 [47] when a new PLMN that is not an equivalent PLMN is accessed.

To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the AMF should select the Mobility Management back-off timer value so that the deferred requests are not synchronized.

If the UE required to report 5GSM Core Network Capability change, or the Always-on PDU Session Requested indication while the NAS MM congestion control timer was running and was unable to initiate MM signalling, the UE defers the related MM signalling until the MM congestion control timer expires and initiates after the expiry of the timer.

In the case of a UE with scheduled communication pattern, the AMF may consider the UE's communication pattern while selecting a value for the Mobility Management back-off timer so that the UE does not miss its only scheduled communication window.

The AMF should not reject Registration Request message for Mobility Registration Update that are performed when the UE is already in CM-CONNECTED state.

The AMF may reject the Service Request message and a UL NAS Transfer with a Mobility Management back-off time when the UE is already in CM-CONNECTED state. If UE receives a DL NAS Transfer message from the AMF while the Mobility Management back off timer is running, the UE shall stop the Mobility Management back-off timer.

For CM-IDLE state mobility, the AMF may reject Registration Request messages for Mobility Registration Update by including a Mobility Management back off time value in the Registration Reject message.

If UE registered in the same PLMN for 3GPP access and non-3GPP access and receives a Mobility Management back-off time from the AMF, the back-off time (and corresponding start and stop) is applied equally to both 3GPP access and non-3GPP access. If UE registered in different PLMNs for 3GPP access and non-3GPP access respectively and receives a Mobility Management back-off time, the back-off time is only applied to the PLMN that provides the time to the UE.

If the AMF rejects Registration Request messages or Service Request with a Mobility Management back-off time which is larger than the sum of the UE's Periodic Registration Update timer and the Implicit Deregistration timer, the AMF should adjust the mobile reachable timer and/or Implicit Deregistration timer such that the AMF does not implicitly deregister the UE while the Mobility Management back-off timer is running.

NOTE: This is to minimize signalling after the Mobility Management back-off timer expires.

If the AMF deregisters the UE with an indication of re-registration required, the UE behaviour for handling the back-off timer(s) is as specified in TS 24.501 [47].

5.19.7.3 DNN based congestion control

DNN based congestion control is designed for the purpose of avoiding and handling of NAS SM signalling congestion for the UEs with a back-off timer associated with or without a DNN regardless of the presence of an S-NSSAI. Both UE and 5GC shall support the functionality to enable DNN based congestion control.

SMFs may apply DNN based congestion control towards the UE by rejecting PDU Session Establishment Request message, or PDU Session Modification Request message except for those sent for the purpose of reporting 3GPP PS Data Off status change for a specific DNN with a running back-off timer. The SMF may release PDU Sessions belonging to a congested DNN by sending a PDU Session Release Command message towards the UE with a DNN back-off timer. If a DNN back-off time is set in the PDU Session Release Command message, the cause value of "reactivation requested" shall not be set.

When DNN based congestion control is activated at AMF e.g., configured by OAM, the AMF provides a NAS Transport Error message for the NAS Transport message carrying an SM message, and in the NAS Transport Error message it includes a DNN back-off timer.

The UE associates the received back-off time with the DNN (i.e. no DNN, DNN only) which the UE included in the uplink NAS MM message carrying the corresponding NAS SM request message.

The UE associates the received back-off time with the DNN (i.e. no DNN, DNN only) in any PLMN unless the DNN associated with the back-off timer is an LADN DNN in which case the UE only associates it to the PLMN in which the back-off time was received.

The UE behaves as follows when the DNN back-off timer is running:

- If a DNN is associated with the back-off timer, the UE shall not initiate any Session Management procedures for the congested DNN. The UE may initiate Session Management procedures for other DNNs. The UE shall not initiate any Session Management procedure for the corresponding APN when UE moves to EPS. The UE may initiate Session Management procedures for other APNs when the UE moves to EPS;

- If no DNN is associated with the back-off timer, the UE may only initiate Session Management requests of any PDU Session Type for a specific DNN;

- Upon Cell/TA/PLMN/RAT change, change of untrusted non-3GPP access network or change of Access Type, the UE shall not stop the back-off timer;

- The UE is allowed to initiate the Session Management procedures for high priority access and emergency services;

- The UE is allowed to initiate the Session Management procedure for reporting Data Off status change to the network;

- If the UE receives a network initiated Session Management message other than PDU Session Release Command for the congested DNN associated to a running back-off timer, the UE shall stop the back-off timer and respond to the 5GC;

- If the UE receives a PDU Session Release Command message for the congested DNN, it shall stop the back-off timer unless it receives a new back-off time from SMF;

- The UE is allowed to initiate PDU Session Release procedure (i.e. sending PDU Session Release Request message). The UE shall not stop the back-off timer when the related PDU Session is released;

- The list above is not an exhaustive list, i.e. more details of the above actions and further conditions, if any, are specified in TS 24.501 [47].

If UE initiates one of the Session Management procedures that are exempted from NAS congestion control, the UE indicates that the carried NAS SM message is exempted from NAS congestion control in the UL NAS Transport message as described in TS 24.501 [47]. When the DNN based congestion control is activated at AMF, if the UE indicates that the NAS SM message in the UL NAS Transport message is exempted from NAS congestion control, the AMF shall not apply DNN based congestion control on the UL NAS Transport message and shall forward the NAS SM message to the corresponding SMF with an indication that the message was received with exemption indication. The

SMF evaluates whether the NAS SM message is allowed to be exempted from DNN based congestion control. If it is not, the SMF rejects the message, e.g. the SMF shall reject PDU Session Modification received if it is not for Data Off status reporting).

The UE shall maintain a separate back-off timer for each DNN that the UE may use.

To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the 5GC should select the back-off timer value so that deferred requests are not synchronized.

If the UE required to report 5GSM Core Network Capability change, or the Always-on PDU Session Requested indication while DNN based congestion control was running and was unable to initiate SM signalling, the UE defers the related SM signalling until the DNN based congestion control timer expires and initiates the necessary SM signalling after the expiry of the timer.

The DNN based Session Management congestion control is applicable to the NAS SM signalling initiated from the UE in the Control Plane. The Session Management congestion control does not prevent the UE from sending and receiving data or initiating Service Request procedures for activating User Plane connection towards the DNN(s) that are under Session Management congestion control.

5.19.7.4 S-NSSAI based congestion control

S-NSSAI based congestion control is designed for the purpose of avoiding and handling of NAS signalling congestion for the UEs with back-off timer associated with or without an S-NSSAI regardless of the presence of a DNN.

The UE associates the received back-off time with the S-NSSAI and DNN (i.e. no S-NSSAI and no DNN, no S-NSSAI, S-NSSAI only, an S-NSSAI and a DNN) which was included in the uplink NAS MM message carrying the corresponding NAS SM request message for the PLMN which is under congestion.

S-NSSAI based congestion control is applied as follows:

- If an S-NSSAI is determined as congested, then the SMF may apply S-NSSAI based congestion control towards the UE for SM requests except for those sent for the purpose of reporting 3GPP PS Data Off status change for a specific S-NSSAI and provides a back-off time and an indication of HPLMN congestion;

- If the UE receives an S-NSSAI based back-off time without an indication of HPLMN congestion, the UE shall apply the S-NSSAI back-off timer only in the PLMN in which the back-off time was received. If the UE receives S-NSSAI based back-off time with an indication of HPLMN congestion, the UE shall apply the S-NSSAI based back-off timer in the PLMN in which the back-off time was received and in any other PLMN;

- The SMF may release PDU Sessions belonging to a congested S-NSSAI by sending a PDU Session Release Request message towards the UE with a back-off time associated either to the S-NSSAI only (i.e. with no specific DNN) or a combination of the S-NSSAI and a specific DNN;

- If S-NSSAI based congestion control is activated at AMF e.g., configured by OAM and an S-NSSAI is determined as congested, then the AMF applies S-NSSAI based congestion control towards the UE for UE-initiated Session Management requests. In this case, the AMF provides a NAS Transport Error message for the NAS Transport message carrying the SM message, and in the NAS Transport Error message it includes a back-off timer;

- The UE behaves as follows in the PLMN where the S-NSSAI based congestion control applies when the back-off timer is running:

    - If the back-off timer was associated with an S-NSSAI only (i.e. not associated with an S-NSSAI and a DNN), the UE shall not initiate any Session Management procedures for the congested S-NSSAI;

    - If the back-off timer was associated with an S-NSSAI and a DNN, then the UE shall not initiate any Session Management procedures for that combination of S-NSSAI and DNN;

    - If the UE receives a network-initiated Session Management message other than PDU Session Release Command for the congested S-NSSAI, the UE shall stop this back-off timer and respond to the 5GC;

    - If the UE receives a PDU Session Release Command message for the congested S-NSSAI, it shall stop the back-off timer unless it receives a new back-off time from SMF;

- Upon Cell/TA/PLMN/RAT change, change of untrusted non-3GPP access network or change of Access Type, the UE shall not stop the back-off timer for any S-NSSAI or any combination of S-NSSAI and DNN;
- The UE is allowed to initiate the Session Management procedures for high priority access and emergency services for the S-NSSAI;
- The UE is allowed to initiate the Session Management procedure for reporting Data Off status change for the S-NSSAI or the combination of S-NSSAI and DNN.

- If the back-off timer is not associated to any S-NSSAI, the UE may only initiate Session Management procedures for specific S-NSSAI;
- If the back-off timer is not associated to any S-NSSAI and DNN, the UE may only initiate Session Management procedures for specific S-NSSAI and DNN;
- The UE is allowed to initiate PDU Session Release procedure (e.g. sending PDU Session Release Request message). The UE shall not stop the back-off timer when the related PDU Session is released;
- The list above is not an exhaustive list, i.e. more details of the above actions and further conditions, if any, are specified in TS 24.501 [47].

The UE shall maintain a separate back-off timer for each S-NSSAI and for each combination of S-NSSAI and DNN that the UE may use.

If UE initiates one of the Session Management procedure that are exempt from NAS congestion control, the UE indicates that the carried NAS SM message is exempted from NAS congestion control in the UL NAS Transport message as described in TS 24.501 [47]. When the S-NSSAI based congestion control is activated at AMF, if the UE indicates that the NAS SM message in the UL NAS Transport message is exempted from NAS congestion control, the AMF shall not apply S-NSSAI based congestion control on the UL NAS Transport message and shall forward the NAS SM message to the corresponding SMF with an indication that the message was received with exemption indication. The SMF evaluates whether that the NAS SM message is allowed to be exempted from S-NSSAI based congestion control. If it is not, the SMF rejects the message, e.g. the SMF shall reject PDU Session Modification received if it is not for Data Off status reporting.

The back-off timer associated with an S-NSSAI or a combination of an S-NSSAI and a DNN shall only apply to congestion control for Session Management procedures when UE is in 5GS.

To avoid that large amounts of UEs initiate deferred requests (almost) simultaneously, the 5GC should select the value of the back-off timer for the S-NSSAI based congestion control so that deferred requests are not synchronized.

If the UE required to report 5GSM Core Network Capability change, or the Always-on PDU Session Requested indication while S-NSSAI based congestion control timer was running and was unable to initiate SM signalling, the UE defers the related SM signalling until the S-NSSAI based congestion control timer expires and initiates the necessary SM signalling after the expiry of the timer.

The S-NSSAI based congestion control does not prevent the UE from sending and receiving data or initiating Service Request procedure for activating User Plane connection for a PDU Session associated to the S-NSSAI that is under the congestion control.

5.19.7.5 Group specific NAS level congestion control

The group specific NAS level congestion control applies to a specific group of UEs. Group specific NAS level congestion control is performed at the 5GC only, and it is transparent to UE. The AMF or SMF or both may apply NAS level congestion control for a UE associated to an Internal-Group Identifier (see clause 5.9.7).

NOTE: 5GC logic for Group specific NAS level congestion control is not described in this Release of the specification.

5.19.7.6 Control Plane data specific NAS level congestion control

Under overload conditions the AMF may restrict requests from UEs for data transmission via Control Plane CIoT 5GS Optimisation. A Control Plane data back-off timer may be returned by the AMF (e.g. in Registration Accept messages, Service Reject message or Service Accept message). While the Control Plane data back-off timer is running, the UE shall not initiate any data transfer via Control Plane CIoT 5GS Optimisation, i.e. the UE shall not send any Control

Plane Service Request with uplink data as defined in TS 24.501 [47]. The AMF shall store the Control Plane data back-off timer per UE and shall not process any further requests (other than exception reporting and a response to paging) for Data Transport via a Control Plane Service Request from that UE while the Control Plane data back-off timer is still running.

NOTE 1: The Control Plane data back-off timer does not affect any other mobility management or session management procedure.

NOTE 2: The Control Plane data back-off timer does not apply to user plane data communication.

If the UE is allowed to send exception reporting, the UE may send an initial NAS Message for exception reporting even if Control Plane data back-off timer is running.

The UE may respond to paging with an initial NAS Message without uplink data even if the Control Plane data back-off timer is running.

If the AMF receives an initial NAS Message in reponse to a paging, and the AMF has a Control Plane data back-off timer running for the UE, and the AMF is not overloaded, and AMF decides to accept the Control Plane Service Request, then the AMF shall respond with Service Accept without the Control Plane data back-off timer and stop the Control Plane data back-off timer. If the UE receives a Service Accept without the Control Plane data back-off timer from the AMF while the Control Plane data back-off timer is running, the UE shall stop the Control Plane data back-off timer. The Control Plane data back-off timer in the UE and the AMF is stopped at PLMN change.

If the AMF receives a Control Plane Service Request with uplink data, and decides to send the UE a Control Plane data back-off timer, the AMF may decide to process the Control Plane Service Request with uplink data, i.e. decrypt and forward the data payload, or not based on the following:

- If the UE has indicated Release Assistance Information that no further Uplink and Downlink Data transmissions are expected, then the AMF may process (integrity check/decipher/forward) the received Control Plane data packet, and send a Service Accept to the UE with Control Plane data back-off timer. The UE interprets this as successful transmission of the Control Plane data packet starts the Control Plane data back-off timer.

- For all other cases, the AMF may decide to not process the received Control Plane data packet and send a Service Reject to the UE with Control Plane data back-off timer. The UE interprets this indication as unsuccessful delivery of the control plane data packet and starts the Control Plane data back-off timer. The AMF may take into consideration whether the PDU Session is set to Control Plane only to make the decision whether to reject the packet and send Service Reject or move the PDU Session to user plane and process the data packet as described in next bullet.

- Alternatively, if UE has not provided Release Assistance Information, and the PDU Session not set to Control Plane only, and UE supports N3 data transfer, then the AMF may initiate establishment of N3 bearer according to the procedure defined in TS 23.502 [3] clause 4.2.3. In this case the AMF may also return a Control Plane data back-off timer within the Service Accept.

The AMF only includes the Control Plane data back-off timer if the UE has indicated support for Control Plane CIoT 5GS optimizations in the Registration Request.

5.20 External Exposure of Network Capability

The Network Exposure Function (NEF) supports external exposure of capabilities of network functions. External exposure can be categorized as Monitoring capability, Provisioning capability, Policy/Charging capability and Analytics reporting capability. The Monitoring capability is for monitoring of specific event for UE in 5G System and making such monitoring events information available for external exposure via the NEF. The Provisioning capability is for allowing external party to provision of information which can be used for the UE in 5G System. The Policy/Charging capability is for handling QoS and charging policy for the UE based on the request from external party. The Analytics reporting capability is for allowing an external party to fetch or subscribe/unsubscribe to analytics information generated by 5G System.

Monitoring capability is comprised of means that allow the identification of the 5G network function suitable for configuring the specific monitoring events, detect the monitoring event, and report the monitoring event to the authorised external party. Monitoring capability can be used for exposing UE's mobility management context such as UE location, reachability, roaming status, and loss of connectivity. AMF stores URRP-AMF information in the MM

context to determine the NFs that are authorised to receive direct notifications from the AMF. UDM stores URRP-AMF information locally to determine authorised monitoring requests when forwarding indirect notifications.

Provisioning capability allows an external party to provision the Expected UE Behaviour or the 5GLAN group information or service specific information to 5G NF via the NEF. The provisioning comprises of the authorisation of the provisioning external third party, receiving the provisioned external information via the NEF, storing the information, and distributing that information among those NFs that use it. The externally provisioned data can be consumed by different NFs, depending on the data. In the case of provisioning the Expected UE Behaviour, the externally provisioned information which is defined as the Expected UE Behaviour parameters in TS 23.502 [3] clause 4.15.6.3 or Network Control parameter TS 23.502 [3] clause 4.15.6.3a consists of information on expected UE movement, Expected UE Behaviour parameters or expected Network Configuration parameter. The provisioned Expected UE Behaviour parameters may be used for the setting of mobility management or session management parameters of the UE. In the case of provisioning the 5GLAN group information the externally provisioned information is defined as the 5GLAN group parameters in TS 23.502 [3] clause 4.15.6.7, and it consists of some information on the 5GLAN group. The affected NFs are informed via the subscriber data update as specified in TS 23.502 [3] clause 4.15.6.2. The externally provisioned information which is defined as the Service Parameters in clause 4.15.6.7 of TS 23.502 [3] consists of service specific information used for supporting the specific service in 5G system. The provisioned Service Parameters may be delivered to the UEs. The affected NFs are informed of the data update.

Policy/Charging capability is comprised of means that allow the request for session and charging policy, enforce QoS policy, and apply accounting functionality. It can be used for specific QoS/priority handling for the session of the UE, and for setting applicable charging party or charging rate.

Analytics reporting capability is comprised of means that allow discovery of type of analytics that can be consumed by external party, the request for consumption of analytics information generated by NWDAF.

An NEF may support CAPIF functions for external exposure as specified in clause 6.2.5.1.

An NEF may support exposure of NWDAF analytics as specified in TS 23.288 [86].

5.20a Data Collection from an AF

An NF that needs to collect data from an AF may subscribe/unsubscribe to notifications regarding data collected from an AF, either directly from the AF or via NEF.

The data collected from an AF is used as input for analytics by the NWDAF.

The details for the data collected from an AF as well as interactions between NEF, AF and NWDAF are described in TS 23.288 [86].

5.21 Architectural support for virtualized deployments

5.21.0 General

5GC supports different virtualized deployment scenarios, including but not limited to the options below:

- A Network Function instance can be deployed as distributed, redundant, stateless, and scalable NF instance that provides the services from several locations and several execution instances in each location.
    - This type of deployments would typically not require support for addition or removal of NF instances for redundancy and scalability. In the case of an AMF this deployment option may use enablers like, addition of TNLA, removal of TNLA, TNLA release and rebinding of NGAP UE association to a new TNLA to the same AMF.
- A Network Function instance can also be deployed such that several network function instances are present within a NF set provide distributed, redundant, stateless and scalability together as a set of NF instances.
    - This type of deployments may support for addition or removal of NF instances for redundancy and scalability. In the case of an AMF this deployment option may use enablers like, addition of AMFs and TNLAs, removal of AMFs and TNLAs, TNLA release and rebinding of NGAP UE associations to a new TNLA to different AMFs in the same AMF set.

- The SEPP, although not a Network Function instance, can also be deployed distributed, redundant, stateless, and scalable.

- The SCP, although not a Network Function instance, can also be deployed distributed, redundant, and scalable.

Also, deployments taking advantage of only some or any combination of concepts from each of the above options is possible.

5.21.1 Architectural support for N2

5.21.1.1 TNL associations

5G-AN node shall have the capability to support multiple TNL associations per AMF, i.e. AMF name.

An AMF shall provide the 5G-AN node with the weight factors for each TNL association of the AMF.

The AMF shall be able to request the 5G-AN node to add or remove TNL associations to the AMF.

The AMF shall be able to indicate to the 5G-AN node the set of TNL associations used for UE-associated signalling and the set of TNL associations used for non-UE associated signalling.

NOTE: The TNL association(s) indicated for UE-associated and non-UE associated signalling can either be overlap or be different.

5.21.1.2 NGAP UE-TNLA-binding

While a UE is in CM-Connected state the 5G-AN node shall maintain the same NGAP UE-TNLA-binding (i.e. use the same TNL association and same NGAP association for the UE) unless explicitly changed or released by the AMF.

An AMF shall be able to update the NGAP UE-TNLA-binding (i.e. change the TNL association for the UE) in CM-CONNECTED state at any time.

An AMF shall be able to update the NGAP UE-TNLA-binding (i.e. change the TNL association for the UE) in response to an N2 message received from the 5G-AN by triangular redirection (e.g. by responding to the 5G-AN node using a different TNL association).

An AMF shall be able to command the 5G-AN node to release the NGAP UE-TNLA-binding for a UE in CM-CONNECTED state while maintaining N3 (user-plane connectivity) for the UE at any time.

5.21.1.3 N2 TNL association selection

The 5G-AN node shall consider the following factors for selecting a TNL association for the AMF for the initial N2 message e.g. N2 INITIAL UE MESSAGE:

- Availability of candidate TNL associations.

- Weight factors of candidate TNL associations.

The AMF may use any TNL association intended for non-UE associated signalling for initiation of the N2 Paging procedure.

5.21.2 AMF Management

5.21.2.1 AMF Addition/Update

The 5G System should support establishment of association between AMF and 5G-AN node.

A new AMF can be added to an AMF set and association between AMF and GUAMI can be created and/or updated as follows:

- AMF shall be able to dynamically update the NRF with the new or updated GUAMI(s) to provide mapping between GUAMI(s) and AMF information. Association between GUAMI(s) and AMF is published to NRF. In

addition, to deal with planned maintenance and failure, an AMF may optionally provide backup AMF information, i.e. it act as a backup AMF if the indicated GUAMI associated AMF is unavailable. It is assumed that the backup AMF and the original AMF are in the same AMF set as they have access to the same UE context. Based on that information one GUAMI is associated with an AMF, optionally with a backup AMF used for planned removal and/or another (same or different) backup AMF used for failure.

- Upon successful update, the NRF considers the new and/or updated GUAMI(s) for providing AMF discovery results to the requester. Requester can be other CP network functions.

- The new AMF provides its GUAMI to 5G-AN and 5G-AN store this association. If the association between the same GUAMI and another AMF exists in the 5G-AN (e.g. due to AMF planned removal), the previously stored AMF is replaced by the new AMF for the corresponding GUAMI association.

Information about new AMF should be published and available in the DNS system. It should allow 5G-AN to discover AMF and setup associations with the AMF required. N2 setup procedure should allow the possibility of AMFs within the AMF Set to advertise the same AMF Pointer and/or distinct AMF Pointer value(s) to the 5G-AN node.

To support the legacy EPC core network entity (i.e. MME) to discover and communicate with the AMF, the information about the AMF should be published and available in the DNS system. Furthermore, GUMMEI and GUAMI encoding space should be partitioned to avoid overlapping values in order to enable MME discover an AMF without ambiguity.

5.21.2.2 AMF planned removal procedure

5.21.2.2.1 AMF planned removal procedure with UDSF deployed

An AMF can be taken graciously out of service as follows:

- If an UDSF is deployed in the network, then the AMF stores the context for registered UE(s) in the UDSF. The UE context includes the AMF UE NGAP ID that is unique per AMF set. In order for the AMF planned removal procedure to work graciously, 5G-S-TMSI shall be unique per AMF Set. If there are ongoing transactions (e.g. N1 procedure) for certain UE(s), AMF stores the UE context(s) in the UDSF upon completion of an ongoing transaction.

- The AMF deregister itself from NRF indicating due to AMF planned removal.

NOTE 1: It is assumed that the UE contexts from the old AMF include all event subscriptions with peer CP NFs.

NOTE 2: Before removal of AMF the overload control mechanism can be used to reduce the amount of ongoing transaction.

An AMF identified by GUAMI(s) shall be able to notify the 5G-AN that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF. Upon receipt of the indication that an AMF(identified by GUAMI(s)) is unavailable, 5G-AN shall take the following action:

- 5G-AN should mark this AMF as unavailable and not consider the AMF for selection for subsequent N2 transactions until 5G-AN learns that it is available (e.g. as part of discovery results or by configuration).

- During NGAP Setup procedure, the AMF may include an additional indicator that the AMF will rebind or release the NGAP UE-TNLA-binding on a per UE-basis for UE(s) in CM-CONNECTED state. If that indicator is included and the 5G-AN supports timer mechanism, the 5G-AN starts a timer to control the release of NGAP UE-TNLA-binding. For the duration of the timer or until the AMF releases or re-binds the NGAP UE-TNLA-binding the AN does not select a new AMF for subsequent UE transactions. Upon timer expiry, the 5G-AN releases the NGAP UE UE-TNLA-binding(s) with the corresponding AMF for the respective UE(s), for subsequent N2 message, the 5G-AN should select a different AMF from the same AMF set when the subsequent N2 message needs to be sent.

NOTE 3: For UE(s) in CM-CONNECTED state, after indicating that the AMF is unavailable for processing UE transactions and including an indicator that the AMF releases the NGAP UE-TNLA-binding(s) on a per UE-basis, the AMF can either trigger a re-binding of the NGAP UE associations to an available TNLA on a different AMF in the same AMF set or use the NGAP UE-TNLA-binding per UE release procedure defined in TS 23.502 [3] to release the NGAP UE-TNLA-binding on a per UE-basis while requesting the AN to maintain N3 (user plane connectivity) and UE context information.

NOTE 4: The support and the use of timer mechanism in 5G-AN is up to implementation.

- If the instruction does not include the indicator, for UE(s) in CM-CONNECTED state, 5G-AN considers this as a request to release the NGAP UE-TNLA-binding with the corresponding AMF for the respective UE(s) while maintaining N3 (user plane connectivity) and UE context information. For subsequent N2 message, the 5G-AN should select a different AMF from the same AMF set when the subsequent N2 message needs to be sent.

- For UE(s) in CM-IDLE state, when it subsequently returns from CM-IDLE state and the 5G-AN receives an initial NAS message with a 5G S-TMSI or GUAMI pointing to an AMF that is marked unavailable, the 5G-AN should select a different AMF from the same AMF set and forward the initial NAS message. If the 5G-AN can't select an AMF from the same AMF set, the 5G-AN selects another new AMF as described in clause 6.3.5.

An AMF identified by GUAMI(s) shall be able to instruct other peer CP NFs, subscribed to receive such a notification, that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF. If the CP NFs register with NRF for AMF unavailable notification, then the NRF shall be able to notify the subscribed NFs to receive such a notification that AMF identified by GUAMI(s) will be unavailable for processing transactions. Upon receipt of the notification that an AMF (GUAMI(s)) is unavailable, the other CP NFs shall take the following actions:

- CP NF should mark this AMF (identified by GUAMI(s)) as unavailable and not consider the AMF for selection for subsequent MT transactions until the CP NF learns that it is available (e.g. as part of NF discovery results or via NF status notification from NRF).

- Mark this AMF as unavailable while not changing the status of UE(s) associated to this AMF (UE(s) previously served by the corresponding AMF still remain registered in the network), and AMF Set information.

- For the UE(s) that were associated to the corresponding AMF, when the peer CP NF needs to initiate a transaction towards the AMF that is marked unavailable, CP NF should select another AMF from the same AMF set (as in clause 6.3.5) and forward the transaction together with the old GUAMI. The new AMF retrieves UE context from the UDSF. If CP NF needs to send a notification to new AMF which is associated with a subscription from the old AMF, the CP NF shall exchange the old AMF information embedded in the Notification Address with the new AMF information, and use that Notification Address for subsequent communication.

NOTE 5: If the CP NF does not subscribe to receive AMF unavailable notification (either directly from the AMF or via NRF), the CP NF may attempt forwarding the transaction towards the old AMF and detect that the AMF is unavailable after certain number of attempts. When it detects unavailable, it marks the AMF and its associated GUAMI(s) as unavailable. CP NF should select another AMF from the same AMF set (as in clause 6.3.5) and forward the transaction together with the old GUAMI. The new AMF retrieves UE context from the UDSF and process the transaction.

Following actions should be performed by the newly selected AMF:

- When there is a transaction with the UE the newly selected AMF retrieves the UE context from the UDSF based on SUPI, 5G-GUTI or AMF UE NGAP ID and processes the UE message accordingly and updates the 5G-GUTI towards the UE, if necessary. For UE(s) in CM-CONNECTED state, it may also update the NGAP UE association with a new AMF UE NGAP ID towards the 5G-AN and replace the GUAMI in the UE context stored at the 5G-AN with the new GUAMI associated with the newly selected AMF if the 5G-GUTI has been updated. The AMF also informs the NG-RAN of the new UE Identity Index Value (derived from the new 5G-GUTI).

- When there is a transaction with the UE, the new selected AMF updates the peer NFs (that subscribed to receive AMF unavailability notification from old AMF), with the new selected AMF information.

- If the new AMF is aware of a different AMF serving the UE (by implementation specific means) it forwards the uplink N2 signalling of the UE to that AMF directly if necessary, the 5G-AN shall be able to receive the message from a different AMF, or it rejects the transaction from the peer CP NFs with a cause to indicate that new AMF has been selected, the peer CP NFs resend the transaction to the new AMF.

NOTE 6: This bullet above addresses situations where 5G-AN node selects an AMF and CP NFs select another AMF for the UE concurrently. It also addresses the situation where CP NFs select an AMF for the UE concurrently

- If the UE is in CM-IDLE state and the new AMF does not have access to the UE context, the new AMF selects one available AMF from the old AMF set as described in clause 6.3.5. The selected AMF retrieves the UE context from the UDSF and provides the UE context to the new AMF. If the new AMF doesn't receive the UE context then the AMF may force the UE to perform Initial Registration.

5.21.2.2.2 AMF planned removal procedure without UDSF

An AMF can be taken graciously out of service as follows:

- The AMF can forward registered UE contexts, UE contexts grouped by the same GUAMI value, to target AMF(s) within the same AMF set, including the source AMF name used for redirecting UE's MT transaction. The UE context includes the per AMF Set unique AMF UE NGAP ID. In order for the AMF planned removal procedure to work graciously, 5G-S-TMSI shall be unique per AMF set. If there are ongoing transactions (e.g. N1 procedure) for certain UE(s), AMF forwards the UE context(s) to the target AMF upon completion of an ongoing transaction.

- The AMF deregister itself from NRF indicating due to AMF planned removal.

NOTE 1: It is assumed that the UE contexts from the old AMF include all event subscriptions with peer CP NFs.

NOTE 2: Before removal of AMF the overload control mechanism can be used to reduce the amount of ongoing transaction.

An AMF shall be able to instruct the 5G-AN that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF and its corresponding target AMF(s). The target AMF shall be able to update the 5G-AN that the UE(s) served by the old GUAMI(s) are now served by target AMF. The target AMF provides the old GUAMI value that the 5G-AN can use to locate UE contexts served by the old AMF. Upon receipt of the indication that an old AMF is unavailable, 5G-AN shall take the following action:

- 5G-AN should mark this AMF as unavailable and not consider the AMF for selection for subsequent N2 transactions until 5G-AN learns that it is available (e.g. as part of discovery results or by configuration). The associated GUAMIs are marked as unavailable.

- During NGAP Setup, the AMF may include an additional indicator that the AMF will rebind or release the NGAP UE-TNLA-binding on per UE-basis. If that indicator is included and the 5G-AN supports timer mechanism, the 5G-AN starts a timer to control the release of NGAP UE-TNLA-binding(s). For the duration of the timer or until the AMF releases or re-binds the NGAP UE-TNLA-binding, the AN does not select a new AMF for subsequent transactions. Upon timer expiry, the 5G-AN releases the NGAP UE-TNLA-binding(s) with the corresponding AMF for the respective UE(s), for subsequent N2 message, the 5G-AN uses GUAMI which points to the target AMF that replaced the old unavailable AMF, to forward the N2 message to the corresponding target AMF(s).

NOTE 3: For UE(s) in CM-CONNECTED state, after indicating that the AMF is unavailable for processing UE transactions and including an indicator that the AMF releases the NGAP UE-TNLA-binding on a per UE-basis, the AMF can either trigger a re-binding of the NGAP UE associations to an available TNLA on a different AMF within the same AMF set or use the NGAP UE-TNLA-binding per UE release procedure defined in TS 23.502 [3] to release the NGAP UE-TNLA-binding on a per UE-basis while requesting the AN to maintain N3 (user plane connectivity) and UE context information.

NOTE 4: The support and the use of timer mechanism in 5G-AN is up to implementation.

If the instruction does not include the indicator, for UE(s) in CM-CONNECTED state, 5G-AN considers this as a request to release the NGAP UE UE-TNLA-binding(s) with the corresponding AMF for the respective UE(s) while maintaining N3 (user plane connectivity) and UE context information. For subsequent N2 message, the 5G-AN uses GUAMI based resolution which points to the target AMF that replaced the old unavailable AMF, to forward the N2 message to the corresponding target AMF(s).

- For UE(s) in CM-IDLE state, when it subsequently returns from CM-IDLE state and the 5G-AN receives an initial NAS message with a 5G S-TMSI or GUAMI, based resolution the 5G-AN uses 5G S-TMSI or GUAMI which points to the target AMF that has replaced the old unavailable AMF and, the 5G-AN forwards N2 message.

An AMF shall be able to instruct other peer CP NFs, subscribed to receive such a notification, that it will be unavailable for processing transactions by including GUAMI(s) configured on this AMF and its corresponding target AMF(s). The target AMF shall update the CP NF that the old GUAMI(s) is now served by target AMF. The old AMF provides the old GUAMI value to target AMF and the target AMF can use to locate UE contexts served by the old AMF. If the CP NFs register with NRF for AMF unavailable notification, then the NRF shall be able to notify the subscribed NFs to receive such a notification (along with the corresponding target AMF(s)) that AMF identified by GUAMI(s) will be

unavailable for processing transactions. Upon receipt of the notification that an AMF is unavailable, the other CP NFs shall take the following action:

- Mark this AMF and its associated GUAMI(s) as unavailable while not changing the status of UE(s) associated to this AMF (UE(s) previously served by the corresponding AMF still remain registered in the network), and AMF Set information.

- For the UE(s) that were associated to the corresponding AMF, when the peer CP NF needs to initiate a transaction towards the AMF that is marked unavailable and the old unavailable AMF was replaced by the target AMF, CP NF should forward the transaction together with the old GUAMI to the target AMF(s). If CP NF needs to send a notification to new AMF which is associated with a subscription from the old AMF, the CP NF shall exchange the old AMF information embedded in the Notification Address with the new AMF information, and use that Notification Address for subsequent communication.

NOTE 5: If the CP NF does not subscribe to receive AMF unavailable notification (either directly with the AMF or via NRF), the CP NF may attempt forwarding the transaction towards the old AMF and detect that the AMF is unavailable after certain number of attempts. When it detects unavailable, it marks the AMF and its associated GUAMI(s) as unavailable.

The following actions should be performed by the target AMF:

- To allow AMF process ongoing transactions for some UE(s) even after it notifies unavailable status to the target AMF, the target AMF keeps the association of the old GUAMI(s) and the old AMF for a configured time. During that configured period, if target AMF receives the transaction from the peer CP NFs and cannot locate UE context, it rejects the transaction with old AMF name based on that association, and the indicated AMF is only used for the ongoing transaction. The peer CP NFs resend the transaction to the indicated AMF only for the ongoing transaction. For subsequent transactions, peer CP NFs should use the target AMF. When the timer is expired, the target AMF deletes that association information.

- When there is a transaction with the UE the target AMF uses SUPI, 5G-GUTI or AMF UE NGAP ID to locate UE contexts and processes the UE transactions accordingly and updates the 5G-GUTI towards the UE, if necessary. For UE(s) in CM-CONNECTED state, it may also update the NGAP UE association with a new AMF UE NGAP ID towards the 5G-AN and replace the GUAMI in the UE context stored at the 5G-AN with the new GUAMI associated with the newly selected AMF if the 5G-GUTI has been updated. The AMF also informs the NG-RAN of the new UE Identity Index Value (derived from the new 5G-GUTI).

- Target AMF shall not use old GUAMI to allocate 5G-GUTI for UE(s) that are being served by Target AMF.

5.21.2.3 Procedure for AMF Auto-recovery

In order to try and handle AMF failure in a graceful manner (i.e. without impacting the UE), AMF can either back up the UE contexts in UDSF, or per GUAMI granularity in other AMFs (serving as backup AMF for the indicated GUAMI).

NOTE 1: Frequency of backup is left to implementation.

For deployments without UDSF, for each GUAMI the backup AMF information (in association to the GUAMI) is configured in the AMF. The AMF sends this information to 5G-AN and other CP NFs during the N2 setup procedure or the first (per NF) interaction with other CP NFs.

In the case that an AMF fails and the 5G-AN/peer CP NFs detect that the AMF has failed, or the 5G-AN/peer CP NFs receives notification from another AMF in the same AMF set that this AMF has failed, following actions are taken:

- The OAM deregister the AMF from NRF indicating due to AMF failure.

- 5G-AN marks this AMF as failed and not consider the AMF for selection until explicitly notified.

- For UE(s) in CM-CONNECTED state, 5G-AN considers failure detection or failure notification as a trigger to release the NGAP UE-TNLA-binding(s) with the corresponding AMF for the respective UE(s) while maintaining N3 (user plane connectivity) and other UE context information. For subsequent N2 message, if the backup AMF information of the corresponding failed AMF is not available the 5G-AN should select a different AMF (as in clause 6.3.5) from the same AMF set when the subsequent N2 message needs to be sent for the UE(s). If no other AMF from the AMF set is available, then it can select an AMF (implementation dependent)

from the same AMF Region as in clause 6.3.5. If backup AMF information of the corresponding failed AMF is available, the 5G-AN forwards the N2 message to the backup AMF.

NOTE 2: One AMF in the AMF set may be configured to send this failure notification message.

- For UE(s) in CM-IDLE state, when it subsequently returns from CM-IDLE state and the 5G-AN receives an initial NAS message with a S-TMSI or GUAMI pointing to an AMF that is marked failed, if the backup AMF information of the corresponding failed AMF is not available the 5G-AN should select a different AMF from the same AMF set and forward the initial NAS message. If no other AMF from the AMF set is available, then it can select an AMF (implementation dependent) from the same AMF Region as in clause 6.3.5. If backup AMF information of the corresponding failed AMF is available, the 5G-AN forwards the N2 message to the backup AMF.

- Peer CP NFs consider this AMF as unavailable while retaining the UE context.

- For the UE(s) that were associated to the corresponding AMF, when the peer CP NF needs to initiate a transaction towards the AMF, if backup AMF information of the corresponding failed AMF is not available, CP NF should select another AMF from the same AMF set and forward the transaction together with the old GUAMI. If neither the backup AMF nor any other AMF from the AMF set is available, then CP NF can select an AMF from the same AMF Region as in clause 6.3.5. If backup AMF information of the corresponding failed AMF is available, the CP NF forwards transaction to the backup AMF. If CP NF needs to send a notification to new AMF which is associated with a subscription from the old AMF, the CP NF shall exchange the old AMF information embedded in the Notification Address with the new AMF information, and use that Notification Address for subsequent communication.

- When the 5G-AN or CP NFs need to select a different AMF from the same AMF set,

  - For deployments with UDSF, any AMF from the same AMF set can be selected.

  - For deployments without UDSF, the backup AMF is determined based on the GUAMI of the failed AMF.

Following actions should be taken by the newly selected AMF:

- For deployments with UDSF, when there is a transaction with the UE the newly selected AMF retrieves the UE context from the UDSF using SUPI, 5G-GUTI or AMF UE NGAP ID and it processes the UE message accordingly and updates the 5G-GUTI towards the UE, if necessary.

- For deployments without UDSF, backup AMF (the newly selected AMF), based on the failure detection of the old AMF, instructs peer CP NFs and 5G-AN that the UE contexts corresponding to the GUAMI of the failed AMF is now served by this newly selected AMF. The backup AMF shall not use old GUAMI to allocate 5G-GUTI for UE(s) that are being served by Target AMF. The backup AMF uses the GUAMI to locate the respective UE Context(s).

- When there is a transaction with the UE, the new AMF updates the peer NFs (that subscribed to receive AMF unavailability notification from old AMF) with the new AMF information.

- If the new AMF is aware of a different AMF serving the UE (by implementation specific means) it redirects the uplink N2 signalling to that AMF, or reject the transaction from the peer CP NFs with a cause to indicate that new AMF has been selected. The peer CP NFs may wait for the update from the new AMF and resend the transaction to the new AMF.

NOTE 3: This bullet above addresses situations where 5G-AN node selects an AMF and other CP NFs select an AMF for the UE concurrently. It also addresses the situation where CP NFs select an AMF for the UE concurrently.

NOTE 4: It is assumed that the UE contexts from the old AMF include all event subscriptions with peer CP NFs.

- If the UE is in CM-IDLE state and the new AMF does not have access to the UE context, the new AMF selects one available AMF from the old AMF set as described in clause 6.3.5. The selected AMF retrieves the UE context from the UDSF and provides the UE context to the new AMF. If the new AMF doesn't receive the UE context then the AMF may force the UE to perform Initial Registration.

- If the UE is in CM-CONNECTED state, the new AMF may also update the NGAP UE association with a new AMF UE NGAP ID towards the 5G-AN and replace the GUAMI in the UE context stored at the 5G-AN with the new GUAMI associated with the newly selected AMF if the 5G-GUTI has been updated.

NOTE 5: The above N2 TNL association selection and AMF management is applied to the selected PLMN.

5.21.3 Network Reliability support with Sets

5.21.3.1 General

A Network Function instance can be deployed such that several network function instances are present within an NF Set to provide distribution, redundancy and scalability together as a Set of NF instances. The same is also supported for NF Services. This can be achieved when the equivalent NFs and NF Services share the same context data or by Network Function/NF Service Context Transfer procedures as specified in clause 4.26 of TS 23.502 [3].

NOTE: A NF can be replaced by an alternative NF within the same NF Set in the case of scenarios such as failure, load balancing, load re-balancing.

Such a network reliability design shall work in both communication modes, i.e. Direct Communication and Indirect Communication. In the Direct Communication mode, the NF Service consumer is involved in the reliability related procedures. In Indirect Communication mode, the SCP is involved in the reliability related procedures.

5.21.3.2 NF Set and NF Service Set

Equivalent Control Plane NFs may be grouped into NF Sets, e.g. several SMF instances are grouped into an SMF Set. NFs within a NF Set are interchangeable because they share the same context data, and may be deployed in different locations, e.g. different data centers.

In the case of SMF, multiple instances of SMFs within an SMF Set need to be connected to the same UPF:

- If the N4 association is established between a SMF instance and an UPF, each N4 association is only managed by the related SMF instance.
- If only one N4 association is established between a SMF Set and an UPF, any SMF in the SMF Set should be able to manage the N4 association with the UPF.

Furthermore, for a given UE and PDU Session any SMF in the SMF Set should be able to control the N4 session with the UPF (however, at any given time, only one SMF in the SMF Set will control the UPF for a given UE's PDU Session).

A Control Plane NF is composed of one or multiple NF Services. Within a NF a NF service may have multiple instances. These multiple NF Service instances can be grouped into NF Service Set if they are interchangeable with each other because they share the same context data.

NOTE: The actual mapping of instances to a given Set is up to deployment.

5.21.3.3 Reliability of NF instances within the same NF Set

The NF producer instance is the NF instance which host the NF Service Producer. When the NF producer instance is not available, another NF producer instance within the same NF Set is selected.

For Direct Communication mode, the NF Service consumer may subscribe to status change notifications of NF instance from the NRF. If the NF Service consumer is notified by the NRF or detects by itself (e.g. request is not responded) that the NF producer instance is not available anymore, another available NF producer instance within the same NF Set is selected by the NF Service consumer.

For Indirect Communication mode, the SCP or NF Service consumer may subscribe to status change notifications of NF instance from the NRF and selects another NF producer instance within the same NF Set if the original NF producer instance serving the UE is not available anymore.

NOTE: It is up to the implementation on how the SCP knows a NF producer instance is not available anymore.

5.21.3.4 Reliability of NF Services

When multiple NF Service instances within a NF Service Set are exposed to the NF Service consumer or SCP and the failure of NF Service instance is detected or notified by the NRF, i.e. it is not available anymore, the NF Service

consumer or SCP selects another NF Service instance of the same NF Service Set within the NF instance, if available. Otherwise the NF Service consumer or SCP selects a different NF instance within the same NF Set.

NOTE: The NF Producer instance can change the NF Service instance in the response to the service request.

When multiple NF Service instances within a NF Service Set are exposed to the NF Service consumer or SCP as a single NF Service, the reliability, i.e. the selection of an alternative NF Service instance is handled within the NF instance.

5.21.4 Network Function/NF Service Context Transfer

5.21.4.1 General

Network Function/NF Service Context Transfer Procedures allow transfer of Service Context of a NF/NF Service from a Source NF/NF Service Instance to the Target NF/NF Service Instance e.g. before the Source NF/NF Service can gracefully close its NF/NF Service. Service Context Transfer procedures are supported as specified in clause 4.26 of TS 23.502 [3].

Source NF / OA&M system determines when Source NF needs to transfer UE contexts to an NF in another NF set. Source NF should initiate this only for UE(s) that are not active in order to limit and avoid impacting services offered to corresponding UE(s).

5.22 System Enablers for priority mechanism

5.22.1 General

The 5GS and the 5G QoS model allow classification and differentiation of specific services such as listed in clause 5.16, based on subscription-related and invocation-related priority mechanisms. These mechanisms provide abilities such as invoking, modifying, maintaining, and releasing QoS Flows with priority, and delivering QoS Flow packets according to the QoS characteristics under network congestion conditions.

Subscription-related Priority Mechanisms include the ability to prioritize flows based on subscription information, including the prioritization of RRC Connection Establishment based on Unified Access Control mechanisms and the establishment of prioritized QoS Flows.

Invocation-related Priority Mechanisms include the ability for the service layer to request/invoke the activation of prioritized QoS Flows through an interaction over Rx/N5 and packet detection in the UPF.

QoS Mechanisms applied to established QoS Flows include the ability to fulfil the QoS characteristics of QoS Flows through preservation of differentiated treatment for prioritized QoS Flow and resource distribution prioritization.

Messages associated with priority services that are exchanged over service-based interfaces may include a Message Priority header to indicate priority information, as specified in TS 23.502 [3] and TS 29.500 [49].

In addition, the separation of concerns between the service classification provided by the core network through the association of Service Data Flows to QoS, and the enforcing of QoS differentiation in (R)AN through the association of QoS Flows to Data Radio bearers, supports the prioritization of QoS Flows when a limitation of the available data radio bearers occurs.

In addition, it also includes the ability for the service layer to provide instructions on how to perform pre-emption of media flows with the same priority assigned through an interaction over Rx as defined in TS 23.503 [45].

5.22.2 Subscription-related Priority Mechanisms

Subscription-related mechanisms which are always applied:

- (R)AN: During initial Access Network Connection Establishment, the Establishment Cause is set to indicate that special treatment is to be applied by the (R)AN in the radio resource allocation as specified in clause 5.2 for 3GPP access.

- **AMF:** Following Access Network Connection Establishment, the receipt of the designated Establishment Cause (i.e. high priority access) by the AMF will result in priority handling of the "Initial UE Message" received as part of the Registration procedures of clause 4.2.2 of TS 23.502 [3] and the Service Request procedures of clause 4.2.3 of TS 23.502 [3]. In addition, certain exemptions to Control Plane Congestion and Overload Control are provided as specified in clause 5.19.

Subscription-related mechanisms which are conditionally applied:

- **UE:** When barring control parameters are broadcast by the RAN, access barring based on Access Identity(es) configured in the USIM and/or an Access Category is applied prior to an initial upstream transmission for the UE which provides a mechanism to limit transmissions from UEs categorized as non-prioritized, while allowing transmissions from UEs categorized as prioritized (such as MPS subscribed UEs), during the RRC Connection Establishment procedure as specified in clause 5.2.

- **UDM:** One or more ARP priority levels are assigned for prioritized or critical services. The ARP of the prioritized QoS Flows for each DN is set to an appropriate ARP priority level. The 5QI is from the standard value range as specified in clause 5.7.2.7. In addition, Priority Level may be configured for the standardized 5QIs, and if configured, it overwrites the default value specified in the QoS characteristics Table 5.7.4-1.

- **PCF:** The "IMS Signalling Priority" information is set for the subscriber in the UDM, and the PCF modifies the ARP of the QoS Flow used for IMS signalling, for each DN which supports prioritized services leveraging on IMS signalling, to an appropriate ARP priority level assigned for that service.

5.22.3 Invocation-related Priority Mechanisms

The generic mechanisms used based on invocation-related Priority Mechanisms for prioritised services are based an interaction with an Application Server and between the Application Server and the PCF over Rx/N5 interface, as described in TS 23.228 [15] clause 5.21 in the case of MPS using IMS.

NOTE: Clause 5.21 in TS 23.228 [15] is applicable to 5GS, with the understanding that the term PCRF corresponds to PCF in the 5GS.

Invocation-related mechanisms for Mobile Originations e.g. via SIP/IMS:

- PCF: When an indication for a session arrives over the Rx/N5 Interface and the UE does not have priority for the signalling QoS Flow, the PCF derives the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, of the QoS Flow for Signalling as per Service Provider policy as specified in clause 6.1.3.11 of TS 23.503 [45].

- PCF: For sessions such as MPS, when establishing or modifying a QoS Flow for media as part of the session origination procedure, the PCF selects the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, to provide priority treatment to the QoS Flow(s).

- PCF: When all active sessions to a particular DN are released, and the UE is not configured for priority treatment to that particular PDU Session for a DN, the PCF will downgrade the IMS Signalling QoS Flows from appropriate settings of the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, to those entitled by the UE based on subscription.

Invocation-related mechanisms for Mobile Terminations e.g. via SIP/IMS:

- PCF: When an indication for a session arrives over the Rx/N5 Interface, mechanisms as described above for Mobile Originations are applied.

- UPF: If an IP packet arrives at the UPF for a UE that is CM-IDLE, the UPF sends a "Data Notification" including the information to identify the QoS Flow for the DL data packet to the SMF, as specified in clause 4.2.3.3 of TS 23.502 [3].

- SMF: If a " Data Notification" message arrives at the SMF for a QoS Flow associated with an ARP priority level value that is entitled for priority use, delivery of priority indication during the Paging procedure is provided by inclusion of the ARP in the N11 interface "N1N2MessageTransfer" message, as specified in clause 4.2.3.3 of TS 23.502 [3].

- AMF: If an "N1N2MessageTransfer" message arrives at the AMF containing an ARP priority level value that is entitled for priority use, the AMF handles the request with priority and includes the "Paging Priority" IE in the

N2 "Paging" message set to a value assigned to indicate that there is an IP packet at the UPF entitled to priority treatment, as specified in clause 4.2.3.3 of TS 23.502 [3].

- SMF: For a UE that is not configured for priority treatment, upon receiving the "N7 Session Management Policy Modification" message from the PCF with an ARP priority level that is entitled for priority use, the SMF sends an "N1N2MessageTransfer" to update the ARP for the Signalling QoS Flows, as specified in clause 4.3.3.2 of TS 23.502 [3].

- AMF: Upon receiving the "N1N2MessageTransfer" message from the SMF with an ARP priority level that is entitled for priority use, the AMF updates the ARP for the Signalling QoS Flows, as specified in clause 4.3.3.2 of TS 23.502 [3].

- (R)AN: Inclusion of the "Paging Priority" in the N2 "Paging" message triggers priority handling of paging in times of congestion at the (R)AN as specified in clause 4.2.3.3 of TS 23.502 [3].

Invocation-related mechanisms for the Priority PDU connectivity services:

- PCF: If the state of the Priority PDU connectivity services is modified from disabled to enabled, the QoS Flow(s) controlled by the Priority PDU connectivity services are established/modified to have the service appropriate settings of the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, using the PDU Session Modification procedure as specified in clause 4.3.3 of TS 23.502 [3].

- PCF: If the state of Priority PDU connectivity services is modified from enabled to disabled, the QoS Flow(s) controlled by the Priority PDU connectivity services are modified from service appropriate settings of the ARP and 5QI parameters, plus associated QoS characteristics as appropriate, to those entitled by the UE as per subscription, using the PDU Session Modification procedure as specified in clause 4.3.3 of TS 23.502 [3].

5.22.4 QoS Mechanisms applied to established QoS Flows

Mechanisms applied to established QoS Flows:

- (R)AN: QoS Flows requested in the Xn "Handover Request" or N2 "Handover Request" which are marked as entitled to priority by virtue of inclusion of an ARP value from the set allocated by the Service Provider for prioritised services are given priority over requests for QoS Flows which do not include an ARP from the set as specified in clause 4.9 of TS 23.502 [3].

- SMF: Congestion management procedures in the SMF will provide priority to QoS Flows established for sessions during periods of extreme overload. Prioritised services are exempt from any session management congestion controls. See clause 5.19.

  AMF: Congestion management procedures in the AMF will provide priority to Mobility Management procedures required for the prioritised services during periods of extreme overload. Prioritised services are exempt from Mobility Restrictions and any Mobility Management congestion controls. See clauses 5.3.4.1.1 and 5.19.5.

  QoS Flows whose ARP parameter is from the set allocated by the Service Provider for prioritised services' use shall be exempt from release during QoS Flow load rebalancing.

  (R)AN, UPF: IMS Signalling Packets associated with prioritised services' use are handled with priority. Specifically, during times of severe congestion when it is necessary to drop packets on the IMS Signalling QoS Flow to ensure network stability, these FEs shall drop packets not associated with priority signalling such as MPS or Mission Critical services before packets associated with priority signalling. See clauses 5.16.5 and 5.16.6.

- (R)AN, UPF: During times of severe congestion when it is necessary to drop packets on a media QoS Flow to ensure network stability, these FEs shall drop packets not associated with priority sessions such as MPS or Mission Critical services before packets associated with sessions. See clauses 5.16.5 and 5.16.6.

5.23 Supporting for Asynchronous Type Communication

Asynchronous type communication (ATC) enables 5GC to delay synchronizing UE context with the UE, so as to achieve an efficient signalling overhead and increase system capacity.

5GC supports asynchronous type communication with the following functionality:

- Capability to store the UE context based on the received message, and synchronize the UE context with the involved network functions or UE later;

For network function (e.g. PCF, UDM, etc.) triggered signalling procedure (e.g. network triggered Service Request procedure, network triggered PDU Session Modification procedure, etc.), if the UE CM state in the AMF is CM-IDLE state, the AMF updates and stores the UE context based on the received message without paging UE immediately. When the UE CM state in the AMF enters CM-CONNECTED state, the AMF forwards N1 and N2 message to synchronize the UE context with the (R)AN and/or the UE.

5.24 3GPP PS Data Off

This feature, when activated by the user, prevents traffic via 3GPP access of all IP packets, Unstructured and Ethernet data except for those related to 3GPP PS Data Off Exempt Services. The 3GPP PS Data Off Exempt Services are a set of operator services, defined in TS 22.011 [25] and TS 23.221 [23], that are the only allowed services when the 3GPP PS Data Off feature has been activated by the user. The 5GC shall support 3GPP PS Data Off operation in both non-roaming and roaming scenarios.

UEs may be configured with up to two lists of 3GPP PS Data Off Exempt Services and the list(s) are provided to the UEs by HPLMN via Device Management or UICC provisioning. When the UE is configured with two lists, one list is valid for the UEs camping in the home PLMN and the other list is valid for any VPLMN the UE is roaming in. When the UE is configured with a single list, without an indication to which PLMNs the list is applicable, then this list is valid for the home PLMN and any PLMN the UE is roaming in.

NOTE 1: The operator needs to ensure coordinated list(s) of 3GPP Data Off Exempt Services provisioned in the UE and configured in the network.

The UE reports its 3GPP PS Data Off status in PCO (Protocol Configuration Option) to (H-)SMF during UE requested PDU Session Establishment procedure for establishment of a PDU Session associated with 3GPP access and/or non-3GPP access. The UE does not need to report PS Data Off status during the PDU Session Establishment procedure for handover of the PDU Session between 3GPP access and non 3GPP access if 3GPP PS Data Off status is not changed since the last report. The PS Data Off status for a PDU Session does not affect data transfer over non-3GPP access.

If 3GPP PS Data Off is activated, the UE prevents the sending of uplink IP packets, Unstructured and Ethernet data except for those related to 3GPP PS Data Off Exempt Services, based on the pre-configured list(s) of Data Off Exempt Services.

If 3GPP PS Data Off is activated for a UE with MA PDU Sessions established through the ATSSS feature (see clause 5.32), the data transferred over the non-3GPP access of the MA PDU sessions are unaffected, which is ensured by the policy for ATSSS Control as specified in clause 5.32.3.

The UE shall immediately report a change of its 3GPP PS Data Off status in PCO by using UE requested PDU Session Modification procedure. This also applies to the scenario of inter-RAT mobility to NG-RAN and to scenarios where the 3GPP PS Data Off status is changed when the session management back-off timer is running as specified in clause 5.19.7.3 and clause 5.19.7.4. For UEs in Non-Allowed Area (or not in Allowed Area) as specified in clause 5.3.4.1, the UE shall also immediately report a change of its 3GPP PS Data Off status for the PDU Session. For UEs moving out of LADN area and the PDU Session is still maintained as specified in clause 5.6.5, the UE shall also immediately report a change of its 3GPP PS Data Off status for the PDU Session.

The additional behaviour of the SMF for 3GPP PS Data Off is controlled by local configuration or policy from the PCF as defined in TS 23.503 [45].

NOTE 2: For the PDU Session used for IMS services, the 3GPP Data Off Exempt Services are enforced in the IMS domain as specified TS 23.228 [15]. Policies configured in the (H-)SMF/PCF need to ensure those services are always allowed when the 3GPP Data Off status of the UE is set to "activated".

5.25 Support of OAM Features

5.25.1 Support of Tracing: Signalling Based Activation/Deactivation of Tracing

5GS supports tracing as described in TS 32.421 [66]. 5GS support may include subscriber tracing (tracing targeting a SUPI) or equipment tracing (tracing targeting a PEI) but also other forms of tracing further described in TS 32.421 [66].

NOTE 1: TS 23.501 / TS 23.502 [3] / TS 23.503 [45] only describe how 5GS signalling supports delivery of Trace Requirements about a UE (Signalling Based Activation/Deactivation of Tracing). OAM delivery of tracing requirements as well as the transfer of tracing results to one or more Operations Systems are out of scope of these documents.

The content of Trace Requirements about a UE (e.g. trace reference, address of the Trace Collection Entity, etc.) is defined in TS 32.421 [66].

Trace Requirements about a UE may be configured in subscription data of the UE and delivered together with other subscription data by the UDM towards the AMF, the SMF and/or the SMSF.

Signalling Based Activation/Deactivation of Tracing is limited to PLMNs of a single operator.

NOTE 2: Trace Requirements are not delivered between V-SMF and H-SMF or not provided by the UDM to an AMF / SMF / SMSF of a non-equivalent (H)PLMN.

NOTE 3: Signalling Based Activation/Deactivation of tracing for in-bound roamers is not defined in this version of the specification.

The AMF propagates Trace Requirements about a UE received from the UDM to network entities not retrieving subscription information from UDM, i.e. to the 5G-AN, to the AUSF and to the PCF. The AMF also propagates Trace Requirements to the SMF and to the SMSF.

Trace Requirements about a UE may be sent by the AMF to the 5G-AN as part of:

- the N2 procedures used to move the UE from CM-IDLE to CM-CONNECTED or,
- the N2 procedures to request a Hand-over from a target NG-RAN or,
- a stand-alone dedicated N2 procedure when tracing is activated while the UE is CM-CONNECTED.

Trace Requirements about a UE sent to a 5G-AN shall not contain information on the SUPI or on the PEI of the UE. Trace Requirements are directly sent from Source to Target NG-RAN in the case of Xn Hand-Over.

The SMF propagates Trace Requirements about a UE received from the UDM to the UPF (over N4) and to the PCF. The SMF provides Trace Requirements to the PCF when it has selected a different PCF than the one received from the AMF.

Once the SMF or the SMSF has received subscription data, Trace Requirements received from UDM supersede Trace requirements received from the AMF. Trace Requirements are exchanged on N26 between the AMF and the MME.

5.25.2 Support of OAM-based 5G VN group management

5GS supports 5G LAN-type service as defined in clause 5.29. 5G LAN-type service includes the 5G VN group management that can be configured by a network administrator.

The parameters for 5G VN group is defined in clause 5.29.

The 5G VN group parameters about a UE may be configured in subscription data of the UE and delivered together with other subscription data by the UDM towards the AMF and SMF.

5.26 Configuration Transfer Procedure

The purpose of the Configuration Transfer is to enable the transfer of information between two RAN nodes at any time via NG interface and the Core Network. An example of application is to exchange the RAN node's IP addresses in order to be able to use Xn interface between the NG-RAN node for Self-Optimised Networks (SON), as specified in TS 38.413 [34].

5.26.1 Architecture Principles for Configuration Transfer

Configuration Transfer between two RAN node provides a generic mechanism for the exchange of information between applications belonging to the RAN nodes.

In order to make the information transparent for the Core Network, the information is included in a transparent container that includes source and target RAN node addresses, which allows the Core Network nodes to route the messages. The mechanism is depicted in figure 5.26 1.

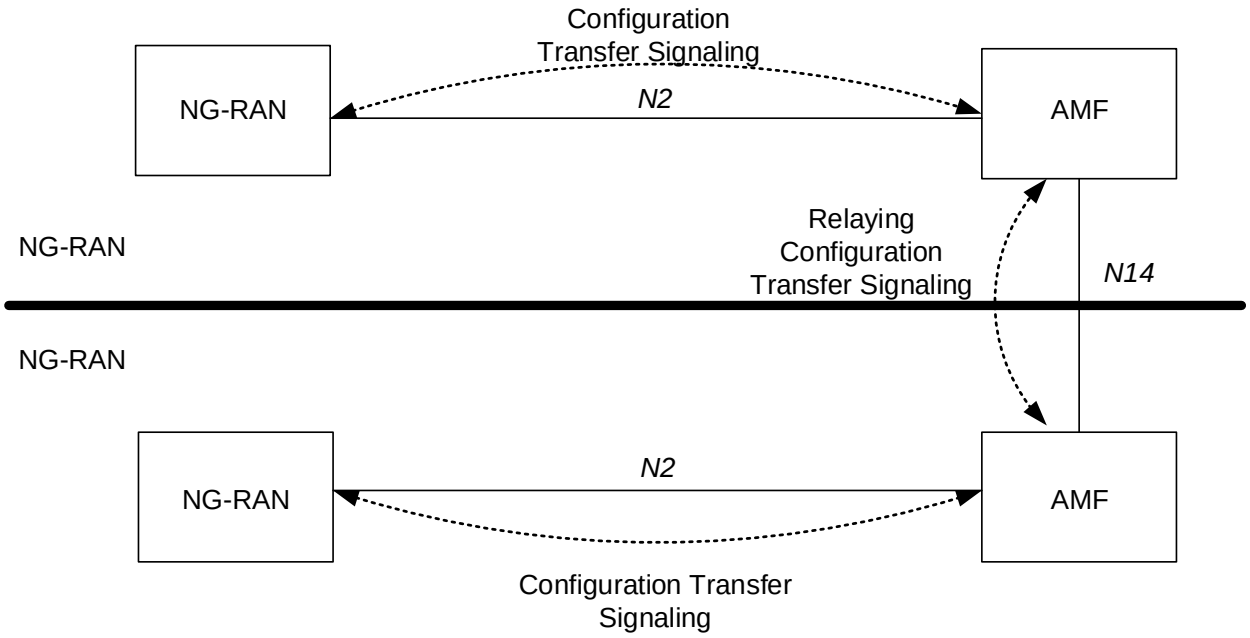


Figure 5.26-1: inter NG-RAN Configuration Transfer basic network architecture

The NG-RAN transparent containers are transferred from the source NG-RAN node to the destination NG-RAN node by use of Configuration Transfer messages.

A Configuration Transfer message is used from the NG-RAN node to the AMF over N2 interface, a AMF Configuration Transfer message is used from the AMF to the NG-RAN over N2 interface, and a Configuration Transfer Tunnel message is used to tunnel the transparent container from a source AMF to a target AMF over the N14 interface.

Each Configuration Transfer message carrying the transparent container is routed and relayed independently by the core network node(s).

5.26.2 Addressing, routing and relaying

5.26.2.1 Addressing

All the Configuration Transfer messages contain the addresses of the source and destination RAN nodes. An NG-RAN node is addressed by the Target NG-RAN node identifier.

5.26.2.2 Routing

The following description applies to all the Configuration Transfer messages used for the exchange of the transparent container.

The source RAN node sends a message to its core network node including the source and destination addresses. The AMF uses the destination address to route the message to the correct AMF via the N14 interface.

The AMF connected to the destination RAN node decides which RAN node to send the message to, based on the destination address.

5.26.2.3 Relaying

The AMF performs relaying between N2 and N14 messages as described in TS 38.413 [34], TS 29.518 [71].

5.27 Time Sensitive Communications

5.27.0 General

This clause describes 5G System features that support TSC and allow the 5G System to be integrated transparently as a bridge in an IEEE TSN network.

During the PDU Session establishment, the UE shall request to establish a PDU Session as an always-on PDU Session, and the PDU Sessions used for TSC are established as Always-on PDU session as described in clause 5.6.13. In this release of the specification:

- Home Routed PDU Sessions are not supported for TSC services;
- TSC PDU Sessions are supported only with PDU Session type Ethernet and SSC mode 1;
- Service continuity for TSC PDU Sessions is not supported when the UE moves from 5GS to EPS.

5.27.1 TSN Time Synchronization

5.27.1.1 General

For supporting TSN time synchronization, the 5GS is integrated with the external network as a TSN bridge as described in clauses 4.4.8 and 5.28.1. It shall be modelled as an IEEE 802.1AS [104] compliant entity according to TS 22.104 [105]. For TSN Synchronization, the entire E2E 5G system can be considered as an IEEE 802.1AS [104] "time-aware system". Only the TSN Translators (TTs) at the edges of the 5G system need to support the IEEE 802.1AS [104] operations. UE, gNB, UPF, NW-TT and DS- TTs are synchronized with the 5G GM (i.e. the 5G internal system clock) which shall serve to keep these network elements synchronized. The TTs located at the edge of 5G system fulfil all functions related to IEEE 802.1AS [104], e.g. (g)PTP support, timestamping, Best Master Clock Algorithm (BMCA), rateRatio. Figure 5.27.1-1 illustrates the 5G and TSN clock distribution model via 5GS.

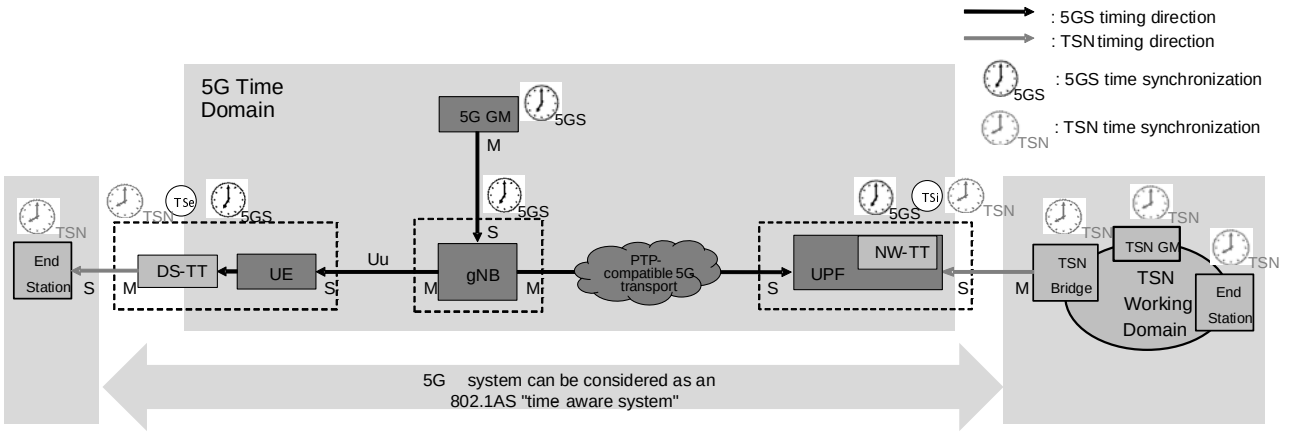


Figure 5.27.1-1: 5G system is modelled as IEEE 802.1AS compliant time aware system for supporting TSN time synchronization

Figure 5.27.1-1 depicts the two synchronizations systems considered: the 5GS synchronization and the TSN domain synchronization, as well as the Master (M) and Slave (S) ports considered when the TSN GM is located at TSN working domain.

- 5GS synchronization: Used for NG RAN synchronization. 5G RAN synchronization is specified in TS 38.331 [28].
- TSN domain synchronization: Provides synchronization service to TSN network. This process follows IEEE 802.1AS [104].

The two synchronization processes can be considered independent from each other and the gNB only needs to be synchronized to the 5G GM clock.

To enable TSN synchronization, the 5GS calculates and adds the measured residence time between the TTs into the Correction Field (CF) of the synchronization packets of the TSN working domain.

5.27.1.2 Distribution of timing information

5.27.1.2.1 Distribution of 5G internal system clock

The 5G internal system clock shall be made available to all user plane nodes in the 5G system. The UPF and NW-TT may get the 5G internal system clock via the underlying PTP compatible transport network with mechanisms outside the scope of 3GPP. The 5G internal system clock shall be made available to UE with signaling of time information related to absolute timing of radio frames as described in TS 38.331 [28]. The 5G internal system clock shall be made available to DS-TT by the UE.

5.27.1.2.2 Distribution of TSN clock and time-stamping

The mechanisms for distribution of TSN clock and time-stamping described in this clause are according to IEEE 802.1AS [104].

Upon reception of a downlink gPTP message the NW-TT makes an ingress timestamping (TSi) for each gPTP event (Sync) message and uses the cumulative rateRatio received inside the gPTP message payload (carried within Sync message for one-step operation or Follow_up message for two-step operation) to calculate the link delay from the upstream TSN node (gPTP entity) expressed in TSN GM time as specified in IEEE 802.1AS [104]. NW-TT then calculates the new cumulative rateRatio (i.e. the cumulative rateRatio of the 5GS) as specified in IEEE 802.1AS [104] and modifies the gPTP message payload (carried within Sync message for one-step operation or Follow_up message for two-step operation) as follows:

- Adds the link delay from the upstream TSN node in TSN GM time to the correction field.
- Replaces the cumulative rateRatio received from the upstream TSN node with the new cumulative rateRatio.
- Adds TSi in the Suffix field of the gPTP packet as described in Annex H.

UPF then forwards the gPTP message from TSN network to the UEs via all PDU sessions terminating in this UPF that the UEs have established to the TSN network. All gPTP messages are transmitted on a QoS Flow that complies with the residence time upper bound requirement specified in IEEE 802.1AS [104].

NOTE: The sum of the UE-DS-TT residence time and the PDB of the QoS Flow needs to be lower than the residence time upper bound requirement for a time-aware system specified in IEEE 802.1AS [104].

A UE receives the gPTP messages and forwards them to the DS-TT. The DS-TT then creates egress timestamping (TSe) for the gPTP event (Sync) messages for external TSN working domains. The difference between TSi and TSe is considered as the calculated residence time spent within the 5G system for this gPTP message expressed in 5GS time. The DS-TT then uses the rateRatio contained inside the gPTP message payload (carried within Sync message for one-step operation or Follow_up message for two-step operation) to convert the residence time spent within the 5GS in TSN GM time and modifies the payload of the gPTP message that it sends towards the downstream TSN node as follows:

- Adds the calculated residence time expressed in TSN GM time to the correction field.
- Removes TSi from the Suffix field.

5.27.1.3 Support for multiple TSN working domains

Each TSN working domain sends its own gPTP messages. The related Ethernet frames carry the gPTP multicast Ethernet destination MAC address and the gPTP message carries a specific PTP "domainNumber" that indicates the time domain they are referring to. The NW-TT makes ingress timestamping (TSi) for the gPTP event messages of all domains and forwards the gPTP messages of all domains to the UEs as specified in clause 5.27.1.2.2.

A UE receives gPTP messages and forwards them all to the DS-TT. The DS-TT receives the original TSN clock timing information and the corresponding TSi via gPTP messages for one or more TSN working domains. The DS-TT then makes egress timestamping (TSe) for the gPTP event messages for every external TSN working domain. Ingress and egress time stamping is based on the 5G system clock at NW-TT and DS-TT.

NOTE 1: An end-station can select TSN timing information of interest based on the "domainNumber" in the gPTP message.

The process described in "Distribution of TSN clock and time-stamping" is thus repeated for each TSN working domain between a DS-TT and the NW-TT it is connected to.

NOTE 2: If all TSN working domains can be made synchronous and the synchronization can be provided by the 5G clock, the NW-TT output ports towards the connected TSN networks propagate the 5G clock using the 802.1AS profile (i.e. the 5G system as an IEEE 802.1AS [104] compliant time-aware system).

NOTE 3: In this Release of specification, support for multiple TSN working domains is limited related to IEEE 802.1AS [104] for time synchronization procedure but it does not apply to interaction involving TSN AF and CNC. The corresponding IEEE specifications (i.e. IEEE 802.1Q [98]) are supported only for one specific TSN working domain and it is assumed that specific TSN working domain is associated with IEEE 802.1Q [98].

5.27.1a Periodic deterministic QoS

This feature allows the 5GS to support periodic deterministic communication where the traffic characteristics are known a-priori, and a schedule for transmission from the UE to a downstream node, or from the UPF to an upstream node is provided via external protocols outside the scope of 3GPP (e.g. IEEE TSN).

The features include the following:

- Providing TSC Assistance Information (TSCAI) that describe TSC flow traffic patterns at the gNB ingress and UE egress interfaces for traffic in downlink and uplink direction, respectively;
- Support for hold & forward buffering mechanism in DS-TT and NW-TT to de-jitter flows that have traversed the 5G System.

5.27.2 TSC Assistance Information (TSCAI)

TSC assistance information describes TSC traffic characteristics for use in the 5G System. The knowledge of TSN traffic pattern is useful for the gNB to allow it to more efficiently schedule periodic, deterministic traffic flows either via Configured Grants, Semi-Persistent Scheduling or with dynamic grants. TSC assistance information, as defined in Table 5.27.2-1, is provided from SMF to 5G-AN, e.g. upon QoS Flow establishment. The TSCAI parameters are set according to corresponding parameters obtained from the TSN AF. The TSN AF identifies the PDU session as described in clause 5.28.2.

The TSN AF is responsible for obtaining PSFP (IEEE 802.1Q [98]) parameters and use them to calculate traffic pattern parameters (such as burst arrival time with reference to the ingress port, periodicity, and flow direction) and responsible of forwarding these parameters in TSC Assistance Container to the SMF (via PCF). TSN AF may enable aggregation of TSN streams if the TSN streams belong to the same traffic class, terminate in the same egress port and have the same periodicity and compatible Burst arrival time. One set of parameters and one container are being calculated by the AF for multiple TSN streams to enable aggregation of TSN streams to the same QoS Flow.

Annex I describe how the traffic pattern information is determined.

NOTE 1: Further details of aggregation of TSN streams (including determination of burst arrival times that are compatible so that TSN streams can be aggregated) are left for implementation.

In this case, TSN AF creates one TSC Assistance Container for the aggregated TSN streams. The SMF will bind PCC rules with a TSC Assistance Container as described in clause 6.1.3.2.4 of TS 23.503 [45]. The SMF derives TSCAI on a per QoS Flow basis and send it to 5G-AN. The Burst Arrival Time and Periodicity component of the TSCAI that the SMF signals to the 5G-AN are specified with respect to the 5G clock. The SMF is responsible for mapping the Burst Arrival Time and Periodicity from a TSN clock to the 5G clock based on the time offset and cumulative rateRatio between TSN time and 5GS time as measured and reported by the UPF.

The TSCAI parameter determination in SMF is done as follows:

- For traffic in downlink direction, the SMF corrects the Burst Arrival Time in the TSN Assistance Container based on the latest received time offset measurement from the UPF and sets the TSCAI Burst Arrival Time as the sum of the corrected value and CN PDB as described in clause 5.7.3.4.

- For traffic in uplink direction, the SMF corrects the Burst Arrival Time in the TSN Assistance Container based on the latest received time offset measurement from the UPF and sets the TSCAI Burst Arrival Time as the sum of the corrected value and UE-DS-TT Residence Time.

- The SMF corrects the Periodicity in the TSN Assistance Container by the previously received cumulative rateRatio from the UPF and sets the TSCAI Periodicity as the corrected value.

- The SMF sets the TSCAI Flow Direction as the Flow Direction in the TSN Assistance Container.

NOTE 2: In order for the TSN AF to get Burst Arrival Time, Periodicity on a per TSN stream basis, support for IEEE 802.1Q [98] (as stated in clause 4.4.8.2) Per-Stream Filtering and Policing (PSFP) with stream gate operation is a prerequisite.

In the case of drift between TSN time and 5G time, the UPF updates the offset to SMF using the N4 Report Procedure as defined in TS 23.502 [3] clause 4.4.3.4. In the case of change of cumulative rateRatio between TSN time and 5G time, the UPF updates the cumulative rateRatio to SMF using the N4 Report Procedure as defined in TS 23.502 [3] clause 4.4.3.4. The SMF may then trigger a PDU Session Modification as defined in TS 23.502 [3] clause 4.3.3 in order to update the TSCAI parameter to the NG-RAN without requiring AN or N1 specific signalling exchange with the UE.

NOTE 3: In order to prevent frequent updates from the UPF, the UPF sends the offset or the cumulative rateRatio only when the difference between the current measurement and the previously reported measurement is larger than a threshold as described in TS 23.502 [3] clause 4.4.3.4.

Table 5.27.2-1: TSC Assistance Information

Assistance Information	Description
Flow Direction	The direction of the TSC flow (uplink or downlink).
Periodicity	It refers to the time period between start of two bursts.
Burst Arrival time	The arrival time of the data burst at either the ingress of the RAN (downlink flow direction) or egress interface of the UE (uplink flow direction).

5.27.3 Support for TSC QoS Flows

TSC QoS Flows use a Delay Critical GBR resource type and TSC Assistance Information. TSC QoS Flows may use standardized 5QIs, pre-configured 5QIs or dynamically assigned 5QI values (which requires signalling of QoS characteristics as part of the QoS profile) as specified in clause 5.7.2. For each instance of Periodicity, within each Period (defined by periodicity value), TSC QoS Flows are required to transmit only one burst of maximum size MDBV within the 5G-AN PDB. Known QoS Flow traffic characteristics provided in the TSCAI may be used to optimize scheduling in the 5GS.

The following is applicable for the QoS profile defined for TSC QoS Flows:

1. The TSC Burst Size may be used to set the MDBV as follows:

   The maximum TSC Burst Size is considered as the largest amount of data within a time period that is equal to the value of 5G-AN PDB of the 5QI that was set for this traffic class. The maximum value of TSC Burst Size should be mapped to a 5QI with MDBV that is equal or higher. This 5QI also shall have a PDB value that satisfies the bridge delay capabilities reported for the corresponding traffic class. For TSC QoS Flows, the Maximum Burst Size of the aggregated TSC streams to be allocated to this QoS Flow can be similarly mapped to a 5QI with MDBV value that is equal or higher, and the PDB of this 5QI shall also satisfy the bridge delay capabilities reported.

2. The PDB is explicitly divided into 5G-AN PDB and CN PDB as described in clause 5.7.3.4. Separate delay budgets are necessary for calculation of expected packet transmit times on 5G System interfaces. For the TSC QoS Flow, the5G-AN PDB is set to value of 5QI PDB minus the CN PDB as described in clause 5.7.3.4. The CN PDB may be static value or dynamic value and is up to the implementation of 5GS bridge.

3. The Maximum Flow Bitrate calculated by the TSN AF as per Annex I.1 may be used to set GFBR.

4. ARP is set to a pre-configured value.

5.27.4 Hold and Forward Buffering mechanism

DS-TT and NW-TT support a hold and forward mechanism to schedule traffic as defined in IEEE 802.1Q [98] if 5GS is to participate transparently as a bridge in a TSN network. The Hold and Forward buffering mechanism allows PDB based 5GS QoS to be used for TSC traffic since packets need only arrive at NW-TT or DS-TT egress prior to their scheduled transmission time.

5GS provides AdminControlList and AdminBaseTime as defined in IEEE 802.1Q [98] on a per Ethernet port basis to DS-TT and NW-TT for the hold and forward buffer as described in clause 5.28.3.

NOTE: How Hold and Forward buffer is supported by the TSN Translator is up to implementation.

5.27.5 5G System Bridge delay

In order for the 5G System to participate as a TSN bridge according to gate schedules specified, the 5GS Bridge is required to provide Bridge Delays as defined in IEEE 802.1Qcc [95] for each port pair and traffic class of the 5GS bridge to an IEEE TSN system. In order to determine 5GS Bridge Delays, the following components are needed:

1. UE-DS-TT Residence Time: the time taken within the UE and DS-TT to forward a packet between the UE and DS-TT port. UE-DS-TT Residence Time is provided at the time of PDU Session Establishment by the UE to the network.

NOTE 1: UE-DS-TT Residence Time is the same for uplink and downlink traffic and applies to all traffic classes.

2. Per traffic class minimum and maximum delays between the UE and the UPF/NW-TT that terminates the N6 interface (including UPF and NW-TT residence times), independent of frame length that a given 5GS deployment supports. The per-traffic class delays between the UE and the UPF/NW-TT are pre-configured in the TSN AF (see clause 5.28.4).

The TSN AF calculates the 5GS independentDelayMin and independentDelayMax values for each port pair and for each traffic class using the above components.

The dependentDelayMin and dependentDelayMax for 5GS Bridge specify the time range for a single octet of an Ethernet frame to transfer from ingress to egress and include the time to receive and store each octet of the frame, which depends on the link speed of the ingress Port as per IEEE 802.1Qcc [95].

NOTE 2: Further details how TSN AF determines dependentDelayMin and dependentDelayMax are up to implementation.

Since Residence times may vary among UEs and per traffic class delay between the UE and the UPF/NW-TT may vary among UPFs, the 5GS Bridge Delay is determined after the PDU Session Establishment for the corresponding UPF and the UE by the TSN AF. The TSN AF deduces the related port pair(s) from the port number of the DS-TT Ethernet port and port number of the serving NW-TT Ethernet port(s) when the TSN AF receives the 5GS Bridge information for a newly established PDU Session and caculates the bridge delays per port pair.

5.28 Support of integration with TSN

5.28.1 5GS TSN bridge management

5GS functions acts as one or more TSN Bridges of the TSN network. The 5GS Bridge is composed of the ports on a single UPF (i.e. PSA) side, the user plane tunnel between the UE and UPF, and the ports on the DS-TT side. For each 5GS Bridge of a TSN network, the port on NW-TT support the connectivity to the TSN network, the ports on DS-TT side are associated to the PDU Session providing connectivity to the TSN network.

The granularity of the 5GS TSN bridge is per UPF. The bridge ID of the 5GS TSN bridge is bound to the UPF ID of the UPF as identified in TS 23.502 [3]. The TSN AF stores the binding relationship between a port on UE/DS-TT side and a PDU Session during reporting of 5GS TSN bridge information. The TSN AF also stores the information about ports on the UPF/NW-TT side. The UPF/NW-TT forwards traffic to the appropriate egress port based on the traffic forwarding information. From the TSN AF point of view, a 5GS TSN bridge has a single NW-TT entity within UPF and the NW-TT may have multiple ports that are used for traffic forwarding.

NOTE 1: How to realize single NW-TT entity within UPF is up to implementation.

There is only one PDU Session per DS-TT port for a given UPF. All PDU Sessions which connect to the same TSN network via a specific UPF are grouped into a single 5GS bridge. The capabilities of each port on UE/DS-TT side and UPF/NW-TT side are integrated as part of the configuration of the 5GS Bridge and are notified to TSN AF and delivered to CNC for TSN bridge registration and modification.

NOTE 2: It is assumed that all PDU sessions which connect to the same TSN network via a specific UPF are handled by the same TSN AF.

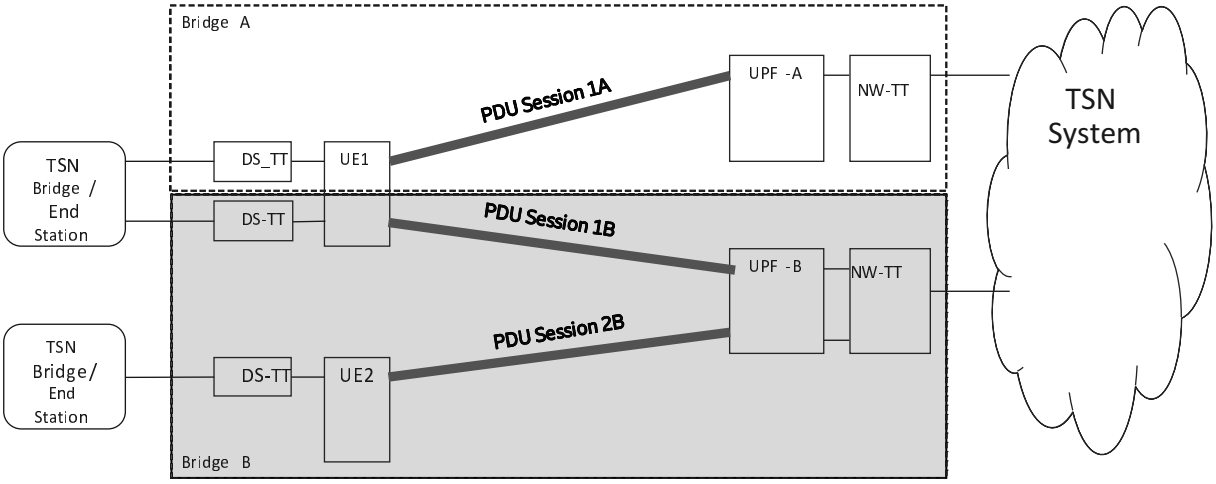


Figure 5.28.1-1: Per UPF based 5GS bridge

NOTE 3: If a UE establishes multiple PDU Sessions terminating in different UPFs, then the UE is represented by multiple 5GS TSN bridges.

In order to support TSN traffic scheduling over 5GS Bridge, the 5GS supports the following functions:

- Configure the bridge information in 5GS.
- Report the bridge information of 5GS Bridge to TSN network after PDU session establishment.
- Receiving the configuration from TSN network as defined in clause 5.28.2.
- Map the configuration information obtained from TSN network into 5GS QoS information (e.g. 5QI, TSC Assistance Information) of a QoS Flow in corresponding PDU Session for efficient time-aware scheduling, as defined at clause 5.28.2.

The bridge information of 5GS Bridge is used by the TSN network to make appropriate management configuration for the 5GS Bridge. The bridge information of 5GS Bridge includes at least the following:

- Information for 5GS Bridge:
  - Bridge ID

    Bridge ID is to distinguish between bridge instances within 5GS. The Bridge ID can be derived from the unique bridge MAC address as described in IEEE 802.1Q [98], or set by implementation specific means ensuring that unique values are used within 5GS;
  - Bridge Name (Bridge Name as defined in IEEE 802.1Q [98]);
  - Number of Ports;
  - list of port numbers.
- Capabilities of 5GS Bridge as defined in 802.1Qcc [95]:
  - 5GS Bridge delay per port pair per traffic class, including 5GS Bridge delay (dependent and independent of frame size, and their maximum and minimum values: independentDelayMax, independentDelayMin, dependentDelayMax, dependentDelayMin), ingress port number, egress port number and traffic class.
  - Propagation delay per port (txPropagationDelay), including transmission propagation delay, egress port number.
  - VLAN Configuration Information.

  NOTE 4: This Release of the specification does not support the modification of VLAN Configuration Information at the TSN AF.
- Topology of 5GS Bridge as defined in IEEE 802.1AB [97]:
  - Chassis ID subtype and Chassis ID of the 5GS Bridge.
- Traffic classes and their priorities per port as defined in IEEE 802.1Q [98].
- Stream Parameters as defined in clause 12.31.1 in IEEE 802.1Q [98], in order to support PSFP information:
  - Maximum number of filters, which defines the maximum number of streams that the bridge can handle;
  - Maximum number of gates, which can be equal or less than the maximum number of filters;
  - Maximum number of meters (optional) if meassurements are required;
  - Maximum length of the PSFPAdminControlList parameter that can be handled.

The following parameters: independentDelayMax and independentDelayMin, how to calculate them is left to implementation and not defined in this specification.

Bridge ID of the 5GS Bridge, port number(s) of the Ethernet port(s) in NW-TT could be preconfigured on the UPF. The UPF is selected for a PDU Session serving TSC as described in clause 6.3.3.3.

Port number of Ethernet port on the DS-TT for the PDU Session is assigned by the UPF during PDU session establishment. The port number of the DS-TT Ethernet port for a PDU Session shall be reported to the SMF from the UPF and further stored at the SMF. SMF provides the port number and MAC address of the Ethernet port in DS-TT of the related PDU session and port number(s) and MAC address(es) of the Ethernet port(s) in NW-TT to the TSN AF via

PCF. If a PDU session for which SMF has reported port numbers to TSN AF is released, then SMF informs TSN AF accordingly.

The TSN AF is responsible to receive the bridge information of 5GS Bridge from 5GS, as well as register or update this information to the TSN network.

5.28.2 5GS Bridge configuration

In order to schedule TSN traffic over 5GS Bridge, the configuration information of 5GS Bridge is mapped to 5GS QoS within the corresponding PDU Session. The QoS parameters mapping for TSN is described in TS 23.503 [45] clause 6.1.3.23.

The configuration information of 5GS Bridge as defined in IEEE 802.1Q [98], includes the following:

- Bridge ID of 5GS Bridge.
- Configuration information of scheduled traffic on ports of DS-TT and NW-TT:
  - Egress ports of 5GS Bridge, e.g., ports on DS-TT and NW-TT;
  - Traffic classes and their priorities.

NOTE 1: In this Release of the specification, only support simplified IEEE 802.1Q [98], Annex Q.2 for 5GS.

The configuration information of 5GS Bridge as defined in IEEE 802.1Q [98], includes the following:

- Chassis ID of 5GS Bridge;
- Traffic forwarding information as defined in IEEE 802.1Q [98] clause 8.8.1:
  - Destination MAC address and VLAN ID of TSN stream;
  - Port number in the Port MAP as defined in IEEE 802.1Q [98] clause 8.8.1.
- Configuration information per stream according to IEEE 802.1Q [98] clause 8.6.5.1:
  - Ingress port number of 5GS Bridge, i.e., ports on DS-TT/NW-TT;
  - Stream priority.

NOTE 2: In order to support IEEE 802.1Q [98] clause 8.6.5.1, it is required to support the Stream Identification function as specified by IEEE 802.1CB-2017 [83].

The SMF report the MAC address of the DS-TT port of the related PDU Session to TSN AF via PCF as the MAC address of the PDU Session. The association between the MAC address used by the PDU Session, 5GS Bridge ID and port number on DS-TT is maintained at TSN AF and further used to assist to bind the TSN traffic with the UE's PDU session.

With the Traffic forwarding information as defined in IEEE 802.1Q [98] clause 8.8.1 and PSFP information as defined in IEEE 802.1Q [98] clause 8.6.5.1, the TSN AF identifies the ingress port and egress port for a stream and derives the DS-TT MAC address of corresponding PDU session carrying this stream.

The TSN AF requests the PCF to reserve resources for an AF session with support for Time Sensitive Networking (TSN) as defined in clause 6.1.3.23 in TS 23.503 [45].

The TSN AF uses the stream filter instances in PSFP information as defined in IEEE 802.1Q [98] clause 8.6.5.1, and additionally traffic class information as defined in IEEE 802.1Q [98] clause 8.6.8.4, to derive the service data flow for TSN streams. The TSN AF uses the Priority values in the stream filter instances in PSFP information (if available) as defined in IEEE 802.1Q [98] clause 8.6.5.1, and may additionally use scheduled traffic information as defined in IEEE 802.1Q [98] clause 8.6.8.4, to derive the TSN QoS information for a given TSN stream or flow of aggregated TSN streams. The TSN AF determines the TSC Assistance Container as described in clause 5.27.2. The TSN AF associates the TSN QoS information and TSC Assistance Container with the corresponding service data flow description and provides to the PCF and the SMF as defined in TS 23.503 [45] clause 6.1.3.23.

NOTE 3: When the TSN stream priority information from PSFP is not available (priority value in stream filters is set to wild card) Scheduled traffic information IEEE 802.1Q [98] clause 8.6.8.4 can be used in combination with PSFP IEEE 802.1Q [98] clause 8.6.5.1 to obtain a priority value.

5.28.3 Port and bridge management information exchange in 5GS

5.28.3.1 General

Port and bridge management information is exchanged between CNC and TSN AF. The port management information, is related to Ethernet ports located in DS-TT or NW-TT.

5GS shall support transfer of standardized and deployment-specific port management information transparently between TSN AF and DS-TT or NW-TT, respectively inside a Port Management Information Container. NW-TT may support one or more ports. In this case, each port uses separate Port Management Information Container. 5GS shall also support transfer of standardized and deployment-specific bridge management information transparently between TSN AF and NW-TT, respectively inside a Bridge Management Information Container. Table 5.28.3.1-1 and Table 5.28.3.1-2 list standardized port management information and bridge management information, respectively.

Table 5.28.3.1-1: Standardized port management information

Port management information	Applicability (see Note 6)		Supported operations by TSN AF (see Note 1)	Reference
	DS-TT	NW-TT		
General				
Port management capabilities (see Note 2)	X	X	R	
Bridge delay related information				
txPropagationDelay	X	X	R	IEEE 802.1Qcc [95] clause 12.32.2.1
Traffic class related information				
Traffic class table	X	X	RW	IEEE 802.1Q [98] clause 12.6.3 and clause 8.6.6.
Gate control information				
GateEnabled	X	X	RW	IEEE 802.1Q [98] Table 12-29
AdminBaseTime	X	X	RW	IEEE 802.1Q [98] Table 12-29
AdminControlList	X	X	RW	IEEE 802.1Q [98] Table 12-29
AdminCycleTime (see Note 3)	X	X	RW	IEEE 802.1Q [98] Table 12-29
AdminControlListLength (see Note 3)	X	X	RW	IEEE 802.1Q [98] Table 12-28
Tick granularity	X	X	R	IEEE 802.1Q [98] Table 12-29
General Neighbor discovery configuration (NOTE 4)				
adminStatus	D	X	RW	IEEE 802.1AB [97] clause 9.2.5.1
lldpV2LocChassisIdSubtype	D	X	RW	IEEE 802.1AB [97] Table 11-2
lldpV2LocChassisId	D	X	RW	IEEE 802.1AB [97] Table 11-2
lldpV2MessageTxInterval	D	X	RW	IEEE 802.1AB [97] Table 11-2
lldpV2MessageTxHoldMultiplier	D	X	RW	IEEE 802.1AB [97] Table 11-2
NW-TT port neighbor discovery configuration				
lldpV2LocPortIdSubtype		X	RW	IEEE 802.1AB [97] Table 11-2
lldpV2LocPortId		X	RW	IEEE 802.1AB [97] Table 11-2
DS-TT port neighbor discovery configuration				
lldpV2LocPortIdSubtype	D		RW	IEEE 802.1AB [97] Table 11-2
lldpV2LocPortId	D		RW	IEEE 802.1AB [97] Table 11-2
Neighbor discovery information for each discovered neighbor of NW-TT				
lldpV2RemChassisIdSubtype		X	R	IEEE 802.1AB [97] Table 11-2
lldpV2RemChassisId		X	R	IEEE 802.1AB [97] Table 11-2
lldpV2RemPortIdSubtype		X	R	IEEE 802.1AB [97] Table 11-2
lldpV2RemPortId		X	R	IEEE 802.1AB [97] Table 11-2
TTL		X	R	IEEE 802.1AB [97] clause 8.5.4
Neighbor discovery information for each discovered neighbor of DS-TT (NOTE 5)				

lldpV2RemChassisIdSubtype	D		R	IEEE 802.1AB [97] Table 11-2
lldpV2RemChassisId	D		R	IEEE 802.1AB [97] Table 11-2
lldpV2RemPortIdSubtype	D		R	IEEE 802.1AB [97] Table 11-2
lldpV2RemPortId	D		R	IEEE 802.1AB [97] Table 11-2
TTL	D		R	IEEE 802.1AB [97] clause 8.5.4.1
Per-Stream Filtering and Policing information (NOTE 10)				
Stream Filter Instance Table (NOTE 8)				IEEE 802.1Q [98] Table 12-32
StreamHandleSpec	X	X	RW	IEEE 802.1Q [98] Table 12-32
PrioritySpec	X	X	RW	IEEE 802.1Q [98] Table 12-32
StreamGateInstanceID	X	X	RW	IEEE 802.1Q [98] Table 12-32
Stream Gate Instance Table (NOTE 9)				IEEE 802.1Q [98] Table 12-33
StreamGateInstance	X	X	R	IEEE 802.1Q [98] Table 12-33
PSFPAdminBaseTime	X	X	RW	IEEE 802.1Q [98] Table 12-33
PSFPAdminControlList	X	X	RW	IEEE 802.1Q [98] Table 12-33
PSFPAdminCycleTime	X	X	RW	IEEE 802.1Q [98] Table 12-33
PSFPTickGranularity	X	X	R	IEEE 802.1Q [98] Table 12-33

NOTE 1: R = Read only access; RW = Read/Write access.
NOTE 2: Indicates which standardized and deployment-specific port management information is supported by DS-TT or NW-TT.
NOTE 3: AdminCycleTime and AdminControlListLength are optional for gate control information.
NOTE 4: If DS-TT supports neighbor discovery, then TSN AF sends the general neighbor discovery configuration for DS-TT Ethernet ports to DS-TT. If DS-TT does not support neighbor discovery, then TSN AF sends the general neighbor discovery configuration for DS-TT Ethernet ports to NW-TT using the Bridge Management Information Container (refer to Table 5.28.3.1-2) and NW-TT performs neighbor discovery on behalf on DS-TT.
NOTE 5: If DS-TT supports neighbor discovery, then TSN AF retrieves neighbor discovery information for DS-TT Ethernet ports from DS-TT. If DS-TT does not support neighbor discovery, then TSN AF retrieves neighbor discovery information for DS-TT Ethernet ports from NW-TT, using the Bridge Management Information Container (refer to Table 5.28.3.1-2), the NW-TT performing neighbor discovery on behalf on DS-TT.
NOTE 6: X = applicable; D = applicable when validation and generation of LLDP frames is processed at the DS-TT.
NOTE 7: Void.
NOTE 8: There is a Stream Filter Instance Table per Stream.
NOTE 9: There is a Stream Gate Instance Table per Gate.
NOTE 10: The use of PSFP information is mandatory at the TSN AF and is optional at both DS-TT and NW-TT. TSN AF uses the PSFP information at TSN bridge configuration time to identify the DS-TT MAC address of the PDU Session as described in clause 5.28.2 and for determination of the traffic pattern information as described in Annex I. The PSFP information can be used at the DS-TT (if supported) and at the NW-TT (if supported) for the purpose of per-stream filtering and policing as defined in IEEE 802.1Q [98] clause 8.6.5.1.

Table 5.28.3.1-2: Standardized bridge management information

Bridge management information	Supported operations by TSN AF (see NOTE 1)	Reference
Information for 5GS Bridge		
Bridge Address	R	
Bridge Name	R	
Bridge ID	R	
Topology of 5GS Bridge		
Chassis ID subtype and Chassis ID of the 5GS Bridge	R	IEEE 802.1AB [97]
Traffic forwarding information		
Static Filtering Entry (NOTE 3)	RW	IEEE 802.1Q [98] clause 8.8.1
General Neighbor discovery configuration (NOTE 2)		
adminStatus	RW	IEEE 802.1AB [97] clause 9.2.5.1
lldpV2LocChassisIdSubtype	RW	IEEE 802.1AB [97] Table 11-2
lldpV2LocChassisId	RW	IEEE 802.1AB [97] Table 11-2
lldpV2MessageTxInterval	RW	IEEE 802.1AB [97] Table 11-2
lldpV2MessageTxHoldMultiplier	RW	IEEE 802.1AB [97] Table 11-2
DS-TT port neighbor discovery configuration for DS-TT ports (NOTE 4)		
>DS-TT port neighbor discovery configuration for each DS-TT port		
>> DS-TT port number	RW	
>> lldpV2LocPortIdSubtype	RW	IEEE 802.1AB [97] Table 11-2
>> lldpV2LocPortId	RW	IEEE 802.1AB [97] Table 11-2
Discovered neighbor information for DS-TT ports (NOTE 4)		
>Discovered neighbor information for each DS-TT port (NOTE 4)		
>> DS-TT port number	R	
>> lldpV2RemChassisIdSubtype	R	IEEE 802.1AB [97] Table 11-2
>> lldpV2RemChassisId	R	IEEE 802.1AB [97] Table 11-2
>> lldpV2RemPortIdSubtype	R	IEEE 802.1AB [97] Table 11-2
>> lldpV2RemPortId	R	IEEE 802.1AB [97] Table 11-2
>> TTL	R	IEEE 802.1AB [97] clause 8.5.4.1
Stream Parameters		
Maximum number of filters, which defines the maximum number of streams that the bridge can handle	R	IEEE 802.1Q [98]
Maximum number of gates, which can be equal or less than the maximum number of filters	R	IEEE 802.1Q [98]
Maximum number of meters (optional) if measurements are required	R	IEEE 802.1Q [98]
Maximum length of the PSFPAdminControlList parameter that can be handled		IEEE 802.1Q [98]

NOTE 1: R = Read only access; RW = Read/Write access.
NOTE 2: General neighbor discovery information is included only when NW-TT performs neighbor discovery on behalf of DS-TT.
NOTE 3: If the Static Filtering Entry information is present, NW-TT uses Static Filtering Entry information to determine the NW-TT egress port for forwarding UL TSC traffic. If the Static Filtering Entry information is not present, then the forwarding information as in clause 5.8.2.5.3 applies.
NOTE 4: DS-TT discovery configuration and DS-TT discovery information are used only when DS-TT does not support LLDP and NW-TT performs neighbor discovery on behalf of DS-TT. These IEs are deliverered via the procedures for the PDU session for the DS-TT port, while the other IEs of the table are deliverered via the procedures for any of the PDU sessions of the 5GS TSN bridge.

Exchange of port and bridge management information between TSN AF and NW-TT or DS-TT allows TSN AF to:

1) retrieve port management information for a DS-TT or NW-TT Ethernet port or bridge management information for a 5GS TSN bridge;

2) send port management information for a DS-TT or NW-TT Ethernet port or bridge management information for a 5GS TSN bridge;

3) subscribe to and receive notifications if specific port management information for a DS-TT or NW-TT Ethernet port changes or bridge management information changes.

Exchange of port management information between TSN AF and NW-TT or DS-TT is initiated by DS-TT or NW-TT to:

- notify TSN AF if port management information has changed that TSN AF has subscribed for.

Exchange of bridge management information between TSN AF and NW-TT is initiated by NW-TT to:

- notify TSN AF if bridge management information has changed that TSN AF has subscribed for.

Exchange of port management information is initiated by DS-TT to:

- provide port management capabilities, i.e. provide information indicating which standardized and deployment-specific port management information is supported by DS-TT.

TSN AF indicates inside the Port Management Information Container or Bridge Management Information Container whether it wants to retrieve or send port or bridge management information or intends to (un-)subscribe for notifications.

5.28.3.2 Transfer of port or bridge management information

Port management information is transferred transparently via 5GS between TSN AF and DS-TT or NW-TT, respectively, inside a Port Management Information Container (PMIC). Bridge management information is transferred transparently via 5GS between TSN AF and NW-TT inside a Bridge Management Information Container (BMIC). The transfer of port or bridge management information is as follows:

- To convey port management information from DS-TT or NW-TT to TSN AF:

  - DS-TT provides a PMIC and the DS-TT port MAC address to the UE, which includes the PMIC as an optional Information Element of an N1 SM container and triggers the UE requested PDU Session Establishment procedure or PDU Session Modification procedure to forward the PMIC to the SMF. SMF forwards the PMIC and the port number of the related DS-TT Ethernet port to TSN AF as described in TS 23.502 [3] clause 4.3.3.2;

  - NW-TT provides PMIC(s) and/or BMIC to the UPF, which triggers the N4 Session Level Reporting Procedure to forward the PMIC(s) and/or BMIC to SMF. SMF in turn forwards the PMIC(s) and the port number(s) of the related NW-TT Ethernet port(s), or the BMIC, to TSN AF as described in TS 23.502 [3] clause 4.16.5.1.

NOTE: There has to be at least one established PDU session for DS-TT port before the UPF can report PMIC/BMIC information towards the AF.

- To convey port management information from TSN AF to DS-TT:
  - TSN AF provides a PMIC, MAC address reported for a PDU Session (i.e. MAC address of the DS-TT port related to the PDU session) and the port number of the Ethernet port to manage to the PCF by using the AF Session level Procedure, which forwards the information to SMF based on the MAC address using the PCF initiated SM Policy Association Modification procedure as described in TS 23.502 [3] clause 4.16.5.2. SMF determines that the port number relates to a DS-TT Ethernet port and based on this forwards the PMIC to DS-TT using the network requested PDU Session Modification procedure as described in TS 23.502 [3] clause 4.3.3.2.

- To convey port or bridge management information from TSN AF to NW-TT:
  - TSN AF selects a PCF-AF session corresponding to any of the DS-TT MAC addresses for the related PDU sessions of this 5G TSN bridge and provides a PMIC(s) and the related NW-TT port number(s) and/or BMIC to the PCF. The PCF uses the PCF initiated SM Policy Association Modification procedure to forward the information received from TSN AF to SMF as described in TS 23.502 [3] clause 4.16.5.2. SMF determines that the included information needs to be delivered to the NW-TT either by determining that the port number(s) relate(s) to a NW-TT Ethernet port(s) or based on the presence of BMIC, and forwards the container(s) and/or related port number(s) to NW-TT using the N4 Session Modification procedure described in TS 23.502 [3] clause 4.4.1.3.

5.28.3.3 VLAN Configuration Information

The CNC obtains the 5GS bridge VLAN configuration from TSN AF as per IEEE 802.1Q [98] clause 12.10.1.1. The TSN AF and UPF/NW-TT are pre-configured with same 5GS bridge VLAN configuration.

NOTE: In this Release, the VLAN Configuration Information are pre-configured at the TSN AF and the NW-TT and is not exchanged between the TSN AF and the UPF/NW-TT.

5.28.4 QoS mapping tables

The mapping tables between the traffic class and 5GS QoS Profile is provisioned and further used to find suitable 5GS QoS profile to transfer TSN traffic over the PDU Session. QoS mapping procedures are performed in two phases: (1) QoS capability report phase as described in clause 5.28.1, and (2) QoS configuration phase as in clause 5.28.2

(1) The TSN AF shall be pre-configured (e.g. via OAM) with a mapping table. The mapping table contains TSN traffic classes, pre-configured bridge delays (i.e. the preconfigured delay between UE and UPF/NW-TT) and priority levels. Once the PDU session has been setup and after retrieving the information related to UE-DS-TT residence time, the TSN AF deduces the port pair(s) consisting of one NW-TT port and one DS-TT port and determines the bridge delay per port pair per traffic class based on the pre-configured bridge delay and the UE-DS-TT residence time. The TSN AF updates bridge delays per port pair and traffic class and reports the bridge delays and other relevant TSN information such as the Traffic Class Table for every port, according to the IEEE 802.1Q [98] and IEEE 802.1Qcc [95] to the CNC.

(2) CNC distributes the TSN QoS requirements and TSN scheduling parameters to 5GS Bridge via TSN AF.

The PCF mapping table provides a mapping from TSN QoS information (see TS 23.503 [45], clauses 6.2.1.2 and 6.1.3.23) to 5GS QoS profile. Based on trigger from TSN AF, the PCF may trigger PDU session modification procedure to establish a new 5G QoS Flow or use the pre-configured 5QI for 5G QoS Flow for the requested traffic class according to the selected QoS policies and the TSN AF traffic requirements.

Figure 5.28.4-1 illustrates the functional distribution of the mapping tables.

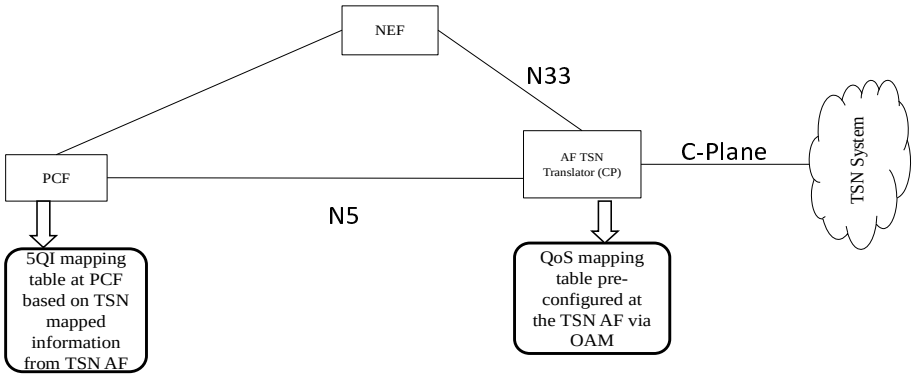


Figure 5.28.4-1: QoS Mapping Function distribution between PCF and TSN AF

The minimum set of TSN QoS-related parameters that are relevant for mapping the TSN QoS requirements are used by the TSN AF: traffic classes and their priorities per port, TSC Burst Size of TSN streams, 5GS bridge delays per port pair and traffic class (independentDelayMax, independentDelayMin, dependentDelayMax, dependentDelayMin), propagation delay per port (txPropagationDelay) and UE-DS-TT residence time.

Once the CNC has received the necessary information, it proceeds to calculate scheduling and paths. The configuration information is then set in the bridge as described in clauses 5.28.2 and 5.28.3. The most relevant information received is the PSFP information and the scheduling for every traffic class and port of the bridge. At this point, it is possible to retrieve the TSN QoS requirements by identifying the traffic class of the port. The traffic class to TSN QoS and delay requirement mapping can be performed using the QoS mapping table in the TSN AF as specified in TS 23.503 [45]. Subsequently in the PCF, the 5G QoS Flow can be configured by selecting a 5QI as specified in TS 23.503 [45]. This feedback approach uses the reported information to the CNC and the feedback of the configuration information coming from the CNC to perform the mapping and configuration in the 5GS.

If the Maximum Burst Size of the aggregated TSC streams in the traffic class is provided by CNC via TSN AF to PCF, PCF can derive the required MDBV taking the Maximum Burst Size as input. If the default MDBV associated with a standardized 5QI or a pre-configured 5QI in the QoS mapping table cannot satisfy the aggregated TSC Burst Size, the PCF provides the derived MDBV in the PCC rule and then the SMF performs QoS Flow binding as specified in clause 6.1.3.2.4 of TS 23.503 [45].

Maximum Flow Bit Rate is calculated over PSFPAdminCycleTime as described in Annex I and provided by the TSN AF to the PCF, while GBR is calculated over an Averaging Window for the 5QI by the PCF. The Maximum Flow Bit Rate is adjusted according to Averaging Window associated with a pre-configured 5QI in the QoS mapping table or another selected 5QI (as specified in TS 23.503 [45]) to obtain GBR of the 5GS QoS profile. GBR is then used by SMF to calculate the GFBR per QoS flow. QoS mapping table in the PCF between TSN parameters and 5GS parameters should match the delay, aggregated TSC burst size and priority, while preserving the priorities in the 5GS. An operator enabling TSN services via 5GS can choose up to eight traffic classes to be mapped to 5GS QoS profiles.

Once the 5QIs to be used for TSN streams are identified by the PCF as specified in TS 23.503 [45], then it is possible to enumerate as many bridge port traffic classes as the number of selected 5QIs.

5.29 Support for 5G LAN-type service

5.29.1 General

The service requirements for 5G LAN-type service are specified in TS 22.261 [2].

A 5G Virtual Network (VN) group consists of a set of UEs using private communication for 5G LAN-type services.

5.29.2 5G VN group management

5G System supports management of 5G VN Group identification and membership (i.e. definition of 5G VN group identifiers and membership) and 5G VN Group data (i.e. definition of 5G VN group data). The 5G VN Group management can be configured by a network administrator or can be managed dynamically by AF.

A 5G VN group is characterized by the following:

- 5G VN group identities: External Group ID and Internal Group ID are used to identify the 5G VN group.
- 5G VN group membership: The 5G VN group members are uniquely identified by GPSI. The group as described in clause 5.2.3.3.1 of TS 23.502 [3] is applicable to 5G LAN-type services.
- 5G VN group data. The 5G VN group data may include the following parameters: PDU session type, DNN, S-NSSAI and Application descriptor, Information related with secondary authentication / authorization (e.g. to enable IP address assignment by the DN-AAA).

  The Information related with secondary authentication / authorization corresponds to the procedures described in clause 5.6.6; it allows e.g. the AF to provide DN-AAA server addressing information and possibly to request the SMF to get the UE IP address from the DN-AAA server.

In order to support dynamic management of 5G VN Group identification and membership, the NEF exposes a set of services to manage (e.g. add/delete/modify) 5G VN groups and 5G VN members. The NEF also exposes services to dynamically manage 5G VN group data.

A 5G VN group is identified by the AF using External Group ID. The NEF provides the External Group ID to UDM. The UDM maps the External Group ID to Internal Group ID. For a newly created 5G VN Group, an Internal Group ID is allocated by the UDM.

The NEF can retrieve the Internal Group ID from UDM via Nudm_SDM_Get service operation (External Group ID, Group Identifier translation).

An External Group ID for a 5G VN group corresponds to a unique set of 5G VN group data parameters.

The 5G VN group configuration is either provided by OA&M or provided by an AF to the NEF.

When configuration is provided by an AF, the procedures described in TS 23.502 [3] clause 4.15.6.2 apply for storing the 5G VN group identifiers, group membership information and group data in the UDR, as follows:

- The NEF provides the External Group ID, 5G VN group membership information and 5G VN group data to the UDM.
- The UDM updates the Internal Group ID-list of the corresponding UE's subscription data in UDR, if needed.
- The UDM updates the Group Identifier translation in the Group Subscription data with the Internal Group ID, External Group ID and list of group members, if needed.
- The UDM stores/updates the 5G VN group data (PDU session type, DNN and S-NSSAI, Application descriptor, Information related with secondary authentication / authorization) in UDR.

NOTE 1: It is assumed that all members of a 5G VN group belong to the same UDM Group ID. The NEF can select a UDM instance supporting the UDM Group ID of any of the member GPSIs of the 5G VN group.

NOTE 2: Shared data mechanisms as defined in TS 29.503 [122] can be used to support large 5G VN groups.

If a UE is member of a 5G VN Group, UDM retrieves UE subscription data and corresponding 5G VN group data from UDR, and provides the AMF and SMF with UE subscription data with 5G VN group data included.

The PCF generates URSP rules based on 5G VN group data. The PCF retrieves 5G VN group data from UDR. The PCF(s) that have subscribed to modifications of 5G VN group data receive(s) a Nudr_DM_Notify notification of data change from the UDR. The PCF receives at the UE Policy association establishment the Internal Group ID from the AMF, so that PCF identifies the 5G VN group data that needs to be used to generate URSP rules to the UE.

An AF may update the UE Identities of the 5G VN group at any time after the initial provisioning.

In this Release of the specification, only a 1:1 mapping between DNN and 5G VN group is supported.

The PCF delivers 5G VN group configuration information (DNN, S-NSSAI, PDU session type) to the UE for each GPSI that belongs to a 5G-LAN group. The 5G VN group configuration information is delivered in the URSP from the PCF to the UE using the UE Configuration Update procedure for transparent UE Policy delivery as described in TS 23.502 [3] clause 4.2.4.3 and TS 23.503 [45] clause 6.1.2.2.

5.29.3 PDU Session management

Session management as defined for 5GS in clause 5.6 is applicable to 5GLAN-type services with the following clarification and enhancement:

- A UE gets access to 5G LAN-type services via a PDU Session of IP PDU Session type or Ethernet PDU Session type.
- A PDU Session provides access to one and only one 5G VN group
- A dedicated SMF is responsible for all the PDU Sessions for communication of a certain 5G VN group. SMF selection is described in clause 6.3.2.

NOTE 1: The network is configured so that the same SMF is always selected for a certain 5G VN group.

NOTE 2: Having a dedicated SMF serving a 5G VN does not contradict that redundancy solutions can be used to achieve high availability.

- A DNN and a S-NSSAI are associated with a 5G VN group.
- The UE provides a DNN associated with the 5G VN group to access the 5G LAN-type services for that 5G VN, using the PDU Session Establishment procedure described in TS 23.502 [3], clause 4.3.2.
- During establishment of the PDU Session, secondary authentication as described in clause 5.6.6 and in TS 23.502 [3], clause 4.3.2.3, may be performed in order to authenticate and authorize the UE for accessing the DNN associated with the 5G VN group. Authentication and authorization for a DNN using secondary authentication implies authentication and authorization for the associated 5G VN group. There is no 5G VN group specific authentication or authorization defined.
- The SM level subscription data for a DNN and S-NSSAI available in UDM, as described in clause 5.6.1, applies to the DNN and S-NSSAI associated to a 5G VN group.
- Session management related policy control for a DNN and S-NSSAI as described in TS 23.502 [3], is applicable to the DNN and S-NSSAI associated to a 5G VN group. This includes also usage of URSP, for the UE to determine how to route outgoing traffic to a PDU Session for the DNN and S-NSSAI associated to a 5G VN group.
- Session and service continuity SSC mode 1, SSC mode 2, and SSC mode 3 as described in clause 5.6.9 are applicable to N6-based traffic forwarding of 5G VN communication within the associated 5G VN group.
- A PDU Session provides unicast, broadcast and multicast communication for the DNN and S-NSSAI associated to a 5G VN group. The PSA UPF determines whether the communication is for unicast, broadcast or multicast based on the destination address of the received data, and performs unicast, broadcast or multicast communication handling.
- During the PDU Session Establishment procedure, the SMF retrieves SM subscription data related to 5GLAN type service from the UDM as part of the UE subscription data for the DNN.
- In order to realize N19 traffic routing, the SMF correlates PDU sessions established to the same 5G VN group and uses this to configure the UPF with the group level N4-session including packet detection and forwarding rules for N19 tunnelling forwarding.

5.29.4 User Plane handling

User Plane management as defined for 5GS in clause 5.8 is applicable to 5G LAN-type services with the following clarifications:

- There are three types of traffic forwarding methods allowed for 5G VN communication:

- N6-based, where the UL/DL traffic for the 5G VN communication is forwarded to/from the DN;
- N19-based, where the UL/DL traffic for the 5G VN group communication is forwarded between PSA UPFs of different PDU sessions via N19. N19 is based on a shared User Plane tunnel connecting PSA UPFs of a single 5G VN group.
- Local switch, where traffic is locally forwarded by a single UPF if this UPF is the common PSA UPF of different PDU Sessions for the same 5G VN group.

- The SMF handles the user plane paths of the 5G VN group, including:
  - The SMF may prefer to select a single PSA UPF for as many PDU sessions (targeting the same 5G VN group) as possible, in order to implement local switch on the UPF.
  - (if needed) Establishing N19 tunnels between PSA UPFs to support N19-based traffic forwarding.
- For Ethernet PDU Session, the SMF may instruct the UPF(s) to classify frames based on VLAN tags, and to add and remove VLAN tags, on frames received and sent on N6, as described in clause 5.6.10.2.

NOTE 1: For handling VLAN tags for traffic on N6, TSP ID could also be used as described in clause 6.2.2.6 of TS 23.503 [45].

Further description on User Plane management for 5G VN groups is available in clause 5.8.2.13.

When N6-based traffic forwarding is expected, after creation of a 5G VN group the AF can influence the traffic routing for all the members of the 5G VN group, by providing information identifying the traffic, DNAI(s) suitable for selection and an optional indication of traffic correlation together with a 5G VN External Group ID identifying the 5G VN group in an AF request sent to the PCF, as described in clause 5.6.7. If the optional indication of traffic correlation is provided, it means the PDU sessions of the 5G VN group member UEs should be correlated by a common DNAI in the user plane for the traffic. The PCF transforms the AF request into policies that apply to PDU Sessions of the 5G VN group and sends the policies to the SMF. According to the policies, the SMF (re)selects DNAI(s) for the PDU Sessions and configures their UP paths to route the traffic to the selected DNAI(s). If the policies include the traffic correlation indication, the SMF (re)selects a common DNAI for the PDU Sessions so that the traffic of the 5G VN group is routed to the common DNAI.

NOTE 2: When receiving a new PDU session establishment request for a 5G VN group, to avoid unnecessary N19 tunnels between UPFs, SMF can check previously selected UPFs for the same 5G VN group, and decide whether a previously selected UPF could serve the requested PDU session.

NOTE 3: N19 tunnel(s) can be established between a new UPF and other UPF(s) that belongs to a 5G VN group when the new UPF is selected for the 5G VN group during PDU session establishment. The N19 tunnel(s) to a UPF can be released during or after PDU session release when there is no more PDU sessions for a 5G VN group in that UPF. Establishment or release of the N19 tunnels at the UPF is performed within a group-level N4 Session.

5.30 Support for non-public networks

5.30.1 General

A Non-Public Network (NPN) is a 5GS deployed for non-public use, see TS 22.261 [2]. An NPN is either:

- a Stand-alone Non-Public Network (SNPN), i.e. operated by an NPN operator and not relying on network functions provided by a PLMN, or
- a Public Network Integrated NPN (PNI-NPN), i.e. a non-public network deployed with the support of a PLMN.

NOTE: An SNPN and a PLMN can share NG-RAN as described in clause 5.18.

SNPN 5GS deployments are based on the architecture depicted in clause 4.2.3, the architecture for 5GC with untrusted non-3GPP access (Figure 4.2.8.2.1-1) for access to SNPN services via a PLMN (and vice versa) and the additional functionality covered in clause 5.30.2. In this Release, direct access to SNPN is specified for 3GPP access only.

Interworking with EPS is not supported for SNPN. Also, emergency services are not supported for SNPN. Furthermore, roaming is not supported for SNPN, e.g. roaming between SNPNs. Handover between SNPNs, between SNPN and PLMN or PNI NPN are not supported.

Public Network Integrated NPNs are described in clause 5.30.3.

5.30.2 Stand-alone non-public networks

5.30.2.1 Identifiers

The combination of a PLMN ID and Network identifier (NID) identifies an SNPN.

NOTE 1: The PLMN ID used for SNPNs is not required to be unique. PLMN IDs reserved for use by private networks can be used for non-public networks, e.g. based on mobile country code (MCC) 999 as assigned by ITU [78]). Alternatively, a PLMN operator can use its own PLMN IDs for SNPN(s) along with NID(s), but registration in a PLMN and mobility between a PLMN and an SNPN are not supported using an SNPN subscription given that the SNPNs are not relying on network functions provided by the PLMN.

The NID shall support two assignment models:

- Self-assignment: NIDs are chosen individually by SNPNs at deployment time (and may therefore not be unique) but use a different numbering space than the coordinated assignment NIDs as defined in TS 23.003 [19].
- Coordinated assignment: NIDs are assigned using one of the following two options:
  1. The NID is assigned such that it is globally unique independent of the PLMN ID used; or
  2. The NID is assigned such that the combination of the NID and the PLMN ID is globally unique.

NOTE 2: Which legal entities manage the number space is beyond the scope of this specification.

An optional human-readable network name helps to identify an SNPN during manual SNPN selection.

5.30.2.2 Broadcast system information

NG-RAN nodes which provide access to SNPNs broadcast the following information:

- One or multiple PLMN IDs
- List of NIDs per PLMN ID identifying the non-public networks NG-RAN provides access to

NOTE 1: It is assumed that an NG-RAN node supports broadcasting a total of twelve NIDs. Further details are defined in TS 38.331 [28].

NOTE°2: The presence of a list of NIDs for a PLMN ID indicates that the related PLMN ID and NIDs identify SNPNs.

- Optionally a human-readable network name per NID.

NOTE 3: The human-readable network name per NID is only used for manual SNPN selection. The mechanism how human-readable network name is provided (i.e. whether it is broadcasted or unicasted) to the UE is specified in TS 38.331 [28].

- Optionally information, as described in TS 38.300 [27], TS 38.331 [28] and in TS 38.304 [50], to prevent UEs not supporting SNPNs from accessing the cell, e.g. if the cell only provides access to non-public networks.

5.30.2.3 UE configuration and subscription aspects

An SNPN-enabled UE is configured with subscriber identifier (SUPI) and credentials for each subscribed SNPN identified by the combination of PLMN ID and NID.

A subscriber of an SNPN is either:

- identified by a SUPI containing a network-specific identifier that takes the form of a Network Access Identifier (NAI) using the NAI RFC 7542 [20] based user identification as defined in TS 23.003 [19] clause 28.7.2. The realm part of the NAI may include the NID of the SNPN; or

- identified by a SUPI containing an IMSI.

An SNPN-enabled UE supports the SNPN access mode. When the UE is set to operate in SNPN access mode the UE only selects and registers with SNPNs over Uu as described in clause 5.30.2.4.

Emergency services are not supported in SNPN access mode.

NOTE 1: Voice support with emergency services in SNPN access mode is not specified in this release.

If a UE is not set to operate in SNPN access mode, even if it is SNPN-enabled, the UE does not select and register with SNPNs. A UE not set to operate in SNPN access mode performs PLMN selection procedures as defined in clause 4.4 of TS 23.122 [17]. For a UE capable of simultaneously connecting to an SNPN and a PLMN, the setting for operation in SNPN access mode is applied only to the Uu interface for connection to the SNPN. Annex D.4 provides more details.

NOTE 2: Details of activation and deactivation of SNPN access mode are up to UE implementation.

5.30.2.4 Network selection in SNPN access mode

When a UE is set to operate in SNPN access mode the UE does not perform normal PLMN selection procedures as defined in clause 4.4 of TS 23.122 [17].

UEs operating in SNPN access mode read the available PLMN IDs and list of available NIDs from the broadcast system information and take them into account during network selection.

For automatic network selection, the UE selects and attempts to register with the available SNPN identified by a PLMN ID and NID for which the UE has SUPI and credentials. If multiple SNPNs are available that the UE has respective SUPI and credentials for, then how the UE selects an SNPN is based on UE implementation.

For manual network selection UEs operating in SNPN access mode provide to the user the list of SNPNs (each is identified by a PLMN ID and NID) and related human-readable names (if available) of the available SNPNs the UE has respective SUPI and credentials for.

NOTE: The details of SNPN selection is defined in TS 23.122 [17].

When a UE performs Initial Registration to an SNPN, the UE shall indicate the selected NID and the corresponding PLMN ID to NG-RAN. NG-RAN shall inform the AMF of the selected PLMN ID and NID.

5.30.2.5 Network access control

If a UE performs the registration or service request procedure in an SNPN identified by a PLMN ID and a self-assigned NID and there is no subscription for the UE, then the AMF shall reject the UE with an appropriate cause code to temporarily prevent the UE from automatically selecting and registering with the same SNPN.

If a UE performs the registration or service request procedure in an SNPN identified by a PLMN ID and a coordinated assigned NID and there is no subscription for the UE, then the AMF shall reject the UE with an appropriate cause code to permanently prevent the UE from automatically selecting and registering with the same SNPN.

NOTE: The details of rejection and cause codes is defined in TS 24.501 [47].

In order to prevent access to SNPNs for authorized UE(s) in the case of network congestion/overload, Unified Access Control information is configured per SNPN (i.e. as part of the subscription information that the UE has for a given SNPN) and provided to the UE as described in TS 24.501 [47].

5.30.2.6 Cell (re-)selection in SNPN access mode

UEs operating in SNPN access mode only select cells and networks broadcasting both PLMN ID and NID of the selected SNPN.

NOTE: Further details on the NR idle and inactive mode procedures for SNPN cell selection is defined in TS 38.331 [28] and in TS 38.304 [50].

5.30.2.7 Access to PLMN services via stand-alone non-public networks

To access PLMN services, a UE in SNPN access mode that has successfully registered with an SNPN may perform another registration via the SNPN User Plane with a PLMN (using the credentials of that PLMN) following the same architectural principles as specified in clause 4.2.8 (including the optional support for PDU Session continuity between PLMN and SNPN using the Handover of a PDU Session procedures in TS 23.502 [3] clauses 4.9.2.1 and 4.9.2.2) and the SNPN taking the role of "Untrusted non-3GPP access". Annex D, clause D.3 provides additional details.

NOTE: QoS differentiation in the SNPN can be provided on per-IPsec Child Security Association basis by using the UE or network requested PDU Session Modification procedure described in TS 23.502 [3] clause 4.3.3.2. In the PLMN, N3IWF determines the IPsec child SAs as defined in TS 23.502 [3] clause 4.12. The N3IWF is preconfigured by PLMN to allocate different IPsec child SAs for QoS Flows with different QoS profiles.

To support QoS differentiation in the SNPN with network-initiated QoS, the mapping rules between the SNPN and the PLMN are assumed to be governed by an SLA including: 1) mapping between the DSCP markings for the IPsec child SAs on NWu and the corresponding QoS, which is the QoS requirement of the PLMN and is expected to be provided by the SNPN, and 2) N3IWF IP address(es) in the PLMN. The non-alteration of the DSCP field on NWu is also assumed to be governed by an SLA and by transport-level arrangements that are outside of 3GPP scope. The packet detection filters in the SNPN can be based on the N3IWF IP address and the DSCP markings on NWu.

To support QoS differentiation in the SNPN with UE-requested QoS, the UE can request for an IPsec SA the same 5QI from the SNPN as the 5QI provided by the PLMN. It is assumed that UE-requested QoS is used only when the 5QIs used by the PLMN are from the range of standardized 5QIs. The packet filters in the requested QoS rule can be based on the N3IWF IP address and the SPI associated with the IPsec SA.

5.30.2.8 Access to stand-alone non-public network services via PLMN

To access SNPN services, a UE that has successfully registered with a PLMN over 3GPP access may perform another registration via the PLMN User Plane with an SNPN (using the credentials of that SNPN) following the same architectural principles as specified in clause 4.2.8 (including the optional support for PDU Session continuity between PLMN and SNPN using the Handover of a PDU Session procedures in TS 23.502 [3] clauses 4.9.2.1 and 4.9.2.2) and the PLMN taking the role of "Untrusted non-3GPP access" of the SNPN, i.e. using the procedures for Untrusted non-3GPP access in clause 4.12.2 of TS 23.502 [3]. Annex D, clause D.3 provides additional details. The case where UE that has successfully registered with a PLMN over non-3GPP access to access SNPN services is not specified in this Release.

NOTE: QoS differentiation in the PLMN can be provided on per-IPsec Child Security Association basis by using the UE or network requested PDU Session Modification procedure described in TS 23.502 [3] clause 4.3.3.2. In the SNPN, N3IWF determines the IPsec child SAs as defined in TS 23.502 [3] clause 4.12. The N3IWF is preconfigured by SNPN to allocate different IPsec child SAs for QoS Flows with different QoS profiles.

To support QoS differentiation in the PLMN with network-initiated QoS, the mapping rules between the PLMN and the SNPN are assumed to be governed by an SLA including: 1) mapping between the DSCP markings for the IPsec child SAs on NWu and the corresponding QoS, which is the QoS requirement of the SNPN and is expected to be provided by the PLMN, and 2) N3IWF IP address(es) in the SNPN. The non-alteration of the DSCP field on NWu is also assumed to be governed by an SLA and by transport-level arrangements that are outside of 3GPP scope. The packet detection filters in the PLMN can be based on the N3IWF IP address and the DSCP markings on NWu.

To support QoS differentiation in the PLMN with UE-requested QoS, the UE can request for an IPsec SA the same 5QI from the PLMN as the 5QI provided by the SNPN. It is assumed that UE-requested QoS is used only when the 5QIs used by the SNPN are from the range of standardized 5QIs. The packet filters in the requested QoS rule can be based on the N3IWF IP address and the SPI associated with the IPsec SA.

5.30.3 Public Network Integrated NPN

5.30.3.1 General

Public Network Integrated NPNs are NPNs made available via PLMNs e.g. by means of dedicated DNNs, or by one (or more) Network Slice instances allocated for the NPN. The existing network slicing functionalities apply as described in clause 5.15. When a PNI-NPN is made available via a PLMN, then the UE shall have a subscription for the PLMN in order to access PNI-NPN.

NOTE 1: Annex D provides additional consideration to consider when supporting Non-Public Network as a Network Slice of a PLMN.

As network slicing does not enable the possibility to prevent UEs from trying to access the network in areas where the UE is not allowed to use the Network Slice allocated for the NPN, Closed Access Groups may optionally be used to apply access control.

A Closed Access Group identifies a group of subscribers who are permitted to access one or more CAG cells associated to the CAG.

CAG is used for the PNI-NPNs to prevent UE(s), which are not allowed to access the NPN via the associated cell(s), from automatically selecting and accessing the associated CAG cell(s).

NOTE 2: CAG is used for access control e.g. authorization at cell selection and configured in the subscription as part of the Mobility Restrictions i.e. independent from any S-NSSAI. CAG is not used as input to AMF selection nor Network Slice selection. If NPN isolation is desired, operator can better support NPN isolation by deploying network slicing for PNI-NPN, configuring dedicated S-NSSAI(s) for the given NPN as specified in Annex D, clause D.2 and restricting NPN's UE subscriptions to these dedicated S-NSSAI(s).

The following clauses describes the functionality needed for supporting CAGs.

5.30.3.2 Identifiers

The following is required for identification:

- A CAG is identified by a CAG Identifier which is unique within the scope of a PLMN ID;

- A CAG cell broadcasts one or multiple CAG Identifiers per PLMN;

NOTE 1: It is assumed that a cell supports broadcasting a total of twelve CAG Identifiers. Further details are defined in TS 38.331 [28].

- A CAG cell may in addition broadcast a human-readable network name per CAG Identifier:

NOTE 2: The human-readable network name per CAG Identifier is only used for presentation to user when user requests a manual CAG selection.

5.30.3.3 UE configuration, subscription aspects and storage

To use CAG, the UE, that supports CAG as indicated as part of the UE 5GMM Core Network Capability, may be pre-configured or (re)configured with the following CAG information, included in the subscription as part of the Mobility Restrictions:

- an Allowed CAG list i.e. a list of CAG Identifiers the UE is allowed to access; and

- optionally, a CAG-only indication whether the UE is only allowed to access 5GS via CAG cells (see TS 38.304 [50] for how the UE identifies whether a cell is a CAG cell);

The HPLMN may configure or re-configure a UE with the above CAG information using the UE Configuration Update procedure for access and mobility management related parameters described in TS 23.502 [3] in clause 4.2.4.2.,

The above CAG information is provided by the HPLMN on a per PLMN basis. In a PLMN the UE shall only consider the CAG information provided for this PLMN.

When the subscribed CAG information changes, UDM sets a CAG information Subscription Change Indication and sends it to the AMF. The AMF shall provide the UE with the CAG information when the UDM indicates that the CAG information within the Access and Mobility Subscription data has been changed. When AMF receives the indication from the UDM that the CAG information within the Access and Mobility Subscription has changed, the AMF uses the CAG information received from the UDM to update the UE. Once the AMF updates the UE and obtains an acknowledgment from the UE, the AMF informs the UDM that the update was successful and the UDM clears the CAG information Subscription Change Indication flag.

The AMF may update the UE using either the UE Configuration Update procedure after registration procedure is completed, or by including the new CAG information in the Registration Accept or in the Registration Reject.

When the UE is roaming and the Serving PLMN provides CAG information, the UE shall update only the CAG information provided for the Serving PLMN while the stored CAG information for other PLMNs are not updated. When the UE is not roaming and the HPLMN provides CAG information, the UE shall update the CAG information stored in the UE with the received CAG information for all the PLMNs.

The UE shall store the latest available CAG information for every PLMN for which it is provided and keep it stored when the UE is de-registered or switched off, as described in TS 24.501 [47].

NOTE: CAG information has no implication on whether and how the UE accesses 5GS over non-3GPP access.

5.30.3.4 Network and cell (re-)selection, and access control

The following is assumed for network and cell selection, and access control:

- The CAG cell shall broadcast information such that only UEs supporting CAG are accessing the cell (see TS 38.300 [27], TS 38.304 [50]);

NOTE 1: The above also implies that cells are either CAG cells or normal PLMN cells.

- In order to prevent access to NPNs for authorized UE(s) in the case of network congestion/overload, existing mechanisms defined for Control Plane load control, congestion and overload control in clause 5.19 can be used, as well as the access control and barring functionality described in clause 5.2.5, or Unified Access Control using the access categories as defined in TS 24.501 [47] can be used.

- For aspects of automatic and manual network selection in relation to CAG, see TS 23.122 [17];

- For aspects related to cell (re-)selection, see TS 38.304 [50];

- The Mobility Restrictions shall be able to restrict the UE's mobility according to the Allowed CAG list (if configured in the subscription) and include an indication whether the UE is only allowed to access CAG cells (if configured in the subscription);

- During transition from CM-IDLE to CM-CONNECTED, if the UE is accessing the 5GS via a CAG cell:

  - The AMF shall verify whether UE access is allowed by Mobility Restrictions:

NOTE 2: It is assumed that the AMF is made aware of the supported CAG Identifier(s) of the CAG cell by the NG-RAN.

    - If at least one of the CAG Identifier(s) received from the NG-RAN is part of the UE's Allowed CAG list, then the AMF accepts the NAS request;

    - If none of the CAG Identifier(s) received from the NG-RAN are part of the UE's Allowed CAG list, then the AMF rejects the NAS request and the AMF should include CAG information in the NAS reject message. The AMF shall then release the NAS signalling connection for the UE by triggering the AN release procedure; and

    - If the UE is accessing the network via a non-CAG cell and the UE's subscription contains an indication that the UE is only allowed to access CAG cells, then the AMF rejects the NAS request and the AMF should include CAG information in the NAS reject message. The AMF shall then release the NAS signalling connection for the UE by triggering the AN release procedure.

- During transition from RRC Inactive to RRC Connected state:

- When the UE initiates the RRC Resume procedure for RRC Inactive to RRC Connected state transition in a CAG cell, NG-RAN shall reject the RRC Resume request from the UE if none of the CAG Identifiers supported by the CAG cell are part of the UE's Allowed CAG list according to the Mobility Restrictions received from the AMF.

- When the UE initiates the RRC Resume procedure for RRC Inactive to RRC Connected state transition in a non-CAG cell, NG-RAN shall reject the UE's Resume request if the UE is only allowed to access CAG cells according to the Mobility Restrictions received from the AMF.

- During connected mode mobility procedures:

  - Based on the Mobility Restrictions received from the AMF:

    - Source NG-RAN shall not handover the UE to a target NG-RAN node if the target is a CAG cell and none of the CAG Identifiers supported by the CAG cell are part of the UE's Allowed CAG list;

    - Source NG-RAN shall not handover the UE to a non-CAG cell if the UE is only allowed to access CAG cells;

    - If the target cell is a CAG cell, target NG-RAN shall reject the N2 based handover procedure if none of the CAG Identifiers supported by the CAG cell are part of the UE's Allowed CAG list in the Mobility Restriction List;

    - If the target cell is a non-CAG cell, target NG-RAN shall reject the N2 based handover procedure if the UE is only allowed to access CAG cells based on the Mobility Restriction List.

- Update of Mobility Restrictions:

  - When the AMF receives the Nudm_SDM_Notification from the UDM and the AMF determines that the Allowed CAG list or the indication whether the UE is only allowed to access CAG cells have changed;

    - The AMF shall update the Mobility Restrictions in the UE and NG-RAN accordingly; and

    - Upon receiving Mobility Restrictions from AMF, NG-RAN determines if the UE is currently accessing a CAG cell and the CAG Identifier(s) supported by the CAG cell have been removed from the Allowed CAG list or if the UE is currently accessing a non-CAG cell and the indication that the UE is only allowed to access CAG cells has been set in the subscription, then the NG-RAN shall initiate actions for the UE (e.g. a handover or AN release) to ensure that the UE is no longer served by the current cell.

NOTE 3: When the UE is accessing the network for emergency service the conditions for AMF in clause 5.16.4.3 apply.

5.30.3.5 Support of emergency services in CAG cells

Emergency Services are supported in CAG cells, for UEs supporting CAG, whether normally registered or emergency registered as described in clause 5.16.4 and TS 23.502 [3] clause 4.13.4.

A UE may camp on an acceptable CAG cell in limited service state as specified in TS 23.122 [17] and TS 38.304 [50], based on operator policy defined in TS 38.300 [27].

For UEs not supporting CAG, but are emergency registered as described in clause 5.16.4 and TS 23.502 [3] clause 4.13.4, Emergency Services may be supported based on operator policy as defined in TS 38.300 [27].

NOTE: Support for Emergency services requires each cell with a Cell Identity associated with PLMNs or PNI-NPNs to only be connected to AMFs that supports emergency services.

The UE shall select a PLMN (of a CAG cell or non-CAG cell), as described in TS 23.122 [17] and TS 23.167 [18], when initiating emergency services from limited service state.

During handover to a CAG cell, if the UE is not authorized to access the target CAG cell and has emergency services, the target NG-RAN node only accepts the emergency PDU sessions and the target AMF releases the non-emergency PDU connections that were not accepted by the NG-RAN node. Upon completion of handover the UE behave as emergency registered.

5.31 Support for Cellular IoT

5.31.1 General

This clause provides an overview about 5GS optimisations and functionality for support of Cellular Internet-of-Things (Cellular IoT, or CIoT) according to service requirements described in TS 22.261 [2]. Cellular IoT is in earlier 3GPP releases also referred to as Machine Type Communication (MTC) (see TS 23.401 [26], clause 4.3.17). The specific functionality is described in the affected procedures and features of this specification, in TS 23.502 [3], TS 23.503 [45] and other specifications.

In this Release Control Plane CIoT 5GS Optimisations (clause 5.31.4) and User Plane CIoT 5GS Optimisations (clause 5.31.18) are only supported over E-UTRA.

CIoT functionality is provided by the visited and home networks when the networks are configured to support CIoT. It applies to both the non-roaming case and the roaming case and some functionality may be dependent upon the existence of appropriate roaming agreements between the operators.

Some of the CIoT functions are controlled by subscriber data. Other CIoT functions are based on indicators sent by the UE to the network. CIoT functionality is performed by UEs that are configured to support different options as described in clause 5.31.2

Though motivated by scenarios and use cases defined in TS 22.261 [2], the functions added to support CIoT have general applicability and are in no way constrained to any specific scenario, use case or UE types, except where explicitly stated.

In the context of CIoT the term AF denotes an SCS/AS as defined TS 23.682 [36].

5.31.2 Preferred and Supported Network Behaviour

At registration, a UE includes its 5G Preferred Network Behaviour indicating the network behaviour the UE can support and what it would prefer to use.

NOTE: If the UE supports S1-mode then the UE will indicate the supported EPS Network Behaviour Information in the S1 UE network capability IE.

The 5G Preferred Network Behaviour signalled by the UE includes the following information in the 5GMM Capability IE:

- Whether Control Plane CIoT 5GS Optimisation is supported.
- Whether User Plane CIoT 5GS Optimisation is supported.
- Whether N3 data transfer is supported.
- Whether header compression for Control Plane CIoT 5GS Optimisation is supported.

And the following 5G Preferred Network Behaviour in other IEs:

- Whether Control Plane CIoT 5GS Optimisation or User Plane CIoT 5GS Optimisation is preferred.

If N3 data transfer is supported is indicated by the UE, the UE supports data transfer that is not subject to CIoT 5GS Optimisations. If the UE indicates support of User Plane CIoT 5GS Optimisation then it shall also indicate support of N3 data transfer.

The AMF indicates the network behaviour the network accepts in the 5G Supported Network Behaviour information. This indication is per Registered Area. The AMF may indicate one or more of the following:

- Whether Control Plane CIoT 5GS Optimisation is supported.
- Whether User Plane CIoT 5GS Optimisation is supported.
- Whether N3 data transfer is supported.
- Whether header compression for Control Plane CIoT 5GS Optimisation is supported.

If the AMF indicates support of User Plane CIoT 5GS Optimisation then it shall also indicate support of N3 data transfer. If the UE and AMF indicate support for User Plane CIoT 5GS Optimisation, the AMF indicates support of User Plane CIoT 5GS Optimisation support for the UE to NG-RAN.

For NB-IoT UEs that only support Control Plane CIoT 5GS Optimisation, the AMF shall include support for Control Plane CIoT 5GS Optimisation in the Registration Accept message.

A UE that supports the NB-IoT shall always indicate support for Control Plane CIoT 5GS Optimisation.

A UE that supports WB-E-UTRA shall always indicate support for N3 data transfer.

The 5G Preferred Network Behaviour indication from the UE may be used to influence policy decisions that can cause rerouting of the Registration Request from an AMF to another AMF.

5.31.3 Selection, steering and redirection between EPS and 5GS

The UE selects the core network type (EPC or 5GC) based on the broadcast indications for both EPC and 5GC, and the UE's EPC and 5GC Preferred Network Behaviour. Networks that support NB-IoT shall broadcast an indication whether N3 data transfer is supported or not in system information.

When the UE performs the registration procedure it includes its Preferred Network Behaviour (for 5G and EPC) in the Registration Request message and the AMF replies with the 5G Supported Network Behaviour in the Registration Accept message.

If the UE supports any of the CIoT 5GS Optimisations included in 5GC Preferred Network Behaviour, then when the UE performs an Attach or TAU procedure and the UE includes its EPC Preferred Network Behaviour then the UE shall also include its 5GC Preferred Network Behaviour.

In networks that support CIoT features in both EPC and 5GC, the operator may steer UEs from a specific CN type due to operator policy, e.g., due to roaming agreements, Preferred and Supported Network Behaviour, load redistribution, etc. Operator policies in EPC and 5GC are assumed to avoid steering UEs back and forth between EPC and 5GC.

To redirect a UE from 5GC to EPC, when the UE sends a Registration Request, the AMF sends a Registration Reject with an EMM cause value indicating that the UE should not use 5GC. The UE disables N1 mode and re-enables S1 mode, if it was disabled. The UE then performs either an Attach or TAU in EPC as described in clause 5.17.2.

To redirect a UE from EPC to 5GC, when the UE requests an Attach or TAU procedure, the MME sends a reject message with an EMM cause indicating the UE should not use EPC. The UE disables S1 mode and re-enables N1 mode, if it was disabled. The UE then registers with 5GC as described in clause 5.17.2.

When determining whether to redirect the UE, the AMF/MME takes into account the UE support of S1/N1 mode, respectively, and the UE's Preferred Network Behaviour and the Supported Network Behaviour of the network the UE is being redirected towards.

If after redirection the UE cannot find a cell supporting connectivity, the UE may re-enable the disabled N1/S1 mode and then perform Registration, Attach or TAU.

5.31.4 Control Plane CIoT 5GS Optimisation

5.31.4.1 General

The Control Plane CIoT 5GS Optimisation is used to exchange user data between the UE and the SMF as payload of a NAS message in both uplink and downlink directions, avoiding the establishment of a user plane connection for the PDU Session. The UE and the AMF perform integrity protection and ciphering for the user data by using NAS PDU integrity protection and ciphering. For IP and Ethernet data, the UE and the SMF may negotiate and perform header compression.

NOTE: In the context of Control Plane CIoT 5GS Optimisation, established or activated user plane resources/connection refers to radio user plane resources/connection i.e Data Radio Bearer and N3 tunnel.

UE and AMF negotiate support and use of Control Plane CIoT 5GS Optimisation as defined in clause 5.31.2. When the Control Plane CIoT 5GS Optimisation feature is used and the PDU session type is unstructured, the SMF selects either NEF or UPF based on information in the UE's subscription.

If UE and network have negotiated support and use of Control Plane CIoT 5GS Optimisation then the following paragraphs of this clause apply.

During the PDU Session Establishment procedure the AMF indicates to the SMF that Control Plane CIoT 5GS Optimisation is available for data transmission.

During the PDU Session Establishment procedure the AMF also determines based on Preferred and Supported Network Behaviour (see clause 5.31.2), subscription data, other already established PDU Sessions and local policy whether a new PDU session shall only use the Control Plane CIoT 5GS Optimisation (i.e. that a user-plane connection shall never be established for the new PDU session). If a PDU session shall only use Control Plane CIoT 5GS Optimisation, the AMF provides a Control Plane Only Indicator to the SMF during the PDU session establishment. The SMF provides the Control Plane Only Indicator in the Session Management Request to the UE. A UE and SMF receiving the Control Plane Only Indicator for a PDU session shall always use the Control Plane CIoT 5GS Optimisation for this PDU session.

The following rules apply for the use of the Control Plane Only Indicator during PDU session establishment:

- If N3 data transfer was not successfully negotiated, all PDU sessions shall include Control Plane Only Indicator.
- If N3 data transfer was successfully negotiated then:
    - For a new PDU session for a DNN/S-NSSAI for which the Subscription data for SMF Selection includes an Invoke NEF indication (i.e. for a PDU session which will be anchored in NEF), the AMF shall always include the Control Plane Only Indicator.
    - For a new PDU session for a DNN/S-NSSAI for which the Subscription data for SMF Selection does not include an Invoke NEF indication (i.e. for a PDU session which will be anchored in UPF) and that supports interworking with EPS based on the subscription data defined in TS 23.502 [3]:
        - for the first PDU Session the AMF determines based on local policy whether to include the Control Plane Only Indicator or not;
        - if the AMF previously included a Control Plane Only Indicator for PDU sessions that support interworking with EPS based on the subscription data defined in TS 23.502 [3] and that are anchored in UPF, the AMF shall include it also for the new PDU session;
        - if the AMF previously did not include a Control Plane Only Indicator for any of the PDU sessions that support interworking with EPS based on the subscription data defined in TS 23.502 [3] and that are anchored in UPF, the AMF shall not include it for the new PDU session.
- For a new PDU session for a DNN/S-NSSAI for which the Subscription data for SMF Selection does not include an Invoke NEF indication (i.e. for a PDU session which will be anchored in UPF) and that does not support interworking with EPS based on the subscription data defined in TS 23.502 [3], AMF determines individually per PDU session whether to include the Control Plane Only Indicator or not.

As described in clause 5.31.4.2, if UE and AMF successfully negotiate N3 data transfer in addition to Control Plane CIoT 5GS Optimisation, the UE or SMF may request to establish N3 data transfer for one or more PDU sessions for which Control Plane Only Indicator was not received. In CM-CONNECTED, the UE and the network use N3 delivery for PDU sessions for which user plane resources are established, and uses NAS for data transmission for PDU sessions for which user plane resources are not established.

If the AMF determines that Control Plane Only indication associated with PDU Session is not applicable any longer due to e.g. change of Preferred and Supported Network Behaviour, subscription data, and local policy, the AMF should request the SMF to release the PDU Session as specified in clause 4.3.4.2 or clause 4.3.4.3 of TS 23.502 [3].

Early Data Transmission may be initiated by the UE for mobile originated Control Plane CIoT 5GS Optimisation when the RAT Type is E-UTRA.

5.31.4.2 Establishment of N3 data transfer during Data Transport in Control Plane CIoT 5GS Optimisation

If UE and AMF have successfully negotiated N3 data transfer in addition to Control Plane CIoT 5GS Optimisation based on the Preferred and Supported Network Behaviour as defined in clause 5.31.2, then the SMF may decide to establish N3 data transfer for any PDU session for which Control Plane Only Indicator was not included based on local

SMF decision e.g. based on the amount of data transferred in UL or DL using Control Plane CIoT 5GS Optimisation. In that case, the SMF initiates the SMF-triggered N3 data transfer establishment procedure as described in TS 23.502 [3] clause 4.2.10.2.

If UE and AMF successfully negotiate N3 data transfer in addition to Control Plane CIoT 5GS Optimisation based on the Preferred and Supported Network Behaviour as defined in clause 5.31.2, then the UE may decide to establish N3 data transfer for any PDU session for which Control Plane Only Indicator was not included based on local decision, e.g. based on the amount of data to be transferred. In that case, the UE performs the UE triggered N3 data transfer establishment procedure as described in TS 23.502 [3] clause 4.2.10.1.

5.31.4.3 Control Plane Relocation Indication procedure

For intra-NB-IoT mobility when UE and AMF are using Control Plane CIoT 5GS Optimisation, the CP Relocation Indication procedures may be used. The purpose of the CP Relocation Indication procedure is to request the AMF to authenticate the UE's re-establishment request (see TS 33.501 [29]), and initiate the establishment of the UE's N2 connection after the UE has initiated an RRC Re-Establishment procedure in a new NG-RAN node (see TS 38.300 [27]).

The RRC Re-Establishment procedure uses the Truncated 5G-S-TMSI as the UE identifier. The NG-RAN is configured with the sizes of the components of the Truncated 5G-S-TMSI and it is configured with how to recreate the AMF Set ID, the AMF Pointer and 5G-TMSI from the equivalent truncated parameters (see TS 23.003 [19]).

The AMF configures the UE with the Truncated 5G-S-TMSI Configuration that provides the sizes of the components of the Truncated 5G-S-TMSI as described in TS 24.501 [47] during the Registration. The configuration of these parameters are specific to each PLMN.

NOTE: Network sharing default configuration of the sizes of the truncated components is described in TS 23.003 [19].

5.31.5 Non-IP Data Delivery (NIDD)

Functions for NIDD may be used to handle Mobile Originated (MO) and Mobile Terminated (MT) communication for unstructured data (also referred to as Non-IP). Such delivery to the AF is accomplished by one of the following two mechanisms:

- Delivery using the NIDD API;
- Delivery using UPF via a Point-to-Point (PtP) N6 tunnel.

NIDD is handled using an Unstructured PDU session to the NEF. The UE may obtain an Unstructured PDU session to the NEF during the PDU Session Establishment procedure. Whether or not the NIDD API shall be invoked for a PDU session is determined by the presence of a "NEF Identity for NIDD" for the DNN/S-NSSAI combination in the subscription. If the subscription includes a "NEF Identity for NIDD" corresponding with the DNN and S-NSSAI information, then the SMF selects that NEF and uses the NIDD API for that PDU session. The NEF ID for a given DNN and S-NSSAI in the subscription can be updated by using the NIDD configuration procedure.

The NEF exposes the NIDD APIs described in TS 23.502 [3] on the N33/Nnef reference point.

The NEF uses the provisioned policies to map an AF Identity and UE Identity to a DNN/S-NSSAI combination if the Reliable Data Service (RDS) is not enabled. If RDS is enabled, the NEF determines the association based on RDS port numbers and the provisioned policies that may be used to map AF identity and User identity to a DNN.

The NEF also supports distribution of Mobile Terminated messages to a group of UEs based on the NIDD API. If an External Group Identifier is included in the MT NIDD request, the NEF uses the UDM to resolve the External Group Identifier to a list of SUPIs and sends the message to each UE in the group with an established PDU Session.

The Protocol Configuration Options (PCO) may be used to transfer NIDD parameters to and from the UE (e.g. maximum packet size). The PCO is sent in the 5GSM signalling between UE and SMF. NIDD parameters are sent to and from the NEF via the N29 interface.

5.31.6 Reliable Data Service

The Reliable Data Service (RDS) may be used between the UE and NEF or UPF when using a PDU Session of PDU Type 'Unstructured'. The service provides a mechanism for the NEF or UPF to determine if the data was successfully delivered to the UE and for the UE to determine if the data was successfully delivered to the NEF or UPF. When a requested acknowledgement is not received, the Reliable Data Service retransmits the packet. The service is enabled or disabled based on DNN and NSSAI Configuration per SLA.

When the service is enabled, a protocol is used between the end-points of the unstructured PDU Session. The protocol uses a packet header to identify if the packet requires no acknowledgement, requires an acknowledgement, or is an acknowledgment and to allow detection and elimination of duplicate PDUs at the receiving endpoint. RDS supports both single and multiple applications within the UE. Port Numbers in the header are used to identify the application on the originator and to identify the application on the receiver. The UE, NEF and the UPF may support reservation of the source and destination port numbers for their use and subsequent release of the reserved port numbers. Reliable Data Service protocol (as defined in TS 24.250 [80]) also enables applications to query their peer entities to determine which port numbers are reserved and which are available for use at any given time. The header is configured based on Reliable Data Service Configuration information which is obtained in the NIDD configuration, MT NIDD, and MO NIDD procedures with the AF as specified in TS 23.502 [3].

During NIDD Configuration, the AF may indicate which serialization formats it supports for mobile originated and mobile terminated traffic in the Reliable Data Server Configuration. When port numbers are reserved by the UE, the serialization format that will be used by the application may be indicated to the NEF. When port numbers are reserved by the NEF, the serialization format that will be used by the application may be indicated to the UE. If the receiver does not support the indicated serialization format, it rejects the port number reservation request and the sender may re-attempt to reserve the port number with a different serialization format. If, during NIDD Configuration, the AF indicated that it supports multiple serialization formats, the NEF determines the serialization format that it will indicate to the UE based on local policies and previous negotiations with the UE (e.g. the NEF may indicate the same serialization format that was indicated by the UE or avoid indicating a serialization format that was previously rejected by the UE). When serialization formats are configured for reserved port numbers, the NEF stores the serialization formats as part of the Reliable Data Service Configuration and provides the updated Reliable Data Service Configuration to the AF.

NOTE: Whether the UE Application or AF supports a given serialization format is outside the scope of 3GPP specifications.

The UE indicates its capability of supporting RDS in the Protocol Configuration Options (PCO) and the SMF negotiates RDS support with the NEF or UPF. If the NEF or UPF supports and accepts RDS then the SMF indicates to the UE, in the PCO, that the RDS shall be used if enabled in the DNN and NSSAI configuration.

In order to prevent situations where an RDS instance needs to interface to both the user and control plane, RDS may only be used with PDU Sessions for which the "Control Plane CIoT 5GS Optimisation" indication is set or with PDU sessions using the Control Plane CIoT 5GS Optimisation when the AMF does not move the PDU session to the user plane.

Reliable Data Service protocol is defined in TS 24.250 [80].

5.31.7 Power Saving Enhancements

5.31.7.1 General

To enable UE power saving and to enhance MT reachability while using MICO mode, e.g. for CIoT, the following features are specified in the following clauses:

- Extended Discontinuous Reception (DRX) for CM-IDLE and CM-CONNECTED with RRC-INACTIVE;
- MICO mode with Extended Connected Time;
- MICO mode with Active Time;
- MICO mode and Periodic Registration Timer Control.

If a UE requests via NAS to enable both MICO mode with Active Time and extended idle mode DRX, e.g. based on local configuration, Expected UE Behaviour, if available, UE requested Active Time value, UE subscription

information and network policies etc, the AMF may decide to enable MICO mode with or without Active Time, extended idle mode DRX or both.

5.31.7.2 Extended Discontinuous Reception (DRX) for CM-IDLE and CM-CONNECTED with RRC-INACTIVE

5.31.7.2.1 Overview

The UE and the network may negotiate over non-access stratum signalling the use of extended idle mode DRX for reducing its power consumption, while being available for mobile terminating data and/or network originated procedures within a certain delay dependent on the DRX cycle value. Extended DRX in CM-IDLE is supported for E-UTRA connected to 5GC. Extended DRX in CM-CONNECTED with RRC-Inactive mode is supported for WB-E-UTRA and LTE-M connected to 5GC. RRC-Inactive is not supported by NB-IoT connected to 5GC. Neither Extended DRX in CM-IDLE nor extended DRX in CM-CONNECTED with RRC-Inactive are supported for NR.

The negotiation of the eDRX parameters for WB-E-UTRA and LTE-M is supported over any RAT (including NR).

Applications that want to use extended idle mode DRX need to consider specific handling of mobile terminating services or data transfers, and in particular they need to consider the delay tolerance of mobile terminated data. A network side application may send mobile terminated data, an SMS, or a device trigger, and needs to be aware that extended idle mode DRX may be in place. A UE should request for extended idle mode DRX only when all expected mobile terminating communication is tolerant to delay.

NOTE 1: The extended idle mode DRX cycle length requested by UE takes into account requirements of applications running on the UE. Subscription based determination of eDRX cycle length can be used in those rare scenarios when applications on UE cannot be modified to request appropriate extended idle mode DRX cycle length. The network accepting extended DRX while providing an extended idle mode DRX cycle length value longer than the one requested by the UE, can adversely impact reachability requirements of applications running on the UE.

UE and NW negotiate the use of extended idle mode DRX as follows:

If the UE decides to request for extended idle mode DRX, the UE includes an extended idle mode DRX parameters information element in the Registration Request message. The UE may also include the UE specific DRX parameters information element for regular idle mode DRX according to clause 5.4.5. The extended DRX parameters information element includes the extended idle mode DRX cycle length.

The AMF decides whether to accept or reject the UE request for enabling extended idle mode DRX. If the AMF accepts the extended idle mode DRX, the AMF based on operator policies and, if available, the extended idle mode DRX cycle length value in the subscription data from the UDM, may also provide different values of the extended idle mode DRX parameters than what was requested by the UE. The AMF taking into account the RAT specific Subscribed Paging Time Window, the UE's current RAT and local policy also assigns a Paging Time Window length to be used, and provides this value to the UE during Registration Update procedures together with the extended idle mode DRX cycle length in the extended DRX parameter information element. If the AMF accepts the use of extended idle mode DRX, the UE shall apply extended idle mode DRX based on the received extended idle mode DRX length, the UE's current RAT (NB-IoT, WB-E-UTRA or LTE-M) and RAT specific Paging Time Window length. If the UE does not receive the extended DRX parameters information element in the relevant accept message because the AMF rejected its request or because the request was received by AMF not supporting extended idle mode DRX, the UE shall apply its regular discontinuous reception as defined in clause 5.4.5.

For WB-E-UTRA and LTE-M the eNB broadcasts an indicator for support of extended idle mode DRX in 5GC in addition to the existing indicator for support of extended idle mode DRX in EPC as defined in TS 36.331 [51]. This indicator is used by the UE in CM-IDLE state.

NOTE 2: A broadcast indicator for support of extended idle mode DRX is not needed for NB-IoT as it is always supported in NB-IoT.

The specific negotiation procedure handling is described in TS 23.502 [3].

NOTE 3: If the Periodic Registration Update timer assigned to the UE is not longer than the extended idle mode DRX cycle the power savings are not maximised.

For RAT types that support extended DRX for CM-CONNECTED with RRC Inactive state, the AMF passes the UE's accepted idle mode eDRX cycle length value to NG-RAN. If the UE supports eDRX in RRC inactive, based on its UE radio capabilities, NG-RAN configures the UE with an eDRX cycle in RRC-INACTIVE up to the value for the UE's idle mode eDRX cycle as provided by the AMF in "RRC Inactive Assistance Information" as defined in clause 5.3.3.2.5 or up to 10.24 seconds (whichever is lower).

If eDRX cycle is applied in RRC-INACTIVE, the RAN buffers DL packets up to the duration of the eDRX cycle chosen by NG-RAN.

When the UE has PDU Session(s) associated with emergency services, the UE and AMF follow regular discontinuous reception as defined in clause 5.4.5 and shall not use the extended idle mode DRX. Extended idle mode DRX parameters may be negotiated while the UE has PDU Session(s) associated with emergency services. When the PDU Session(s) associated with emergency services are released, the UE and AMF shall reuse the negotiated extended idle mode DRX parameters in the last Registration Update procedure.

The UE shall include the extended DRX parameters information element in each Registration Request message if it still wants to use extended idle mode DRX. At AMF to AMF, AMF to MME and MME to AMF mobility, the extended idle mode DRX parameters are not sent from the old CN node to the new CN node as part of the MM context information.

5.31.7.2.2 Paging for extended idle mode DRX in E-UTRA connected to 5GC

5.31.7.2.2.0 General

For WB-E-UTRA and LTE-M connected to 5GC, the extended idle mode DRX value range will consist of values starting from 5.12s (i.e. 5.12s, 10.24s, 20.48s, etc.) up to a maximum of 2621.44s (almost 44 min). For NB-IoT, the extended idle mode DRX value range will start from 20.48s (i.e., 20.48s, 40.96s, 81.92, etc.) up to a maximum of 10485.76s (almost 3 hours) (see TS 36.304 [52]). The extended idle mode DRX cycle length is negotiated via NAS signalling. The AMF includes the extended idle mode DRX cycle length for WB-E-UTRA, LTE-M or NB-IoT in paging message to assist the NG-RAN node in paging the UE.

For extended idle mode DRX cycle length of 5.12s, the network follows the regular paging strategy as defined in clause 5.4.5.

For extended idle mode DRX cycle length of 10.24s or longer, clauses 5.31.7.2.2.1, 5.31.7.2.2.2 and 5.31.7.2.2.3 apply.

5.31.7.2.2.1 Hyper SFN, Paging Hyperframe and Paging Time Window length

A Hyper-SFN (H-SFN) frame structure is defined on top of the SFN used for regular idle mode DRX. Each H-SFN value corresponds to a cycle of the legacy SFN of 1024 radio frames, i.e. 10.24s. When extended idle mode DRX is enabled for a UE, the UE is reachable for paging in specific Paging Hyperframes (PH), which is a specific set of H-SFN values. The PH computation is a formula that is function of the extended idle mode DRX cycle, and a UE specific identifier, as described in TS 36.304 [52]. This value can be computed at all UEs and AMFs without need for signalling. The AMF includes the extended idle mode DRX cycle length and the PTW length in paging message to assist the NG-RAN nodes in paging the UE.

The AMF also assigns a Paging Time Window length, and provides this value to the UE during Registration Update procedures together with the extended idle mode DRX cycle length. The UE first paging occasion is within the Paging Hyperframe as described in TS 36.304 [52]. The UE is assumed reachable for paging within the Paging Time Window. The start and end of the Paging Time Window is described in TS 36.304 [52]. After the Paging Time Window length, the AMF considers the UE unreachable for paging until the next Paging Hyperfame.

5.31.7.2.2.2 Loose Hyper SFN synchronization

NOTE: This clause applies for extended DRX cycle lengths of 10.24s or longer.

In order for the UE to be paged at roughly similar time, the H-SFN of all NG-RAN nodes and AMFs should be loosely synchronized.

Each NG-RAN node and AMF synchronizes internally the H-SFN counter so that the start of H-SFN=0 coincides with the same a preconfigured time epoch. If NG-RAN nodes and AMFs use different epochs, e.g., due to the use of different time references, the GPS time should be set as the baseline, and the NG-RAN nodes and AMFs synchronize the H-SFN counter based on the GPS epoch considering the time offset between GPS epoch and other time-reference epoch a

preconfigured time. It is assumed that NG-RAN nodes and AMFs are able to use the same H-SFN value with accuracy in the order of legacy DRX cycle lengths, e.g. 1 to 2 seconds. There is no need for synchronization at SFN level.

There is no signalling between network nodes required to achieve this level of loose H-SFN synchronization.

5.31.7.2.2.3 AMF paging and paging retransmission strategy

NOTE: This clause applies for extended DRX cycle lengths of 10.24s or longer.

When the AMF receives trigger for paging and the UE is reachable for paging, the AMF sends the paging request. If the UE is not reachable for paging, then the AMF pages the UE just before the next paging occasion.

The AMF determines the Paging Time Window length and a paging retransmission strategy, and executes the retransmission scheme.

5.31.7.2.3 Paging for a UE registered in a tracking area with heterogeneous support of extended idle mode DRX

When the UE is registered in a registration area with heterogeneous support of extended idle mode DRX (e.g. comprising WB-E-UTRA and NR cells) and has negotiated eDRX, the AMF shall, for any paging procedure, perform at least one paging attempt during a PTW.

NOTE: Heterogeneous support of extended idle mode DRX in tracking areas assigned by AMF in a TAI list can result in significant battery life reduction in the UE as compared to homogeneous support by NG-RAN nodes of extended idle mode DRX.

5.31.7.3 MICO mode with Extended Connected Time

When a UE, using MICO mode, initiates MO signalling or MO data and the AMF is aware of pending or expected MT traffic, the AMF may keep the UE in CM-CONNECTED state and the RAN may keep the UE in RRC-CONNECTED state for an Extended Connected Time period in order to ensure the downlink data and/or signalling is delivered to the UE. The Extended Connected Time is determined by the AMF and is based on local configuration and/or the Maximum Response Time, if provided by the UDM.

The AMF maintains the N2 connection for at least the Extended Connected Time and provides the Extended Connected Time value to the RAN. The Extended Connected Time value indicates the minimum time the RAN should keep the UE in RRC-CONNECTED state regardless of inactivity. The Extended Connected Time value is provided to the RAN together with the

- NAS Registration Accept message; or
- NAS Service Accept message.

5.31.7.4 MICO mode with Active Time

During a Registration procedure the UE may optionally request an Active Time value from the AMF as part of MICO Mode negotiation. In response, if the AMF receives an Active Time value from the UE and determines that the MICO mode is allowed for the UE, the AMF may assign an Active Time value for the UE, e.g. based on local configuration, Expected UE Behaviour if available, UE requested Active Time value, UE subscription information and network policies, and indicates it to the UE during Registration procedure. When an Active Time value is assigned to the UE the AMF shall consider the UE reachable for paging after the transition from CM-CONNECTED to CM-IDLE for the duration of the Active Time.

When the AMF indicates MICO mode with an Active Time to a UE, the registration area may be constrained by paging area size. To avoid paging in the entire PLMN, when the AMF allocates the Active Time the AMF should not allocate "all PLMN" registration area to the UE.

The UE and AMF shall set a timer corresponding to the Active Time value negotiated during the most recent Registration procedure. The UE and AMF shall start the timer upon entering CM-IDLE state from CM-CONNECTED. When the timer expires (i.e. reaches the Active Time) the UE enters MICO mode and the AMF can deduce that the UE has entered MICO mode and is not available for paging. If the UE enters CM-CONNECTED state before the timer expires, the UE and AMF shall stop and reset the timer.

If no Active Time value was negotiated during the most recent Registration procedure the UE shall not start the timer and it shall instead enter MICO mode directly upon entering CM-IDLE state.

Active Time is not transferred between AMF and MME.

5.31.7.5 MICO mode and Periodic Registration Timer Control

If the Expected UE Behaviour indicates the absence of DL communication, the AMF may allow MICO mode for the UE and allocate a large periodic registration timer value based on e.g. Network Configuration parameters to the UE so that the UE can maximise power saving between Periodic Registration Updates.

If the Expected UE Behaviour indicates scheduled DL communication the AMF should allow MICO mode for the UE and allocate a periodic registration timer value such that the UE performs Periodic Registration Update to renegotiate MICO mode before or at the scheduled DL communication time, if the AMF decides to allow MICO mode for the UE.

If the UE supports 'Strictly Periodic Registration Timer Indication', the UE indicates its capability of supporting 'Strictly Periodic Registration Timer Indication' in the Registration Request message. If the UE indicates its support of 'Strictly Periodic Registration Timer Indication' in the Registration Request message, the AMF may provide a Strictly Periodic Registration Timer Indication to the UE together with the periodic registration timer value, e.g. based on Expected UE Behaviour. If the indication is provided by the AMF, the UE and the AMF shall start the periodic registration timer after completion of the Registration procedure. The UE and the AMF shall neither stop nor restart the periodic registration timer when the UE enters CM-CONNECTED, and shall keep it running while in CM-CONNECTED state and after returning to CM-IDLE state. If and only when the timer expires and the UE is in CM-IDLE, the UE shall perform a Periodic Registration Update. If the timer expires and the UE is in CM-CONNECTED state, the AMF and the UE restart the periodic registration timer while still applying 'Strictly Periodic Registration Timer Indication'. The AMF may use the UE Configuration Update procedure to trigger the UE to perform Registration procedure, in which the periodic registration timer value and 'Strictly Periodic Registration Timer Indication' can be renegotiated.

When the UE and the AMF locally disable MICO mode (e.g. when an emergency service is initiated), the UE and the AMF shall not apply 'Strictly Periodic Registration Timer Indication'.

If the periodic registration timer is renegotiated during a Registration procedure, e.g. triggered by UE Configuration Update, and if the periodic registration timer is running, then the periodic registration timer is stopped and restarted using the renegotiated value even when the Strictly Periodic Registration Timer Indication was provided to the UE.

5.31.8 High latency communication

Functions for High latency communication may be used to handle mobile terminated (MT) communication with UEs being unreachable while using power saving functions as specified in clause 5.31.7. "High latency" refers to the initial response time before normal exchange of packets is established. That is, the time it takes before a UE has woken up from its power saving state and responded to an initial downlink packet or signal.

High latency communication is supported by extended buffering of downlink data in the UPF, SMF or NEF when a UE is using power saving functions in CM-IDLE state and the UE is not reachable. For UPF anchored PDU sessions the SMF configures during AN release the UPF with user data Forwarding Action Rule and user data Buffering Action Rule according to TS 29.244 [65]. The rules include instructions whether UPF buffering applies or the user data shall be forwarded to the SMF for buffering in the SMF. For NEF anchored PDU sessions only extended buffering in the NEF is supported in this release of the specification. During the Network Triggered Service Request procedure or Mobile Terminated Data Transport procedures when using Control Plane CIoT 5GS Optimisation, the AMF provides an Estimated Maximum Wait Time to the SMF if the SMF indicates the support of extended buffering. The SMF determines the Extended Buffering Time based on the received Estimated Maximum Wait Time or local configuration. The handling is e.g. specified in the Network Triggered Service Request procedure, clauses 4.2.3.3, 4.2.6, 4.24.2 and 4.25.5 of TS 23.502 [3].

High latency communication is also supported through notification procedures. The following procedures are available based on different monitoring events:

- UE Reachability;
- Availability after DDN failure;
- Downlink Data Delivery Status.

An AF may request a one-time "UE Reachability" notification when it wants to send data to a UE which is using a power saving function (see event subscription procedure in clause 4.15.3.2 of TS 23.502 [3]). The SCS/AS/AF then waits with sending the data until it gets a notification that the UE is reachable (see notification procedures in TS 23.502 [3]).

An AF may request repeated "Availability after DDN failure" notifications where each UE reachability notification is triggered by a preceding DDN failure, i.e. the AF sends a downlink packet to request a UE reachability notification when the UE becomes reachable. That downlink packet is discarded by the UPF or SMF or NEF (see notification procedures in TS 23.502 [3]).

An AF may request repeated "Downlink Data Delivery Status" notifications when it wants indications that DL data has been buffered or when buffered DL data has been delivered to the UE.

An AF may provide parameters related to High latency communication for different methods to UDM, via NEF, as part of provisioning capability as specified in clause 5.20. The UDM can further deliver the parameters to other NFs (e.g. AMF or SMF) as specified in clause 4.15.6 of TS 23.502 [3].

5.31.9 Support for Monitoring Events

The Monitoring Events feature is intended for monitoring of specific events in the 3GPP system and reporting such Monitoring Events via the NEF. The feature allows NFs in 5GS to be configured to detect specific events and report the events to the requested party. Clause 5.20 further discusses the Monitoring capabilities of the NEF.

For CIoT, the list of supported monitoring events is specified in Table 4.15.3.1-1 of TS 23.502 [3].

Support for Monitoring Events can be offered via AMF, UDM and SMF, and can be reported via the NEF, as specified in clause 4.15.3 of TS 23.502 [3].

5.31.10 NB-IoT UE Radio Capability Handling

NB-IoT Radio Capabilities are handled in the network independently from other RATs' Radio Capabilities, see clause 5.4.4.1.

5.31.11 Inter-RAT idle mode mobility to and from NB-IoT

Tracking Areas are configured so that they do not contain both NB-IoT and other RATs' cells, so when the UE is changing RAT type to or from NB-IoT while remaining registered with 5GC, the UE will perform the Mobility Registration Update procedure, see clause 5.3.2.3. When the UE is changing RAT type to or from NB-IoT and moving between 5GC and EPC, during the Registration, Attach or TAU procedure the RAT type change is determined.

The specification in this clause does not apply to RAT type corresponding to Non-3GPP Access type.

PDU session handling is controlled by "PDU Session continuity at inter RAT mobility" in the UE's subscription data, which indicates per DNN/S-NSSAI whether to;

- maintain the PDU session,
- disconnect the PDU session with a reactivation request,
- disconnect the PDU session without reactivation request, or
- leave it up to local VPLMN policy

when the UE moves between a "broadband" RAT (e.g. NR or WB-E-UTRA) and a "narrowband" RAT (NB-IoT).

During PDU session establishment the SMF retrieves the "PDU Session continuity at inter RAT mobility" subscription information (if available) from the UDM. Local SMF configuration is used if "PDU Session continuity at inter RAT mobility" is not available for a PDU Session.

The AMF informs the SMF at an inter-RAT idle mobility event, e.g. to or from NB-IoT connected to 5GC about the RAT type change in the Nsmf_PDUSession_UpdateSMContext message during the Registration procedure. Based on this (H-)SMF handles the PDU session according to "PDU session continuity at inter RAT mobility information" subscription data or based on local policy.

NOTE: The "PDU Session continuity at inter RAT mobility" and "PDN continuity at inter-RAT mobility" subscription should be the same so that the PDU sessions/PDN connections are handled the same by both CN types.

During inter-RAT idle mode mobility to NB-IoT, if a PDU session has more than one QoS rule, the SMF shall initiate a PDU session modification procedure as described in TS 23.502 [3] to remove any non-default QoS rule, and maintain only the default QoS rule.

5.31.12 Restriction of use of Enhanced Coverage

Support of UEs in Enhanced Coverage is specified in TS 36.300 [30].

The usage of Enhanced Coverage requires use of extensive resources (e.g. radio and signalling resources). Specific subscribers can be restricted to use the Enhanced Coverage feature through Enhanced Coverage Restricted information that is stored in the UDM as part of subscription data and specifies per PLMN whether the Enhanced Coverage functionality is restricted or not for the UE. For eMTC, the Enhanced Coverage Restricted information indicates whether CE mode B is restricted for the UE, or both CE mode A and CE mode B are restricted for the UE, or both CE mode A and CE mode B are not restricted for the UE. For NB-IoT, the NB-IoT Enhanced Coverage Restricted information indicates whether the Enhanced Coverage is restricted or not for the UE.

The AMF receives Enhanced Coverage Restricted information from the UDM during the Registration procedure. The AMF based on local configuration, UE Usage setting, UE subscription information and network policies, or any combination of them, determines whether Enhanced Coverage (i.e. CE mode B or both CE mode B & CE mode A) is restricted for the UE and stores updated Enhanced Coverage Restriction information in the UE context in the AMF. If the UE usage setting indicated that UE is "voice centric", then the AMF shall set CE mode B restricted for the UE in Enhanced Coverage Restriction information.

If the UE includes the support for restriction of use of Enhanced Coverage, the AMF sends Enhanced Coverage Restricted information to the UE in the Registration Accept message. The UE shall use the value of Enhanced Coverage Restricted information to determine if enhanced coverage feature is restricted or not. The AMF provides an Enhanced Coverage Restricted information to the RAN via N2 signalling whenever the UE context is established in the RAN, e.g. during N2 Paging procedure, Service Request procedure, Initial Registration and Periodic Registration procedure.

For roaming UEs, if the UDM doesn't provide any Enhanced Coverage Restricted information or the provided Enhanced Coverage Restricted information is in conflict with the roaming agreement, the AMF uses default Enhanced Coverage Restricted information locally configured in the VPLMN based on the roaming agreement with the subscriber's HPLMN.

The UE indicates its capability of support for restriction of use of Enhanced Coverage to the AMF in the Registration procedure for the RAT it is camping on. A UE that supports Enhanced Coverage shall also support restriction of the Enhanced Coverage.

The UE shall assume that restriction for use of Enhanced Coverage is the same in the equivalent PLMNs.

If the UE supports CE mode B and use of CE mode B is not restricted according to the Enhanced Coverage Restriction information in the UE context in the AMF, then the AMF shall use the extended NAS-MM timer setting for the UE as specified in TS 24.501 [47] and shall send the extended NAS-SM timer indication during PDU session establishment to the SMF.

If the UE supports CE mode B and use of CE mode B changes from restricted to unrestricted or vice versa in the Enhanced Coverage Restriction information in the UE context in the AMF (e.g. due to a subscription change) then:

- The AMF determines when to enforce the change of restriction of use of Enhanced Coverage.
- When the UE is in CM-CONNECTED mode, the AMF can use the UE Configuration Update procedure, as specified in step 3a of clause 4.2.4.2 of TS 23.502 [3], to trigger a mobility registration update procedure in CM-CONNECTED mode for the AMF to inform the change of restriction of Enhanced Coverage towards the UE.
- If the UE has already established PDU sessions, then the AMF shall trigger a PDU session modification to the SMFs serving the UE's PDU sessions to update the use of the extended NAS-SM timer setting as described in step 1f of clause 4.3.3.2 of TS 23.502 [3] when the AMF determines that NAS-SM timer shall be updated due to the change of Enhanced Coverage Restriction.

- The UE and network applies the new Enhanced Coverage Restriction information after mobility registration procedure is completed.

Based on the extended NAS-SM timer indication, the SMF shall use the extended NAS-SM timer setting for the UE as specified in TS 24.501 [47].

The support for Enhanced Coverage Restriction Control via NEF enables AF to query status of Enhanced Coverage Restriction or enable/disable Enhanced Coverage Restriction per individual UEs. The procedure for Enhanced Coverage Restriction Control via NEF is described in clause 4.27 of TS 23.502 [3].

5.31.13 Paging for Enhanced Coverage

Support of UEs in Enhanced Coverage is specified in TS 36.300 [30].

Whenever N2 is released and Paging Assistance Data for CE capable UE is available for the UE, the NG-RAN sends it to the AMF as described in TS 23.502 [3] clause 4.2.6.

The AMF stores the received Paging Assistance Data for CE capable UE and, if Enhanced Coverage is not restricted for the UE, then the AMF includes it in every subsequent Paging message for all NG-RAN nodes selected by the AMF for paging.

NOTE: Only the NG-RAN node which cell ID is included in the Paging Assistance Data considers the assistance data.

5.31.14 Support of rate control of user data

5.31.14.1 General

The rate of user data sent to and from a UE (e.g. a UE using CIoT 5GS Optimisations) can be controlled in two different ways:

- Serving PLMN Rate Control;
- Small Data Rate Control.

Serving PLMN Rate Control is intended to allow the Serving PLMN to protect its AMF and the Signalling Radio Bearers in the NG-RAN from the load generated by NAS Data PDUs.

Small Data Rate Control is intended to allow HPLMN operators to offer customer services such as "maximum of Y messages per day".

NOTE: Existing Session-AMBR mechanisms are not suitable for such a service since, for radio efficiency and UE battery life reasons, an AMBR of e.g. > 100kbit/s is desirable and such an AMBR translates to a potentially large daily data volume.

The SMF in the Serving PLMN may send the Small Data rate control parameter for an emergency PDU session.

5.31.14.2 Serving PLMN Rate Control

The Serving PLMN Rate Control value is configured in the (V-)SMF.

NOTE 1: Homogeneous support of Serving PLMN Rate Control in a network is assumed.

At PDU Session establishment and PDU Session modification, the (V-)SMF may inform the UE and UPF/NEF of any per PDU Session local Serving PLMN Rate Control that the Serving PLMN intends to enforce for NAS Data PDUs. The (V-)SMF shall only indicate a Serving PLMN Rate Control command to the UPF if the PDU Session is using N4 and is set to Control Plane only. The (V-)SMF shall only indicate a Serving PLMN Rate Control command to the NEF if that PDN connection is using NEF.

Serving PLMN rate control is operator configurable and expressed as "X NAS Data PDUs per deci hour" where X is an integer that shall not be less than 10. There are separate limits for uplink and downlink NAS Data PDUs:

- The UE shall limit the rate at which it generates uplink NAS Data PDUs to comply with the Serving PLMN policy. In the UE the indicated rate control applies only on the PDU Session where it was received, and therefore the UE shall limit the rate of its uplink NAS Data PDUs to comply with the rate that is indicated for the PDU Session. The indicated rate is valid until the PDU Session is released.

- The UPF/NEF shall limit the rate at which it generates downlink Data PDUs. In the UPF/NEF the indicated rate control applies only on the PDU Session where it was received, and therefore the UPF/NEF shall limit the rate of its downlink Data PDUs to comply with the rate that is indicated for the PDU Session.

- The (V-)SMF may enforce these limits per PDU Session by discarding or delaying packets that exceed these limits. The Serving PLMN Rate does not include SMS using NAS Transport PDUs. The (V-)SMF starts the Serving PLMN Rate Control when the first NAS Data PDU is received.

NOTE 2: If the UE/UPF/NEF start the Serving PLMN rate control at a different time than the (V-)SMF, PDUs sent within the limit enforced at the UE/UPF/NEF can still exceed the limit enforced by the (V-)SMF.

NOTE 3 It is assumed that the Serving PLMN Rate is sufficiently high to not interfere with the Small Data Rate Control as the Small Data Rate Control, if used, is assumed to allow fewer messages. NAS PDUs related to exception reports are not subject to the Serving PLMN Rate Control.

5.31.14.3 Small Data Rate Control

The (H-)SMF may consider, e.g. based on operator policy, subscription, DNN, S-NSSAI, RAT type etc. to determine whether to apply Small Data Rate Control or not. The (H-)SMF can send a Small Data Uplink Rate Control command to the UE using the PCO information element. The (H-)SMF informs the UPF or NEF of any Small Data Rate Control that shall be enforced.

The Small Data Rate Control applies to data PDUs sent on that PDU Session by either Data Radio Bearers or Signalling Radio Bearers (NAS Data PDUs).

The rate control information is separate for uplink and downlink and in the form of:

- an integer 'number of packets per time unit', and

- an integer 'number of additional allowed exception report packets per time unit' once the rate control limit has been reached.

The UE shall comply with this uplink rate control instruction. If the UE exceeds the uplink 'number of packets per time unit', the UE may still send uplink exception reports if allowed and the 'number of additional allowed exception reports per time unit' has not been exceeded. The UE shall consider this rate control instruction as valid until it receives a new one from (H-)SMF.

When a PDU Session is first established, the (H-)SMF may provide the configured Small Data Rate Control parameters to the UE and UPF or NEF.

When the PDU Session is released, the Small Data Rate Control Status (including the number of packets still allowed in the given time unit, the number of additional exception reports still allowed in the given time unit and the termination time of the current Small Data Rate Control validity period) may be stored in the AMF so that it can be retrieved for a subsequent re-establishment of a new PDU Session.

At subsequent establishment of a new PDU Session, the (H-)SMF may receive the previously stored Small Data Rate Control Status and if the validity period has not expired, it provides the parameters to the UE in the PCO and to the UPF/NEF as the initially applied parameters, in addition to the configured Small Data Rate Control parameters. If the initially applied parameters are provided, the UE and UPF or NEF shall apply them and shall use the SMF provided configured Small Data Rate Control parameters once the initially applied Small Data Rate Control validity period expires.

NOTE 1: Storage of Small Data Rate Control Status information for very long time intervals can be implementation specific.

For the UPF and NEF, Small Data Rate Control is based on a 'maximum allowed rate' per direction. If (H-)SMF provided the 'number of additional allowed exception report packets per time unit', then the 'maximum allowed rate' is equal to the 'number of packets per time unit' plus the 'number of additional allowed exception report packets per time unit', otherwise the 'maximum allowed rate' is equal to the 'number of packets per time unit'.

The UPF or NEF may enforce the uplink rate by discarding or delaying packets that exceed the 'maximum allowed rate'. The UPF or NEF shall enforce the downlink rate by discarding or delaying packets that exceed the downlink part of the 'maximum allowed rate'.

NOTE 2: It is assumed that the Serving PLMN Rate is sufficiently high to not interfere with the Small Data Rate Control as the Small Data Rate Control, if used, is assumed to allow fewer messages. NAS PDUs related to exception reports are not subject to the Serving PLMN Rate Control.

For NB-IoT the AMF maintains an "MO Exception Data Counter" which is incremented when the RRC establishment cause "MO exception data" is received from NG-RAN. The AMF reports whether the UE accessed using "MO exception data" RRC establishment cause, to all (H-)SMFs which have PDU Sessions that are subject to Small Data Rate Control and if the UE is accessing using "MO exception data" then the "MO Exception Data Counter" is also provided by the AMF. The SMF indicates each use of the RRC establishment cause "MO Exception Data" by including the related counter on the charging information.

NOTE 3: Since Exception Data PDUs and normal priority PDUs cannot be distinguished within an RRC connection, the AMF is only counting the number of RRC Connection establishments with "MO Exception data" priority.

If the UE moves to EPC then the UE and the PGW-U+UPF store the current Small Data Rate Control Status for all PDU Sessions that are not released. If the UE moves back to 5GC the stored Small Data Rate Control Status is restored and continues to apply to PDU Session(s) that are moved from EPC to 5GC, taking into account remaining validity period of the stored Small Data Rate Control Status. When the UE moves to EPC the Small Data Rate Control Status for all PDU Session(s) may also be stored in the AMF if the PDU Session is released while the UE is connected to EPC and re-established when the UE moves to 5GC. The time to store the Small Data Rate Control Status information is implementation specific.

5.31.15 Control Plane Data Transfer Congestion Control

NAS level congestion control may be applied in general for all NAS messages. To enable congestion control for control plane data transfer, a Control Plane data back-off timer is used, see clause 5.19.7.6.

5.31.16 Service Gap Control

Service Gap Control is an optional feature intended for CIoT UEs to control the frequency at which these UEs can access the network. That is, to ensure a minimum time gap between consecutive Mobile Originated data communications initiated by the UE. This helps reducing peak load situations when there are a large number of these UEs in an operator network. Service Gap Control is intended to be used for "small data allowance plans" for MTC/CIoT UEs where the applications are tolerant to service latency.

NOTE 1: Time critical applications, such as regulatory prioritized services like Emergency services can suffer from the latency caused by the Service Gap Control feature. Therefore Service Gap Control feature is not recommended for subscriptions with such applications and services.

Service Gap Time is a subscription parameter used to set the Service Gap timer and is enforced in the UE and in the AMF on a per UE level (i.e. the same Service Gap Timer applies for all PDU Sessions that the UE has). The UE indicates its capability of support for Service Gap Control in the Registration Request message to the AMF. The AMF passes the Service Gap Time to the UE in the Registration Accept message for a UE that has indicated its support of the Service Gap Control. The Service Gap Control shall be applied in a UE when a Service Gap Time is stored in the UE context and applied in the AMF when the Service Gap Time is stored in the UE Context in the AMF.

Service Gap Control requires the UE to stay in CM-IDLE mode for at least the whole duration of the Service Gap timer before triggering Mobile Originated user data transmission, except for procedures that are exempted (see TS 24.501 [47]). The Service Gap timer shall be started each time a UE moves from CM-CONNECTED to CM-IDLE, unless the connection request was initiated by the paging of a Mobile Terminated event, or after a Mobility or Periodic Registration procedure without Follow-on Request indication and without Uplink data status, which shall not trigger a new or extended Service Gap interval. When a Service Gap timer expires, the UE is allowed to send a connection request again. If the UE does so, the Service Gap timer will be restarted at the next CM-CONNECTED to CM-IDLE transition.

The Service Gap control is applied in CM-IDLE state only and does not impact UE Mobile Originated user data transmission or Mobile Originated signalling in CM-CONNECTED state. The Service Gap timer is not stopped upon

CM-IDLE state to CM-CONNECTED state transition. The UE shall not initiate connection requests for MO user plane data, MO control plane data, or MO SMS when a Service Gap timer is running. The UE shall not initiate PDU Session Establishment Requests when a Service Gap timer is running, unless it is for Emergency services which are allowed. CM-CONNECTED with RRC_INACTIVE is not used for UEs that have a Service Gap Time configured.

NOTE 2: As a consequence of allowing Initial Registration Request procedure, the UE with a running Service Gap timer does not initiate further MO signalling, except for Mobility Registration procedure, until the UE receives MT signalling or after the UE has moved to CM-IDLE state and the Service Gap Timer is not running.

NOTE 3: Implementations need to make sure that latest and up-to-date data are always sent when a Service Gap timer expires.

The AMF may enforce the Service Gap timer by rejecting connection requests for MO user plane data, MO control plane data, or MO SMS when a Service Gap timer is running. The AMF may enforce the Service Gap timer by not allowing MO signalling after Initial Registration requests when a Service Gap timer is running except for Mobility Registration procedure, Periodic Registration procedure or access to the network for regulatory prioritized services like Emergency services, which are allowed. When rejecting the connection requests and the SM signalling after Initial Registration Requests while the Service Gap timer is running, the AMF may include a Mobility Management back-off timer corresponding to the time left of the current Service Gap timer. For UEs that do not support Service Gap Control (e.g. pre-release-16 UEs), Service Gap Control may be enforced using "General NAS level congestion control" as defined in clause 5.19.7.2.

NOTE 4: After MT signalling in CM-CONNECTED state the AMF does not further restrict MO signalling when a Service Gap timer is running as this case is considered equal to a connectivity request in response to paging.

When the AMF starts the Service Gap timer, the AMF should invoke the Service Gap timer with a value that is slightly shorter than the Service Gap Time value provided to the UE based on the subscription information received from the UDM.

NOTE 5: This ensures that the AMF does not reject any UE requests just before the Service Gap timer expires e.g. because of slightly unsynchronized timers between UE and AMF.

A UE which transitions from a MICO mode or eDRX power saving state shall apply Service Gap Control when it wakes up if the Service Gap timer is still running.

Additional aspects of Service Gap Control:

- Service Gap Control applies in all PLMNs.
- When the Service Gap timer is running and the UE receives paging, the UE shall respond as normal.
- Service Gap Control does not apply to exception reporting for NB-IoT.
- Access to the network for regulatory prioritized services like Emergency services are allowed when a Service Gap timer is running.
- Service Gap Control shall be effective also for UEs performing de-registration and re-registration unless access to the network for regulatory prioritized services like Emergency services is required.
- If the Service Gap timer is running, the Service Gap is applied at PLMN selection as follows:

  a) Re-registration to the registered PLMN: The remaining Service Gap timer value survives.

  b) Registration to a different PLMN: The remaining Service Gap timer value survives.

  c) USIM swap: The Service Gap timer is no longer running and the Service Gap feature does not apply, unless re-instantiated by the serving PLMN.

- Multiple uplink packets and downlink packets are allowed during one RRC connection for UE operating within its Rate Control limits.

The following procedures are impacted by Service Gap Control:

- Registration Procedure, see TS 23.502 [3] clause 4.2.2.2;

- UE Triggered Service Request, see TS 23.502 [3] clause 4.2.3.2;

NOTE 6: Since UE triggered Service Request is prevented by Service Gap timer, this implicitly prevents the UE from initiating UPF anchored Mobile Originated Data Transport in Control Plane CIoT 5GS Optimisation (see TS 23.502 [3] clause 4.24.1), NEF Anchored Mobile Originated Data Transport (see TS 23.502 [3] clause 4.25.4) and MO SMS over NAS in CM-IDLE (see TS 23.502 [3] clause 4.13.3.3).

5.31.17 Inter-UE QoS for NB-IoT

To allow NG-RAN to prioritise resource allocation between different UEs accessing via NB-IoT when some of the UEs are using Control Plane CIoT 5GS Optimisation, NG-RAN may, based on configuration, retrieve from the AMF the subscribed NB-IoT UE Priority for any UE accessing via NB-IoT by using the UE's 5G-S-TMSI as the identifier.

In order to reduce signalling load on the AMF, NG-RAN may be configured to request the NB-IoT UE Priority from the AMF e.g. only when the NG-RAN's NB-IoT load exceeds certain threshold(s) or when the NG-RAN needs to cache the QoS profile.

5.31.18 User Plane CIoT 5GS Optimisation

User Plane CIoT 5GS Optimisation enables transfer of user plane data from CM-IDLE without the need for using the Service Request procedure to establish Access Stratum (AS) context in NG-RAN and UE.

If the following preconditions are met:

- UE and AMF negotiated support User Plane CIoT 5GS Optimisation (see clause 5.31.2) over NAS,
- the UE has indicated support of User Plane CIoT 5GS Optimisation in the UE radio capabilities as defined in TS 36.331 [51],
- AMF has indicated User Plane CIoT 5GS Optimisation support for the UE to NG-RAN,
- the UE has established at least one PDU session with active UP connection, i.e. AS context is established in NG-RAN and the UE,

then the RRC connection can be suspended by means of the Connection Suspend Procedure (see clause 4.8.1.2 of TS 23.502 [3]).

Based on a trigger from the NAS layer when a UE is in CM-IDLE with Suspend, the UE should attempt the Connection Resume in CM-IDLE with Suspend procedure (clause 4.8.2.3 of TS 23.502 [3]). If the Connection Resume in CM-IDLE with Suspend procedure fails, the UE initiates the pending NAS procedure. To maintain support for User Plane CIoT 5GS Optimisation for UE mobility across different NG-RAN nodes, the AS Context should be transferred between the NG-RAN nodes, see TS 38.300 [27] and TS 38.423 [99].

By using the Connection Suspend Procedure:

- the UE at transition into CM-IDLE stores the AS information;
- NG-RAN stores the AS information, the NGAP UE association and the PDU session context for that UE;
- AMF stores the NGAP UE association and other information necessary to later resume the UE, interacts with the SMF(s) to deactivate the user plane resources for the UE's PDU Sessions and enters CM-IDLE.

NG-RAN may decide based on implementation to delete the stored UE context and NGAP association. In that case, the RAN shall initiate the AN Release procedure as described in clause 4.2.6 of TS 23.502 [3]. NG-RAN does not initiate any RRC procedure to notify the UE of the UE context release.

By using the Connection Resume in CM-IDLE with Suspend procedure:

- the UE resumes the connection from CM-IDLE with the network using the AS information stored during the Connection Suspend procedure;
- NG-RAN notifies the AMF that the connection with the UE has been resumed;
- AMF enters CM-CONNECTED and interacts with the SMF to activate the user plane resources for the UE's PDU Sessions.

Early Data Transmission may be initiated by the UE for mobile originated User Plane CIoT 5GS Optimisation during Connection Resume.

If the AMF establishes an NGAP UE association with a new NG-RAN node different from the stored NGAP UE association, e.g. the UE initiates service request or registration procedure from a different NG-RAN node, the AMF initiates UE N2 release command towards the old NG-RAN node.

NG-RAN maintains the N3 tunnel endpoint information while a UE is in CM-IDLE with Suspend. UPF is instructed to remove DL N3 Tunnel Info of AN during Connection Suspend procedure, while UPF keeps UL N3 Tunnel Info (i.e. UPF accepts and forwards UL data). If a UE sends MO data with resume procedure, the NG-RAN can send the MO data to the UPF which is addressed by the N3 tunnel endpoint information. In the case of change of serving NG-RAN node due to UE mobility, if NG-RAN determines that it is not able to connect to the UPF which is addressed by the N3 tunnel endpoint information, NG-RAN performs Path Switch procedure before sending the MO data received from the UE.

Early Data Transmission may be initiated by the UE for mobile originated User Plane CIoT 5GS Optimisation when the RAT Type is E-UTRA.

5.31.19 QoS model for NB-IoT

5GC QoS model described in clause 5.7 applies to NB-IoT with the following requirements:

- The default QoS rule shall be the only QoS rule of a PDU Session for a UE connected to 5GC via NB-IoT. There is only one QoS flow (corresponding to the default QoS rule) per PDU session.
- Reflective QoS is not supported over NB-IoT.
- For NB-IoT, there is a 1:1 mapping between the QoS flow corresponding to the default QoS of a PDU session and a Data Radio Bearer when user plane resources are active for that PDU session.
- A maximum of two Data Radio Bearers are supported over NB-IoT. Therefore, at most two PDU sessions can have active user plane resources at the same time.

5.31.20 Category M UEs differentiation

This functionality is used by the network to identify traffic to/from Category M UEs, e.g. for charging differentiation.

A Category M UE using E-UTRA shall provide a Category M indication to the NG-RAN during RRC Connection Establishment procedure as defined in TS 36.331 [51].

When the UE has provided a Category M indication to the NG-RAN during RRC Connection Establishment, the NG-RAN shall provide an LTE-M Indication to the AMF in the Initial UE Message (see TS 23.502 [3] clause 4.2.2.2.1 and TS 38.413 [34]).

When the AMF receives an LTE-M Indication from NG-RAN in an Initial UE Message or from an MME during EPS to 5GS handover, the AMF shall store the LTE-M Indication in the UE context, consider that the RAT type is LTE-M and signal it accordingly to the SMSF during registration procedure for SMS over NAS, to the SMF during PDU Session Establishment or PDU Session Modification procedure. The PCF will also receive the RAT Type as LTE-M, when applicable, from the SMF during SM Policy Association Establishment or SM Policy Association Modification procedure.

The NFs generating CDRs shall include the LTE-M RAT type in their CDRs.

Upon AMF change or inter-system mobility from 5GS to EPS, the source AMF shall provide the "LTE-M Indication" to the target AMF or MME as part of the UE context.

During EPS to 5GS Mobility Registration Procedure, the AMF shall disregard any "LTE-M Indication" received from the MME in the UE context (see TS 23.401 [26]), and take into account the "LTE-M Indication" received from NG-RAN, as specified above.

5.32 Support for ATSSS

5.32.1 General

The ATSSS feature is an optional feature that may be supported by the UE and the 5GC network.

The ATSSS feature enables a multi-access PDU Connectivity Service, which can exchange PDUs between the UE and a data network by simultaneously using one 3GPP access network and one non-3GPP access network and two independent N3/N9 tunnels between the PSA and RAN/AN. The multi-access PDU Connectivity Service is realized by establishing a Multi-Access PDU (MA PDU) Session, i.e. a PDU Session that may have user-plane resources on two access networks.

The UE may request a MA PDU Session when the UE is registered via both 3GPP and non-3GPP accesses, or when the UE is registered via one access only.

After the establishment of a MA PDU Session, and when there are user-plane resources on both access networks, the UE applies network-provided policy (i.e. ATSSS rules) and considers local conditions (such as network interface availability, signal loss conditions, user preferences, etc.) for deciding how to distribute the uplink traffic across the two access networks. Similarly, the UPF anchor of the MA PDU Session applies network-provided policy (i.e. N4 rules) and feedback information received from the UE via the user-plane (such as access network Unavailability or Availability) for deciding how to distribute the downlink traffic across the two N3/N9 tunnels and two access networks. When there are user-plane resources on only one access network, the UE applies the ATSSS rules and considers local conditions for triggering the establishment or activation of the user plane resources over another access.

The type of a MA PDU Session may be one of the following types defined in clause 5.6.1: IPv4, IPv6, IPv4v6, and Ethernet. In this release of the specification, the Unstructured type is not supported. The clause 5.32.6.2.1 and the clause 5.32.6.3.1 below define what Steering Functionalities can be used for each supported type of a MA PDU Session.

The handling of 3GPP PS Data Off feature for MA PDU Session is specified in clause 5.24.

The ATSSS feature can be supported over any type of access network, including untrusted and trusted non-3GPP access networks (see clauses 4.2.8 and 5.5), wireline 5G access networks (see clause 4.2.8), etc., as long as a MA PDU Session can be established over this type of access network.

In this Release of the specification, a MA PDU Session using IPv6 multi-homing (see clause 5.6.4.3) or UL Classifier (see clause 5.6.4.2) is not specified.

In this Release of the specification, support for ATSSS assumes SMF Service Areas covering the whole PLMN or that a MA PDU Session is released over both accesses when the UE moves out of the SMF Service Area.

If the UE, due to mobility, moves from being served by a source AMF supporting ATSSS to a target AMF not supporting ATSSS, the MA PDU Session is released as described in TS 23.502 [3].

NOTE: Deployment of ATSSS that is homogeneous per PLMN or network slice enables consistent behavior. In the case of non-homogenous support of ATSSS in a PLMN/slice (i.e. some NFs in a PLMN/slice may not support ATSSS), MA PDU Sessions can be released due to UE mobility.

The following clauses specify the functionality that enables ATSSS.

5.32.2 Multi Access PDU Sessions

A Multi-Access PDU (MA PDU) Session is managed by using the session management functionality specified in clause 5.6, with the following additions and modifications:

- When the UE wants to request a new MA PDU Session:
  - If the UE is registered to the same PLMN over 3GPP and non-3GPP accesses, then the UE shall send a PDU Session Establishment Request over any of the two accesses. The UE also provides Request Type as "MA PDU Request" in the UL NAS Transport message. The AMF informs the SMF that the UE is registered over both accesses and this triggers the establishment of user-plane resources on both accesses and two N3/N9 tunnels between PSA and the RAN/AN.

- If the UE is registered to different PLMNs over 3GPP and non-3GPP accesses, then the UE shall send a PDU Session Establishment Request over one access. The UE also provides Request Type as "MA PDU Request" in the UL NAS Transport message. After this PDU Session is established with one N3/N9 tunnel between the PSA and (R)AN established, the UE shall send another PDU Session Establishment Request over the other access. The UE also provides the same PDU Session ID and Request Type as "MA PDU Request" in the UL NAS Transport message. Two N3/N9 tunnels and User-plane resources on both accesses are established.

- If the UE is registered over one access only, then the UE shall send a PDU Session Establishment Request over this access. The UE also provides Request Type as "MA PDU Request" in the UL NAS Transport message. One N3/N9 tunnel between the PSA and (R)AN and User-plane resources on this access only are established. After the UE is registered over the second access, the UE shall establish user-plane resources on the second access.

- In the PDU Session Establishment Request that is sent to request a new MA PDU Session, the UE shall provide also its ATSSS capabilities, which indicate the steering functionalities and the steering modes supported in the UE. These functionalities are defined in clause 5.32.6.

- If the UE indicates it is capable of supporting the ATSSS-LL functionality with any steering mode (as specified in clause 5.32.6.1) and the network accepts to activate this functionality, then the network may provide to UE Measurement Assistance Information (see details in clause 5.32.5) and shall provide to UE one or more ATSSS rules.

- If the UE indicates it is capable of supporting the MPTCP functionality with any steering mode and the ATSSS-LL functionality with only the Active-Standby steering mode (as specified in clause 5.32.6.1) and the network accepts to activate these functionalities, then the network provides MPTCP proxy information to UE, and allocates to UE one IP address/prefix for the MA PDU session (as defined in clause 5.8.2.2) and two additional IP addresses/prefixes, called "link-specific multipath" addresses. Further details are provided in clause 5.32.6.2. In addition, the network may provide to UE Measurement Assistance Information and shall provide to UE one or more ATSSS rules including an ATSSS rule for non-MPTCP traffic. The ATSSS rule for non-MPTCP traffic shall use the ATSSS-LL functionality and the Active-Standby Steering Mode to indicate how the non-MPTCP traffic shall be transferred across the 3GPP access and the non-3GPP access in the uplink direction.

- If the UE indicates it is capable of supporting the MPTCP functionality with any steering mode and the ATSSS-LL functionality with any steering mode (as specified in clause 5.32.6.1) and the network accepts to activate these functionalities, then the network provides MPTCP proxy information to UE, and allocates to UE one IP address/prefix for the MA PDU session (as defined in clause 5.8.2.2) and two additional IP addresses/prefixes, called "link-specific multipath" addresses. Further details are provided in clause 5.32.6.2. In addition, the network may provide to UE Measurement Assistance Information and shall provide to UE one or more ATSSS rules.

- If the UE requests an S-NSSAI, this S-NSSAI should be allowed on both accesses. Otherwise, the MA PDU Session shall not be established.

- The SMF determines the ATSSS capabilities supported for the MA PDU Session based on the ATSSS capabilities provided by the UE and per DNN configuration on SMF, as follows:

  a) If the UE includes in its ATSSS capabilities "MPTCP functionality with any steering mode and ATSSS-LL functionality with only Active-Standby steering mode" (as specified in clause 5.32.6.1), the DNN configuration allows both MPTCP and ATSSS-LL with any steering mode, including RTT measurement without using PMF protocol, the MA PDU Session is capable of (1) MPTCP and ATSSS-LL with any steering mode in the downlink, and (2) MPTCP and ATSSS-LL with Active-Standby mode in the uplink.

NOTE 1: In this case, it is assumed that ATSSS-LL with "Smallest Delay" steering mode is selected for the downlink only when the UPF can measure RTT without using the PMF protocol, e.g. by using other means not defined by 3GPP such as using the RTT measurements of MPTCP.

  b) If the UE includes in its ATSSS capabilities "MPTCP functionality with any steering mode and ATSSS-LL functionality with only Active-Standby steering mode" (as specified in clause 5.32.6.1), the DNN configuration allows both MPTCP and ATSSS-LL with any steering mode, but not RTT measurement without using PMF protocol, the MA PDU Session is capable of (1) MPTCP with any steering mode in the downlink (2) ATSSS-LL with any steering mode except Smallest Delay steering mode in the downlink, and (3) MPTCP and ATSSS-LL with Active-Standby mode in the uplink.

c) If the UE includes in its ATSSS capabilities "MPTCP functionality with any steering mode and ATSSS-LL functionality with only Active-Standby steering mode" (as specified in clause 5.32.6.1) and if the DNN configuration allows MPTCP with any steering mode and ATSSS-LL with only Active-Standby steering mode, the MA PDU Session is capable of MPTCP and ATSSS-LL with Active-Standby mode in the uplink and in the downlink.

d) If the UE includes in its ATSSS capabilities "ATSSS-LL functionality with any steering mode" (as specified in clause 5.32.6.1) and the DNN configuration allows ATSSS-LL with any steering mode, the MA PDU Session is capable of ATSSS-LL with any steering mode in the uplink and in the downlink.

e) If the UE includes in its ATSSS capabilities "MPTCP functionality with any steering mode and ATSSS-LL functionality with any steering mode" (as specified in clause 5.32.6.1), and the DNN configuration allows both MPTCP and ATSSS-LL with any steering mode, the MA PDU Session is capable of both MPTCP and ATSSS-LL with any steering mode in the uplink and in the downlink.

The SMF provides the ATSSS capabilities of the MA PDU Session to the PCF during PDU Session Establishment.

- The PCC rules provided by PCF include MA PDU Session Control information (see TS 23.503 [45]). They are used by SMF to derive ATSSS rules for the UE and N4 rules for the UPF. When dynamic PCC is not used for the MA PDU Session, the SMF shall provide ATSSS rules and N4 rules based on local configuration (e.g. based on DNN or S-NSSAI).

- The UE receives ATSSS rules from SMF, which indicate how the uplink traffic should be routed across 3GPP access and non-3GPP access. Similarly, the UPF receives N4 rules from SMF, which indicate how the downlink traffic should be routed across 3GPP access and non-3GPP access.

- When the SMF receives a PDU Session Establishment Request and a "MA PDU Request" indication and determines that UP security protection (see clause 5.10.3) is required for the PDU Session, the SMF shall only confirm the establishment of the MA PDU session if the 3GPP access network can enforce the required UP security protection. The SMF needs not confirm whether the non-3GPP access can enforce the required UP security protection.

- After the MA PDU Session establishment:

  - At any given time, the MA PDU session may have user-plane resources on both 3GPP and non-3GPP accesses, or on one access only, or may have no user-plane resources on any access.

  - The AMF, SMF, PCF and UPF maintain their MA PDU Session contexts, even when the UE deregisters from one access (but remains registered on the other access).

  - When the UE deregisters from one access (but remains registered on the other access), the AMF informs the SMF to release the resource of this access type in the UPF for the MA PDU Session. Subsequently, the SMF notifies the UPF that the access type has become unavailable and the N3/N9 tunnel for the access type are released.

  - If the UE wants to add user-plane resources on one access of the MA PDU Session, e.g. based on access network performance measurement and/or ATSSS rules, then the UE shall send a PDU Session Establishment Request over this access containing PDU Session ID of the MA PDU Session. The UE also provides Request Type as "MA PDU Request" and the same PDU Session ID in the UL NAS Transport message. If there is no N3/N9 tunnel for this access, the N3/N9 tunnel for this access is established.

  - If the UE wants to re-activate user-plane resources on one access of the MA PDU Session, e.g. based on access network performance measurement and/or ATSSS rules, then the UE shall initiate the UE Triggered Service Request procedure over this access.

  - If the network wants to re-activate the user-plane resources over 3GPP access or non-3GPP access of the MA PDU Session, the network shall initiate the Network Triggered Service Request procedure, as specified in TS 23.502 [3], clause 4.22.7.

A MA PDU Session may be established either:

a) when it is explicitly requested by an ATSSS-capable UE; or

b) when an ATSSS-capable UE requests a single-access PDU Session but the network decides to establish a MA PDU Session instead. This is an optional scenario specified in TS 23.502 [3], clause 4.22.3, which may occur when the UE requests a single-access PDU Session but no policy (e.g. no URSP rule) and no local restrictions in the UE mandate a single access for the PDU Session.

A MA PDU Session may be established during a PDU Session modification procedure when the UE moves from EPS to 5GS, as specified in TS 23.502 [3], clause 4.22.6.3.

The AMF indicates as part of the Registration procedure whether ATSSS is supported or not. When ATSSS is not supported, the UE shall not

- request establishment of a MA PDU Session (as described in clause 4.22.2 of TS 23.502 [3]); or
- request addition of User Plane resources for an existing MA PDU Session (as described in clause 4.22.7 of TS 23.502 [3]); or
- request establishment of a PDU Session with "MA PDU Network-Upgrade Allowed" indication (as described in clause 4.22.3 of TS 23.502 [3]); or
- request PDU Session Modification with Request Type of "MA PDU request" or with "MA PDU Network-Upgrade Allowed" indication after moving from EPC to 5GC (as described in clause 4.22.6.3 of TS 23.502 [3]).

An ATSSS-capable UE may decide to request a MA PDU Session based on the provisioned URSP rules. In particular, the UE should request a MA PDU Session when the UE applies a URSP rule, which triggers the UE to establish a new PDU Session and the Access Type Preference component of the URSP rule indicates "Multi-Access" (see TS 23.503 [45]).

5.32.3 Policy for ATSSS Control

If dynamic PCC is to be used for the MA PDU Session, the PCF may take ATSSS policy decisions and create PCC rules that contain MA PDU Session Control information, (as specified in TS 23.503 [45]), which determines how the uplink and the downlink traffic of the MA PDU Session should be distributed across the 3GPP and non-3GPP accesses. If dynamic PCC is not deployed, local policy in SMF is used.

The SMF receives the PCC rules with MA PDU Session Control information and maps these rules into (a) ATSSS rules, which are sent to the UE, and (b) N4 rules, which are sent to the UPF. The ATSSS rules are provided as a prioritized list of rules (see clause 5.32.8), which are applied by the UE to enforce the ATSSS policy in the uplink direction and the N4 Rules are applied by the UPF to enforce the ATSSS policy in the downlink direction.

The ATSSS rules are sent to UE with a NAS message when the MA PDU Session is created or updated by the SMF, e.g. after receiving updated/new PCC rules from the PCF. Similarly, the N4 rules are sent to UPF when the MA PDU Session is created or updated by the SMF.

The details of the policy control related to ATSSS are specified in TS 23.503 [45].

5.32.4 QoS Support

The 5G QoS model for the Single-Access PDU Session is also applied to the MA PDU Session, i.e. the QoS Flow is the finest granularity of QoS differentiation in the MA PDU Session. One difference compared to the Single-Access PDU Session is that in a MA PDU Session there can be separate user-plane tunnels between the AN and the PSA, each one associated with a different access. However, the QoS Flow is not associated with specific access, i.e. it is access agnostic, so the same QoS is supported when the traffic is distributed over 3GPP and non-3GPP accesses. The SMF shall provide the same QFI in 3GPP and non-3GPP accesses so that the same QoS is supported in both accesses.

A QoS Flow of the MA PDU Session may be either Non-GBR or GBR depending on its QoS profile.

For a Non-GBR QoS Flow, the SMF provides a QoS profile 5G-AN(s) during MA PDU Session Establishment or MA PDU Session Modification procedure:

- During MA PDU Session Establishment procedure, the QoS profile to both ANs if the UE is registered over both accesses.
- During MA PDU Session Modification procedure, the QoS profile is provided to the 5G-AN(s) over which the user plane resources are activated.

For a GBR QoS Flow, the SMF shall provide a QoS profile to a single access network as follows:

- If the PCC rule allows a GBR QoS Flow in a single access, the SMF provides the QoS profile for the GBR QoS Flow to the access network allowed by the PCC rule.

- If the PCC rule allows a GBR QoS Flow in both accesses, the SMF decides to which access network to provide the QoS profile for the GBR QoS Flow based on its local policy (e.g. the access where the traffic is ongoing according to the Multi Access Routing rules).

For a GBR QoS Flow, traffic splitting is not supported because the QoS profile is provided to a single access network at a given time. If the UPF determines that it cannot send GBR traffic over the current ongoing access e.g. based on the N4 rules and access availability and unavailability report from the UE as described in clause 5.32.5.3, the UPF shall send an Access Availability report to the SMF. Based on the report, the SMF decides whether to move GBR QoS Flows to the other access:

- if the PCC rule allows the GBR QoS Flows only on this access, the SMF shall release the resources for the GBR QoS Flow and report to the PCF about the removal of the PCC rule.

- if the corresponding PCC rule allows the GBR QoS Flow on both accesses and the other access is not available, the SMF shall release the resources for the GBR QoS Flow and report to the PCF about the removal of the PCC rule.

- if the PCC rule allows the GBR QoS Flow on both accesses and the other access is available, the SMF shall try to move the GBR QoS Flow to the other access. The SMF may trigger a PDU session modification procedure to provide the QoS profile to the other access and release the resources for the GBR QoS Flow in the current access.

    - If Notification Control parameter is not included in the PCC rule for the GBR QoS Flow and the other access does not accept the QoS profile, the SMF shall release the resources for the GBR QoS Flow and report to the PCF about the removal of the PCC rule.

    - if the Notification Control parameter is included in the PCC rule, the SMF shall notify the PCF that GFBR can no longer be guaranteed. After the other access accepts the QoS profile, the SMF shall notify the PCF that GFBR can again be guaranteed. If the other access does not accept the QoS profile, the SMF shall delete the GBR QoS Flow and report to the PCF about the removal of the PCC rule.

NOTE 1: The ATSSS rule for GBR QoS Flow only allows the UE to steer traffic over a single access so that network knows in which access the UE sends GBR traffic. If the network wants to move GBR QoS Flow to the other access, the network needs to update ATSSS rule of the UE.

When the MA PDU Session is established or when the MA PDU Session is modified, the SMF may provide QoS rule(s) to the UE via one access, which are applied by the UE as specified in clause 5.7.1.4. The QoS rule(s) provided by SMF via one access are commonly used for both 3GPP access and non-3GPP access, so the QoS classification is independent of ATSSS rules.

The derived QoS rule generated by Reflective QoS is applied independently of the access on which the RQI was received. When the MPTCP functionality is used in the UE, the UE shall use the IP address/prefix of the MA PDU Session and the final destination address to generate the derived QoS rule.

When MPTCP functionality is enabled for the MA PDU Session:

- any QoS rules or PDRs that apply to the MA PDU Session IP address/prefix and port also apply to the "link-specific multipath" addresses/prefixes and ports used by the UE to establish MPTCP subflows over 3GPP and non-3GPP accesses; and

- any QoS rules or PDRs that apply to the IP address/prefix and port of the final destination server in DN also apply to the IP address and port of the MPTCP proxy for corresponding MPTCP subflows that are terminated at the proxy.

NOTE 2: How these associations are made is left up to the UE and UPF implementations.

5.32.5 Access Network Performance Measurements

5.32.5.1 General principles

When an MA PDU Session is established, the network may provide the UE with Measurement Assistance Information. This information assists the UE in determining which measurements shall be performed over both accesses, as well as whether measurement reports need to be sent to the network.

Measurement Assistance Information shall include the addressing information of a Performance Measurement Function (PMF) in the UPF, the UE can send PMF protocol messages to:

- For a PDU Session of IP type, Measurement Assistance Information contains one IP address for the PMF, one UDP port associated with 3GPP access and another UDP port associated with non-3GPP access;
- For a PDU Session of Ethernet type, Measurement Assistance Information contains one MAC address associated with 3GPP access and another MAC address associated with non-3GPP access.

NOTE 1: To protect the PMF in the UPF (e.g. to block DDOS to the PMF), the IP addresses of the PMF are only accessible from the UE IP address via the N3/N9 interface.

NOTE 2: After the MA PDU Session is released, the same UE IP address/prefix is not allocated to another UE for MA PDU Session in a short time.

The addressing information of the PMF in the UPF is retrieved by the SMF from the UPF during N4 session establishment.

The following PMF protocol messages can be exchanged between the UE and the PMF:

- Messages to allow for Round Trip Time (RTT) measurements, i.e. when the "Smallest Delay" steering mode is used;
- Messages for reporting Access availability/unavailability by the UE to the UPF.

The PMF protocol is specified in TS 24.193 [109].

The PMF protocol messages exchanged between the UE and UPF shall use the QoS Flow associated with default QoS rule over the available access(es).

The QoS Flow associated with default QoS rule for MA PDU Session is Non-GBR QoS Flow.

The UE shall not apply the ATSSS rules and the UPF shall not apply the MAR rules for the PMF protocol messages.

When the UE requests a MA PDU session and indicates it is capable to support the MPTCP functionality with any steering mode and the ATSSS-LL functionality with only the Active-Standby steering mode (as specified in clause 5.32.6.1), the network may send Measurement Assistance Information for the UE to send Access availability/unavailability reports to the UPF. In this case, the UE and UPF shall not perform RTT measurements using PMF as the UE and UPF can use measurements available at the MPTCP layer.

5.32.5.2 Round Trip Time Measurements

RTT measurements can be conducted by the UE and UPF independently. There is no measurement reporting from one side to the other. RTT measurements are defined to support the "Smallest Delay" steering mode.

The estimation of the RTT by the UE and by the UPF is based on the following mechanism:

1. The PMF in the UE sends over the user plane PMF-Echo Request messages to the PMF in the UPF, and the PMF in the UPF responds to each one with a PMF-Echo Response message. Similarly, the PMF in the UPF sends over the user plane PMF-Echo Request messages to the PMF in the UE, and the PMF in the UE responds to each one with a PMF-Echo Response message.
2. In the case of a MA PDU Session of IP type:
    - The PMF in the UE sends PMF messages to the PMF in the UPF over UDP/IP. The destination IP address is the IP address contained in the Measurement Assistance Information and the destination UDP port is one of the two UDP ports contained in the Measurement Assistance Information. One UDP port is used for sending

PMF messages to UPF over 3GPP access and the other UDP port is used for sending PMF messages to UPF over non-3GPP access. The source IP address is the IP address assigned to UE for the MA PDU Session and the source UDP port is a UDP port that is dynamically allocated by the UE for PMF communication. This source UDP port in the UE remains the same for the entire lifetime of the MA PDU Session.

- The PMF in the UPF sends PMF messages to the PMF in the UE over UDP/IP. The source IP address is the same IP address as the one provided in the Measurement Assistance Information and the source UDP port is one of the two UDP ports as provided in the Measurement Assistance Information. One UDP port is used for sending PMF messages to UE over 3GPP access and the other UDP port is used for sending PMF messages to UE over the non-3GPP access. The destination IPv4 address is the IPv4 address assigned to UE for the MA PDU Session (if any) and the destination IPv6 address is an IPv6 address selected by the UE from the IPv6 prefix assigned for the MA PDU Session (if any). The destination UDP port is the dynamically allocated UDP port in the UE, which is contained in all PMF messages received from the UE. If the UE receives Measurement Assistance Information, the UE shall inform the network via the user plane about the UE's dynamically allocated UDP port, and the IPv6 address if IPv6 is used for PMF messages, so that it is possible for the UPF to know the UE's IPv6 address (if applicable) and dynamically allocated UDP port as soon as the MA PDU Session has been established.

3. In the case of a MA PDU Session of Ethernet type:

   - The PMF in the UE sends PMF messages to the PMF in the UPF over Ethernet. The Ethertype is the Ethertype contained in the Measurement Assistance Information and the destination MAC address is one of the two MAC addresses contained in the Measurement Assistance Information. One MAC address is used for sending PMF messages to UPF over 3GPP access and the other MAC address is used for sending PMF messages to UPF over non-3GPP access. The source MAC address is a MAC address of the UE, which remains the same for the entire lifetime of the MA PDU Session.

   - The PMF in the UPF sends PMF messages to the PMF in the UE over Ethernet. The Ethertype is the same Ethertype as the one provided in the Measurement Assistance Information and the source MAC address is one of the two MAC addresses as provided in the Measurement Assistance Information. One MAC address is used for sending PMF messages to UE over 3GPP access and the other MAC address is used for sending PMF messages to UE over non-3GPP access. The destination MAC address is the MAC address of the UE, which is contained in all PMF messages received from the UE. If the UE receives Measurement Assistance Information, the UE shall inform the network via the user plane about the UE's MAC address so that it is possible for the UPF to know the UE's MAC address as soon as the MA PDU Session has been established.

4. When the UP connection of the MA PDU session is deactivated on an access, no PMF-Echo Request messages are sent on this access. The PMF in the UPF shall not send PMF-Echo Request on this access if the UP connection is not available or after it receives notification from the (H-)SMF to stop sending the PMF-Echo Request on this access.

5. The UE and the UPF derive an estimation of the average RTT over an access type by averaging the RTT measurements obtained over this access.

5.32.5.3 Access Availability/Unavailability Report

If required by the network in the Measurement Assistance Information, the UE shall provide access availability/unavailability reports to the network. How the UE detects the unavailability and the availability of an access is based on implementation. When the UE detects the unavailability/availability of an access, it shall:

- build a PMF-Access Report containing the access type and an indication of availability/unavailability of this access;

- send the PMF-Access Report to the UPF via the user plane.

The UPF shall acknowledge the PMF-Access Report received from the UE.

5.32.5.4 Protocol stack for user plane measurements and measurement reports

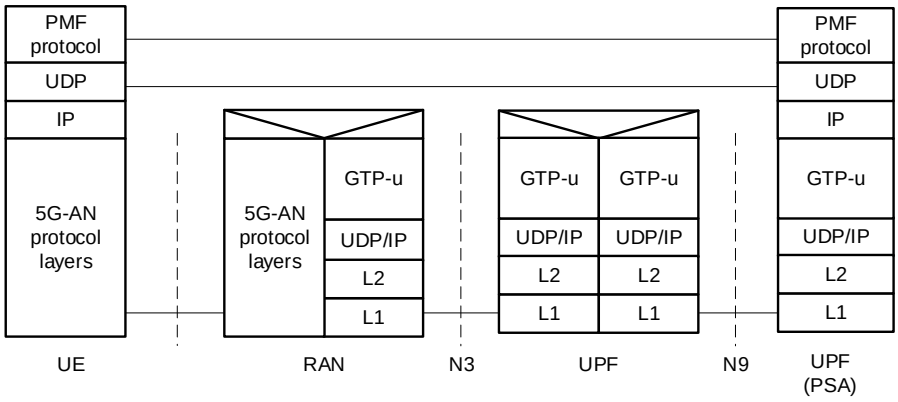


Figure 5.32.5.4-1: UE/UPF measurements related protocol stack for 3GPP access and for an MA PDU Session with type IP

In the case of an MA PDU Session with type Ethernet, the protocol stack over 3GPP access is that same as the one in the above figure, but the PMF protocol operates on top of Ethernet, instead of UDP/IP.

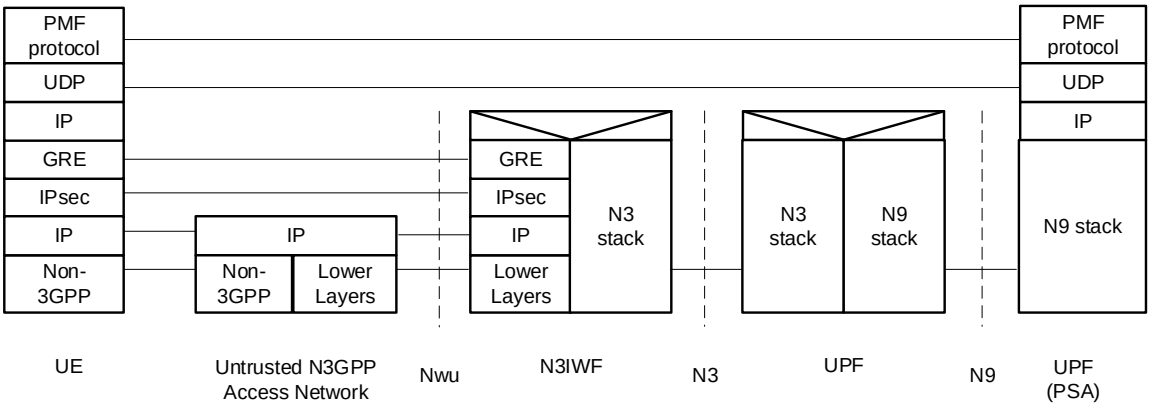


Figure 5.32.5.4-2: UE/UPF measurements related protocol stack for non-3GPP access and for an MA PDU Session with type IP

In the case of an MA PDU Session with type Ethernet, the protocol stack over non-3GPP access is that same as the one in the above figure, but the PMF protocol operates on top of Ethernet, instead of UDP/IP.

5.32.6 Support of Steering Functionalities

5.32.6.1 General

The functionality in an ATSSS-capable UE that can steer, switch and split the MA PDU Session traffic across 3GPP access and non-3GPP access, is called a "steering functionality". An ATSSS-capable UE may support one or more of the following types of steering functionalities:

- High-layer steering functionalities, which operate above the IP layer:
  - In this release of the specification, only one high-layer steering functionality is specified, which applies the MPTCP protocol (IETF RFC 8684 [81]) and is called "MPTCP functionality" (see clause 5.32.6.2.1). This steering functionality can be applied to steer, switch and split the TCP traffic of applications allowed to use MPTCP. The MPTCP functionality in the UE may communicate with an associated MPTCP Proxy functionality in the UPF, by using the MPTCP protocol over the 3GPP and/or the non-3GPP user plane.
- Low-layer steering functionalities, which operate below the IP layer:

- One type of low-layer steering functionality defined in the present document is called "ATSSS Low-Layer functionality", or ATSSS-LL functionality (see clause 5.32.6.3.1). This steering functionality can be applied to steer, switch and split all types of traffic, including TCP traffic, UDP traffic, Ethernet traffic, etc. ATSSS-LL functionality is mandatory for MA PDU Session of type Ethernet. In the network, there shall be in the data path of the MA PDU session one UPF supporting ATSSS-LL.

NOTE: Filters used in ATSSS rules related with a MA PDU Session of type Ethernet can refer to IP level parameters such as IP addresses and TCP/UDP ports.

The UE indicates to the network its supported steering functionalities and steering modes by including in the UE ATSSS Capability one of the following:

1) ATSSS-LL functionality with any steering mode.

   In this case, the UE indicates that it is capable to steer, switch and split all traffic of the MA PDU Session by using the ATSSS-LL functionality with any steering mode specified in clause 5.32.8.

2) MPTCP functionality with any steering mode and ATSSS-LL functionality with only Active-Standby steering mode.

   In this case, the UE indicates that:

   a) it is capable to steer, switch and split the MPTCP traffic of the MA PDU Session by using the MPTCP functionality with any steering mode specified in clause 5.32.8; and

   b) it is capable to steer and switch all other traffic (i.e. the non-MPTCP traffic) of the MA PDU Session by using the ATSSS-LL functionality with the Active-Standby steering mode specified in clause 5.32.8.

3) MPTCP functionality with any steering mode and ATSSS-LL functionality with any steering mode.

   In this case, the UE indicates that:

   a) it is capable to steer, switch and split the MPTCP traffic of the MA PDU Session by using the MPTCP functionality with any steering mode specified in clause 5.32.8; and

   b) it is capable to steer, switch and split all other traffic (i.e. the non-MPTCP traffic) of the MA PDU Session by using the ATSSS-LL functionality with any steering mode specified in clause 5.32.8.

The above steering functionalities are schematically illustrated in the Figure 5.32.6.1-1, which shows an example model for an ATSSS-capable UE supporting the MPTCP functionality and the ATSSS-LL functionality. The MPTCP flows in this figure represent the traffic of the applications for which MPTCP can be applied. The three different IP addresses illustrated in the UE are further described in clause 5.32.6.2.1. The "Low-Layer" in this figure contains functionality that operates below the IP layer (e.g. different network interfaces in the UE), while the "High-Layer" contains functionality that operates above the IP layer.

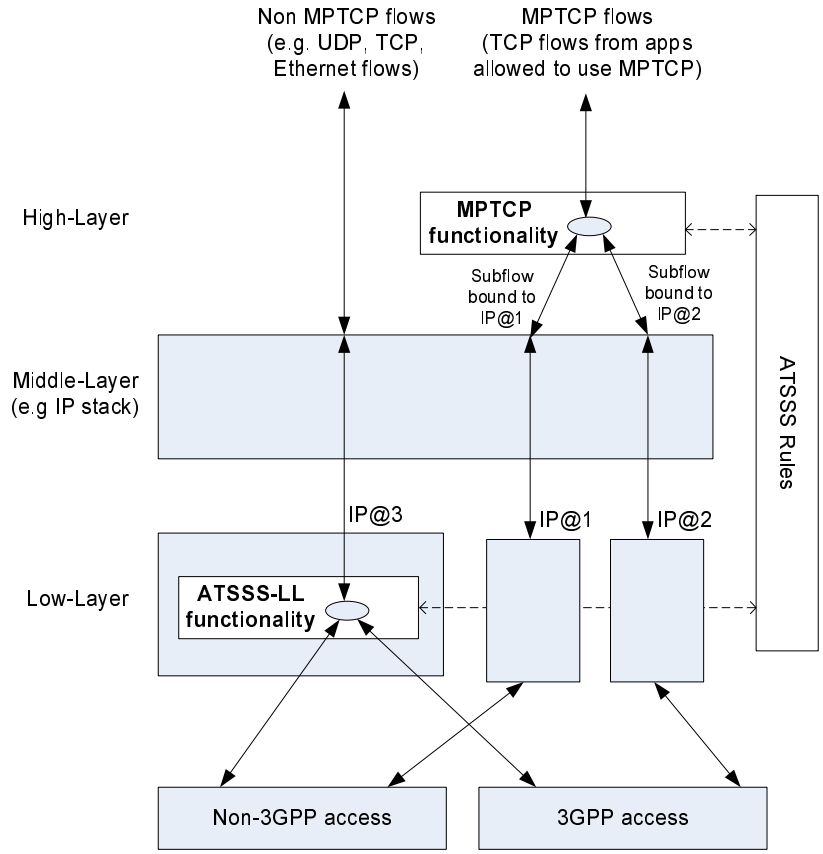


Figure 5.32.6.1-1: Steering functionalities in an example UE model

Within the same MA PDU Session in the UE, it is possible to steer the MPTCP flows by using the MPTCP functionality and, simultaneously, to steer all other flows by using the ATSSS-LL functionality. For the same packet flow, only one steering functionality shall be used.

All steering functionalities in the UE shall take ATSSS decisions (i.e. decide how to steer, switch and split the traffic) by using the same set of ATSSS rules. Similarly, all ATSSS decisions in the UPF shall be taken by applying the same set of N4 rules, which support ATSSS. The ATSSS rules and the N4 rules supporting ATSSS are provisioned in the UE and in the UPF respectively, when the MA PDU Session is established.

If the UE supports both the MPTCP functionality and the ATSSS-LL functionality, it shall use the provisioned ATSSS rules (see TS 23.503 [45]) to decide which steering functionality to apply for a specific packet flow.

5.32.6.2 High-Layer Steering Functionalities

5.32.6.2.1 MPTCP Functionality

As mentioned in clause 5.32.6.1, the MPTCP functionality in the UE applies the MPTCP protocol (IETF RFC 8684 [81]) and the provisioned ATSSS rules for performing access traffic steering, switching and splitting. The MPTCP functionality in the UE may communicate with the MPTCP Proxy functionality in the UPF using the user plane of the 3GPP access, or the non-3GPP access, or both.

The MPTCP functionality may be enabled in the UE when the UE provides an "MPTCP capability" during PDU Session Establishment procedure.

The network shall not enable the MPTCP functionality when the type of the MA PDU Session is Ethernet.

If the UE indicates it is capable of supporting the MPTCP functionality, as described in clause 5.32.2, and the network agrees to enable the MPTCP functionality for the MA PDU Session then:

i) An associated MPTCP Proxy functionality is enabled in the UPF for the MA PDU Session by MPTCP functionality indication received in the Multi-Access Rules (MAR).

ii) The network allocates to UE one IP address/prefix for the MA PDU Session and two additional IP addresses/prefixes, called "link-specific multipath" addresses/prefixes; one associated with 3GPP access and another associated with the non-3GPP access. In the UE, these two IP addresses/prefixes are used only by the MPTCP functionality. Each "link-specific multipath" address/prefix assigned to UE may not be routable via N6. The MPTCP functionality in the UE and the MPTCP Proxy functionality in the UPF shall use the "link-specific multipath" addresses/prefixes for subflows over non-3GPP access and over 3GPP access and MPTCP Proxy functionality shall use the IP address/prefix of the MA PDU session for the communication with the final destination. In Figure 5.32.6.1-1, the IP@3 corresponds to the IP address of the MA PDU Session and the IP@1 and IP@2 correspond to the "link-specific multipath" IP addresses. The following UE IP address management applies:

   - The MA PDU IP address/prefix shall be provided to the UE via mechanisms defined in clause 5.8.2.2.

   - The "link-specific multipath" IP addresses/prefixes shall be allocated by the UPF and shall be provided to the UE via SM NAS signalling.

NOTE 1: After the MA PDU Session is released, the same UE IP addresses/prefixes is not allocated to another UE for MA PDU Session in a short time.

NOTE 2: The act of the UPF performing translation on traffic associated with the "link-specific multipath" addresses to/from the MA PDU session IP address can lead to TCP port collision and exhaustion. The port collision can potentially occur because the UE also uses the MA PDU session IP address for non-MPTCP traffic, and this causes the port namespace of such address to be owned simultaneously by the UE and UPF. In addition, the port exhaustion can potentially occur when the UE creates a large number of flows, because multiple IP addresses used by the UE are mapped to a single MA PDU session IP address on the UPF. The UPF needs to consider these problems based on the UPF implementation, and avoid them by, for example, using additional N6-routable IP addresses for traffic associated to the link-specific multipath addresses/prefixes. How this is done is left to the implementation.

iii) The network shall send MPTCP proxy information to UE, i.e. the IP address, a port number and the type of the MPTCP proxy. The following type of MPTCP proxy shall be supported in this release:

   - Type 1: Transport Converter, as defined in draft-ietf-tcpm-converters-14 [82].

     The MPTCP proxy information is retrieved by the SMF from the UPF during N4 session establishment.

     The UE shall support the client extensions specified in draft-ietf-tcpm-converters-14 [82].

iv) The network may indicate to UE the list of applications for which the MPTCP functionality should be applied. This is achieved by using the Steering Functionality component of an ATSSS rule (see clause 5.32.8).

NOTE 3: To protect the MPTCP proxy function (e.g. to block DDOS to the MPTCP proxy function), the IP addresses of the MPTCP Proxy Function are only accessible from the two "link-specific multipath" IP addresses of the UE via the N3/N9 interface.

v) When the UE indicates it is capable of supporting the MPTCP functionality with any steering mode and the ATSSS-LL functionality with only the Active-Standby steering mode (as specified in clause 5.32.6.1) and these functionalities are enabled for the MA PDU Session, then the UE shall route via the MA PDU Session the TCP traffic of applications for which the MPTCP functionality should be applied (i.e. the MPTCP traffic), as defined in bullet iv. The UE may route all other traffic (i.e. the non-MPTCP traffic) via the MA PDU Session, but this type of traffic shall be routed on one of 3GPP access or non-3GPP access, based on the received ATSSS rule for non-MPTCP traffic (see clause 5.32.2). The UPF shall route all other traffic (i.e. non-MPTCP traffic) based on the N4 rules provided by the SMF. This may include N4 rules for ATSSS-LL, using any steering mode as instructed by the N4 rules.

5.32.6.3 Low-Layer Steering Functionalities

5.32.6.3.1 ATSSS-LL Functionality

The ATSSS-LL functionality in the UE does not apply a specific protocol. It is a data switching function, which decides how to steer, switch and split the uplink traffic across 3GPP and non-3GPP accesses, based on the provisioned ATSSS rules and local conditions (e.g. signal loss conditions). The ATSSS-LL functionality in the UE may be applied to steer, switch and split all types of traffic, including TCP traffic, UDP traffic, Ethernet traffic, etc.

The ATSSS-LL functionality may be enabled in the UE when the UE provides an "ATSSS-LL capability" during the PDU Session Establishment procedure.

The ATSSS-LL functionality is mandatory in the UE for MA PDU Session of type Ethernet. When the UE does not support the MPTCP functionality, the ATSSS-LL functionality is mandatory in the UE for an MA PDU Session of type IP. When the UE supports the MPTCP functionality, the ATSSS-LL functionality with Active-Standby Steering Mode is mandatory in the UE for an MA PDU Session of type IP to support non-MPTCP traffic.

The network shall also support the ATSSS-LL functionality as defined for the UE. The ATSSS-LL functionality in the UPF is enabled for a MA PDU Session by ATSSS-LL functionality indication received in the Multi-Access Rules (MAR).

5.32.7 Interworking with EPS

5.32.7.1 General

Multi-access connectivity using ATSSS via EPC only is not supported. Multi-access connectivity using ATSSS via both EPC and 5GC may be supported as defined in TS 23.316 [84] for the scenario with 5G-RG.

Interworking for MA PDU Session, if allowed by the network, is based on the interworking functionality specified in clause 5.17.2, with the differences and clarifications described in the following clauses.

A PDN Connection in EPS may be modified into a MA PDU Session when transferred to 5GS if the UE and the PGW-C+SMF support the ATSSS feature.

5.32.7.2 Interworking with N26 Interface

Interworking with N26 interface is based on clause 5.17.2.2, with the following differences and clarifications:

- When the UE is registered to the same PLMN over 3GPP and non-3GPP accesses, and the UE request a new MA PDU Session via non-3GPP access, the AMF also includes the indication of interworking with N26 to SMF.
- The SMF does not request EBI allocation when MA PDU Session is established only over non-3GPP access. If MA PDU Session is released over 3GPP access, the allocated EBI(s) for the MA PDU Session is revoked by the SMF as described in TS 23.502 [3] clause 4.11.1.4.3.
- The SMF does not request EBI allocation for GBR QoS Flow if the GBR QoS Flow is only allowed over non-3GPP access.
- When UE moves from 5GS to EPS, for both idle mode and connected mode mobility, if the MA PDU Session is moved to EPS as a PDN connection, the SMF triggers PDU Session Release procedure to release the MA PDU Session over Non-3GPP access in 5GS. UE and SMF remove ATSSS related contexts e.g. ATSSS rules, Measurement Assistance Information.
- When UE moves from 5GS to EPS, for both idle mode and connected mode mobility, if the MA PDU Session is not moved to EPS as a PDN connection, the 3GPP access of this MA PDU session becomes unavailable and the AMF notifies the SMF. In turn, the SMF may decide to move the traffic to Non-3GPP access of the MA PDU session, if it is available. When UE moves back from EPS to 5GS, after the UE is registered over the 3GPP, the UE may add user-plane resources over the 3GPP access to the MA PDU session by triggering PDU Session Establishment procedure as specified in clause 5.32.2.
- After UE moves from EPS to 5GS, for both idle mode and connected mode mobility, if the UE requires MA PDU session, or if no policy in the UE (e.g. no URSP rule) and no local restrictions mandate a single access for the PDU Session, UE triggers the PDU Session Modification procedure as described in clause 4.22.6.3 in TS 23.502 [3] to provide the ATSSS Capability to PGW-C+SMF. The PGW-C+SMF may determine whether to modify this PDU Session to a MA PDU Session in 5GS, e.g. based on PGW-C+SMF and UE's ATSSS Capability, subscription data and local policy. If dynamic PCC is to be used for the MA PDU Session, the PCF decides whether the MA PDU session is allowed or not based on operator policy and subscription data. If the MA PDU Session is allowed, the SMF provides ATSSS rule(s) and Measurement Assistance Information to the UE. If the UE receives ATSSS rules and is not registered to non-3GPP access, the UE establishes the second user-plane over non-3GPP access after the UE is registered to non-3GPP access. If UE was registered to non-3GPP access in 5GS, the UP resources over non-3GPP access are also established by the SMF using the PDU Session Modification procedure.

5.32.7.3 Interworking without N26 Interface

Interworking without N26 interface is based on clause 5.17.2.3, with the following differences and clarifications:

- After UE moves from 5GS to EPS, UE may sends a PDN Connectivity Request with "handover" indication to transfer the MA PDU Session to EPS. Then PGW-C+SMF triggers to release MA PDU in 5GS. If UE does not transfer the MA PDU Session to EPS, UE keeps the MA PDU Session in 5GS. In this case, UE may report to UPF that 3GPP access is unavailable, all MA PDU Session traffic is transported over N3GPP access. Later, if UE returns to 5GS, UE may report the 3GPP access availability to UPF.

- After UE moves from EPS to 5GS, UE may trigger PDU Session Establishment procedure to transfer the PDN Connection to 5GS. During the PDU Session Establishment procedure, UE may request to establish a MA PDU Session by including "MA PDU Request" or, if no policy in the UE (e.g. no URSP rule) and no local restrictions mandate a single access for the PDU Session, the UE may include the "MA PDU Network-Upgrade Allowed" indication.

5.32.8 ATSSS Rules

As specified in clause 5.32.3, after the establishment of a MA PDU Session, the UE receives a prioritized list of ATSSS rules from the SMF. The structure of an ATSSS rule is specified in Table 5.32.8-1.

Table 5.32.8-1: Structure of ATSSS Rule

Information name	Description	Category	SMF permitted to modify in a PDU context	Scope
Rule Precedence	Determines the order in which the ATSSS rule is evaluated in the UE.	Mandatory (NOTE 1)	Yes	PDU context
Traffic Descriptor	*This part defines the Traffic descriptor components for the ATSSS rule.*	Mandatory (NOTE 2)		
Application descriptors	One or more application identities that identify the application(s) generating the traffic (NOTE 3).	Optional	Yes	PDU context
IP descriptors (NOTE 4)	One or more 5-tuples that identify the destination of IP traffic.	Optional	Yes	PDU context
Non-IP descriptors (NOTE 4)	One or more descriptors that identify the destination of non-IP traffic, i.e. of Ethernet traffic.	Optional	Yes	PDU context
Access Selection Descriptor	*This part defines the Access Selection Descriptor components for the ATSSS rule.*	Mandatory		
Steering Mode	Identifies the steering mode that should be applied for the matching traffic.	Mandatory	Yes	PDU context
Steering Functionality	Identifies whether the MPTCP functionality or the ATSSS-LL functionality should be applied for the matching traffic.	Optional (NOTE 5)	Yes	PDU context
NOTE 1: Each ATSSS rule has a different precedence value from the other ATSSS rules. NOTE 2: At least one of the Traffic Descriptor components is present. NOTE 3: An application identity consists of an OSId and an OSAppId. NOTE 4: An ATSSS rule cannot contain both IP descriptors and Non-IP descriptors. NOTE 5: If the UE supports only one Steering Functionality, this component is omitted.				

The UE evaluates the ATSSS rules in priority order.

Each ATSSS rule contains a Traffic Descriptor (containing one or more components described in Table 5.32.8-1) that determines when the rule is applicable. An ATSSS rule is determined to be applicable when every component in the Traffic Descriptor matches the considered service data flow (SDF).

Depending on the type of the MA PDU Session, the Traffic Descriptor may contain the following components (the details of the Traffic Descriptor generation are described in clause 5.32.3):

- For IPv4, or IPv6, or IPv4v6 type: Application descriptors and/or IP descriptors.
- For Ethernet type: Application descriptors and/or Non-IP descriptors.

One ATSSS rule with a "match all" Traffic Descriptor may be provided, which matches all SDFs. When provided, it shall have the least Rule Precedence value, so it shall be the last one evaluated by the UE.

NOTE 1: The format of the "match all" Traffic descriptor of an ATSSS rule is defined in stage-3.

Each ATSSS rule contains an Access Selection Descriptor that contains the following components:

- A Steering Mode, which determines how the traffic of the matching SDF should be distributed across 3GPP and non-3GPP accesses. The following Steering Modes are supported:
  - Active-Standby: It is used to steer a SDF on one access (the Active access), when this access is available, and to switch the SDF to the available other access (the Standby access), when Active access becomes unavailable. When the Active access becomes available again, the SDF is switched back to this access. If the Standby access is not defined, then the SDF is only allowed on the Active access and cannot be transferred on another access.
  - Smallest Delay: It is used to steer a SDF to the access that is determined to have the smallest Round-Trip Time (RTT). As defined in clause 5.32.5, measurements may be obtained by the UE and UPF to determine the RTT over 3GPP access and over non-3GPP access. In addition, if one access becomes unavailable, all SDF traffic is switched to the other available access. It can only be used for the non-GBR SDF.
  - Load-Balancing: It is used to split a SDF across both accesses if both accesses are available. It contains the percentage of the SDF traffic that should be sent over 3GPP access and over non-3GPP access. Load-Balancing is only applicable to non-GBR SDF. In addition, if one access becomes unavailable, all SDF traffic is switched to the other available access, as if the percentage of the SDF traffic transported via the available access was 100%.
  - Priority-based: It is used to steer all the traffic of an SDF to the high priority access, until this access is determined to be congested. In this case, the traffic of the SDF is sent also to the low priority access, i.e. the SDF traffic is split over the two accesses. In addition, when the high priority access becomes unavailable, all SDF traffic is switched to the low priority access. How UE and UPF determine when a congestion occurs on an access is implementation dependent. It can only be used for the non-GBR SDF.
- A Steering Functionality, which identifies whether the MPTCP functionality or the ATSSS-LL functionality should be used to steer the traffic of the matching SDF. This is used when the UE supports multiple functionalities for ATSSS, as specified in clause 5.32.6 ("Support of Steering Functions").

NOTE 2: There is no need to update the ATSSS rules when one access becomes unavailable or available.

As an example, the following ATSSS rules could be provided to UE:

a) "Traffic Descriptor: UDP, DestAddr 1.2.3.4", "Steering Mode: Active-Standby, Active=3GPP, Standby=non-3GPP":
   - This rule means "steer UDP traffic with destination IP address 1.2.3.4 to the active access (3GPP), if available. If the active access is not available, use the standby access (non-3GPP)".

b) "Traffic Descriptor: TCP, DestPort 8080", "Steering Mode: Smallest Delay":
   - This rule means "steer TCP traffic with destination port 8080 to the access with the smallest delay". The UE needs to measure the RTT over both accesses, in order to determine which access has the smallest delay.

c) "Traffic Descriptor: Application-1", "Steering Mode: Load-Balancing, 3GPP=20%, non-3GPP=80%", "Steering Functionality: MPTCP":
   - This rule means "send 20% of the traffic of Application-1 to 3GPP access and 80% to non-3GPP access by using the MPTCP functionality".

5.33 Support for Ultra Reliable Low Latency Communication

5.33.1 General

The following features described in 5.33 may be used to enhance 5GS to support Ultra Reliable Low Latency Communication (URLLC):

- Redundant transmission for high reliability communication.

In this Release, URLLC applies to 3GPP access only.

When a PDU Session is to serve URLLC QoS Flow, the UE and SMF should establish the PDU Session as always-on PDU Session as described in clause 5.6.13.

NOTE 1: How the UE knows whether a PDU Session is to serve a URLLC QoS Flow when triggering PDU Session establishment is up to UE implementation.

NOTE 2: No additional functionality is specified for URLLC in order to support Home Routed roaming scenario in this Release.

5.33.2 Redundant transmission for high reliability communication

5.33.2.1 Dual Connectivity based end to end Redundant User Plane Paths

In order to support highly reliable URLLC services, a UE may set up two redundant PDU Sessions over the 5G network, such that the 5GS sets up the user plane paths of the two redundant PDU Sessions to be disjoint. The user's subscription indicates if user is allowed to have redundant PDU Sessions and this indication is provided to SMF from UDM.

NOTE 1: It is out of scope of 3GPP how to make use of the duplicate paths for redundant traffic delivery end-to-end. It is possible to rely on upper layer protocols, such as the IEEE TSN (Time Sensitive Networking) FRER (Frame Replication and Elimination for Reliability) [83], to manage the replication and elimination of redundant packets/frames over the duplicate paths which can span both the 3GPP segments and possibly fixed network segments as well.

NOTE 2: The following redundant network deployment aspects are within the responsibility of the operator and are not subject to 3GPP standardization:

- RAN supports dual connectivity, and there is sufficient RAN coverage for dual connectivity in the target area.
- UEs support dual connectivity.
- The core network UPF deployment is aligned with RAN deployment and supports redundant user plane paths.
- The underlying transport topology is aligned with the RAN and UPF deployment and supports redundant user plane paths.
- The physical network topology and geographical distribution of functions also supports the redundant user plane paths to the extent deemed necessary by the operator.
- The operation of the redundant user plane paths is made sufficiently independent, to the extent deemed necessary by the operator, e.g. independent power supplies.

Figure 5.33.2.1-1 illustrates an example user plane resource configuration of dual PDU sessions when redundancy is applied. One PDU Session spans from the UE via Master NG-RAN to UPF1 acting as the PDU Session Anchor, and the other PDU Session spans from the UE via Secondary NG-RAN to UPF2 acting as the PDU Session Anchor. As described in TS 37.340 [31], NG-RAN may realize redundant user plane resources for the two PDU sessions with two NG-RAN nodes (i.e. Master NG-RAN and Secondary NG-RAN as shown in Figure 5.33.2.1-1) or a single NG-RAN node. In both cases, there is a single N1 interface towards AMF.

Based on these two PDU Sessions, two independent user plane paths are set up. UPF1 and UPF2 connect to the same Data Network (DN), even though the traffic via UPF1 and UPF2 may be routed via different user plane nodes within the DN.

In order to establish two redundant PDU sessions and associate the duplicated traffic coming from the same application to these PDU sessions, URSP or UE local configuration is used as specified in TS 23.503 [45].

NOTE 3: Using URSP, duplicated traffic from the application, associated to the redundant PDU Sessions, is differentiated by two distinct traffic descriptors, each in a distinct URSP rule. These traffic descriptors need to have different DNNs, IP descriptors or non-IP descriptors (e.g. MAC address, VLAN ID), so that the two redundant PDU sessions are matched to the Route Selection Descriptors of distinct URSP rules.

The redundant user plane set up applies to both IP and Ethernet PDU Sessions.

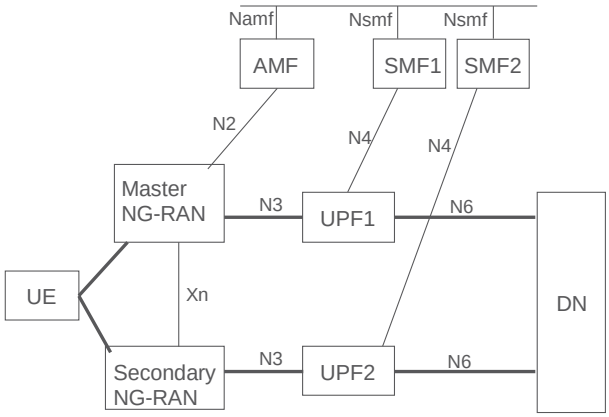


Figure 5.33.2.1-1: Example scenario for end to end redundant User Plane paths using Dual Connectivity

Support of redundant PDU Sessions include:

- UE initiates two redundant PDU Session and provides different combination of DNN and S-NSSAI for each PDU Session.

- The SMF determines whether the PDU Session is to be handled redundantly. The determination is based on the policies provided by PCF for the PDU Session, combination of the S-NSSAI, DNN, user subscription and local policy configuration. The SMF uses these inputs to determine the RSN which differentiates the PDU Sessions that are handled redundantly and indicates redundant user plane requirements for the PDU Sessions in NG-RAN.

- Operator configuration of UPF selection ensures the appropriate UPF selection for disjoint paths.

- At establishment of the PDU Sessions or at transitions to CM-CONNECTED state, the RSN parameter indicates to NG-RAN that redundant user plane resources shall be provided for the given PDU sessions by means of dual connectivity. The value of the RSN parameter indicates redundant user plane requirements for the PDU Sessions. This request for redundant handling is made by indicating the RSN to the NG-RAN node on a per PDU Session granularity. PDU Sessions associated with different RSN values shall be realized by different, redundant UP resources. Based on the RSN and RAN configuration, the NG-RAN sets up dual connectivity as defined in TS 37.340 [31] so that the sessions have end to end redundant paths. When there are multiple PDU Sessions with the RSN parameter set and with different values of RSN, this indicates to NG-RAN that CN is requesting dual connectivity to be set up and the user plane shall be handled as indicated by the RSN parameter and the associated RAN configuration. If the RSN value is provided to the NG-RAN, NG-RAN shall consider the RSN value when it associates the PDU Sessions with NG-RAN UP.

NOTE 4: The decision to set up dual connectivity remains in NG-RAN as defined today. NG-RAN takes into account the additional request for the dual connectivity setup provided by the CN.

- Using NG-RAN local configuration, NG-RAN determines whether the request to establish RAN resources for a PDU Session is fulfilled or not considering user plane requirements indicated by the RSN parameter by means of dual connectivity. If the request to establish RAN resources for PDU Session can be fulfilled by the RAN, the

PDU Session is established even if the user plane requirements indicated by RSN cannot be satisfied. If the NG-RAN determines the request to establish RAN resources cannot be fulfilled then it shall reject the request which eventually triggers the SMF to reject the PDU Session establishment towards the UE. The decision for each PDU Session is taken independently (i.e. rejection of a PDU Session request shall not release the previously established PDU Session). The RAN shall determine whether to notify the SMF if the RAN resources indicated by the RSN parameter can no longer be maintained and SMF can use that to determine if the PDU Session should be released.

- In the case of Ethernet PDU Sessions, the SMF has the possibility to change the UPF (acting as the PSA) and select a new UPF based on the identity of the Secondary NG-RAN for the second PDU Session if the Secondary NG-RAN is modified (or added/released), using the Ethernet PDU Session Anchor Relocation procedure described in clause 4.3.5.8 of TS 23.502 [3].
- The SMF's charging record may reflect the RSN information.
- The RSN indication is transferred from Source NG-RAN to Target NG-RAN in the case of handover.

5.33.2.2 Support of redundant transmission on N3/N9 interfaces

If the reliability of NG-RAN node, UPF and CP NFs are high enough to fulfil the reliability requirement of URLLC services served by these NFs, but the reliability of single N3 tunnel is considered not high enough, e.g. due to the deployment environment of backhaul network, the redundant transmission may be deployed between PSA UPF and NG-RAN via two independent N3 tunnels, which are associated with a single PDU Session, over different transport layer path to enhance the reliability.

To ensure the two N3 tunnels are transferred via disjointed transport layer paths, the SMF or PSA UPF should provide different routing information in the tunnel information (e.g. different IP addresses or different Network Instances), and these routing information should be mapped to disjoint transport layer paths according to network deployment configuration. The SMF indicates NG-RAN and PSA UPF that one of the two CN/AN Tunnel Info is used as the redundancy tunnel of the PDU Session accordingly. The redundant transmission using the two N3/N9 tunnels are performed at QoS flow granularity and are sharing the same QoS Flow ID.

During or after a URLLC QoS flow establishment, if the SMF decided that redundant transmission shall be performed based on authorized 5QI, NG-RAN node capability and/or operator configuration, the SMF informs the PSA UPF and NG-RAN to perform redundant transmission via N4 interface and N2 information accordingly. In this case, NG-RAN should also provide different routing information in the tunnel information (e.g. different IP addresses), and these routing information should be mapped to disjoint transport layer paths according to network deployment configuration.

NOTE 1: The NG-RAN node capability to support the redundant transmission on N3/N9 can be configured in the SMF per network slice or per SMF service area.

If duplication transmission is performed on N3/N9 interface, for each downlink packet of the QoS Flow the PSA UPF received from DN, the PSA UPF replicates the packet and assigns the same GTP-U sequence number to them for the redundant transmission. The NG-RAN eliminates the duplicated packets based on the GTP-U sequence number and then forwards the PDU to the UE.

For each uplink packet of the QoS Flow the NG-RAN received from UE, the NG-RAN replicates the packet and assigns the same GTP-U sequence number to them for redundant transmission. These packets are transmitted to the PSA UPF via two N3 Tunnels separately. The PSA UPF eliminates the duplicated packet based on the GTP-U sequence number accordingly.

NOTE 2: How to realize the sequence number for support of GTP-U duplication over N3/N9 is up to stage 3.

NOTE 3: For redundant transmission on N3/N9 interfaces, reordering is not required on the receiver side.

The PSA UPF and NG-RAN may transmit packets via one or both of the tunnels per QoS Flow based on SMF instruction.

NOTE 4: The AMF selects an SMF supporting redundant transmission based on the requested S-NSSAI and/or DNN.

During UE mobility, when the UE moves from NG-RAN supporting redundant transmission to NG-RAN not supporting redundant transmission, the SMF may release the QoS flow which are subject to redundant transmission.

Figure 5.33.2.2-1 illustrates the case that the redundant transmission is performed only on N3 interface. These packets are transmitted to the NG-RAN via two N3 Tunnels separately. The RAN node and PSA UPF shall support the packet replication and elimination function as described above.

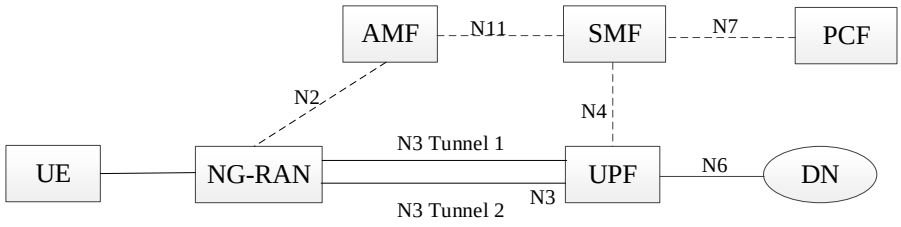


Figure 5.33.2.2-1: Redundant transmission with two N3 tunnels between the PSA UPF and a single NG-RAN node

Two Intermediate UPFs (I-UPFs) between the PSA UPF and the NG-RAN may be used to support the redundant transmission based on two N3 and N9 tunnels between a single NG-RAN node and the PSA UPF. The NG-RAN node and PSA UPF shall support the packet replication and elimination function as described above.

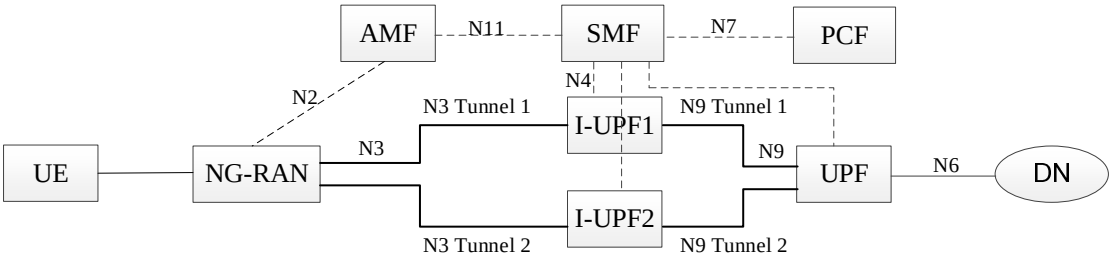


Figure 5.33.2.2-2: Two N3 and N9 tunnels between NG-RAN and PSA UPF for redundant transmission

In figure 5.33.2.2-2, there are two N3 and N9 tunnels between NG-RAN and PSA UPF for the URLLC QoS Flow(s) of the same PDU Session for redundant transmission established during or after a URLLC QoS flow establishment. In the case of downlink traffic, the PSA UPF duplicates the downlink packet of the QoS Flow from the DN and assigns the same GTP-U sequence number to them. These duplicated packets are transmitted to I-UPF1 and I-UPF2 via N9 Tunnel 1 and N9 Tunnel 2 separately. Each I-UPF forwards the packet with the same GTP-U sequence number which receives from the PSA UPF to NG-RAN via N3 Tunnel 1 and N3 Tunnel 2 respectively. The NG-RAN eliminates the duplicated packet based on the GTP-U sequence number. In the case of uplink traffic, the NG-RAN duplicates the packet of the QoS Flow from the UE and assigns the same GTP-U sequence number to them. These duplicated packets are transmitted to I-UPF1 and I-UPF2 via N3 Tunnel 1 and N3 Tunnel 2 separately. Each I-UPF forwards the packet with the same GTP-U sequence number which receives from the NG-RAN to PSA UPF via N9 Tunnel 1 and N9 Tunnel 2 respectively. The PSA UPF eliminates the duplicated packets based on the GTP-U sequence number.

The I-UPFs inserted on one leg of the redundant paths shall not behave in an UL CL or Branching Point role.

5.33.2.3 Support for redundant transmission at transport layer

Redundant transmission can be supported within the 5G System without making any assumption on support for protocols such as IEEE FRER in the application layer (DN only) at the same time it can be supported without requiring redundant GTP-U tunnel over N3. The backhaul provides two disjoint transport paths between UPF and NG-RAN. The redundancy functionality within NG-RAN and UPF make use of the independent paths at transport layer. Support of redundant transmission at transport layer requires no 3GPP protocol impact.

Following are the required steps:

- UE establishes the PDU session for URLLC services. Based on DNN, S-NSSAI, knowledge of supporting redundant transmission at transport layer and other factors as described in clause 6.3.3, SMF selects a UPF that supports redundant transmission at transport layer for the PDU session. One N3 GTP-U tunnel is established between UPF and NG-RAN.

The knowledge of supporting redundant transmission at transport layer can be configured in the SMF, or be configured in UPF and then obtained by the SMF via N4 capability negotiation during N4 Association setup procedure.

- For DL data transmission, UPF sends the DL packets on N3 GTP-U tunnel. Redundant functionality in the UPF duplicates the DL data on the transport layer. Redundant functionality in the NG-RAN eliminates the received duplicated DL data and sends to NG-RAN.

- For UL data transmission, NG-RAN sends the received UL packets on N3 GTP-U tunnel, the Redundant functionality in the NG-RAN performs the redundant handling on the backhaul transport layer. The Redundant functionality in the UPF eliminates the received duplicated UL data and sends to UPF.

5.33.3 QoS Monitoring to Assist URLLC Service

5.33.3.1 General

In this release, the QoS Monitoring is applied for packet delay measurement. The packet delay between UE and PSA UPF is a combination of the RAN part of UL/DL packet delay as defined in TS 38.314 [120] and UL/DL packet delay between NG-RAN and PSA UPF. The NG-RAN is required to provide the QoS Monitoring on the RAN part of UL/DL packet delay measurement. The QoS Monitoring on UL/DL packet delay between NG-RAN and PSA UPF can be performed on different levels of granularities, i.e. per QoS Flow per UE level, or per GTP-U path level, subject to the operators' configuration, and/or 3rd party application request, and/or PCF policy control for the URLLC services.

The PCF generates the authorized QoS Monitoring policy for a service data flow based on the QoS Monitoring request if received from the AF. The PCF includes the authorized QoS Monitoring policy in the PCC rule and provides it to the SMF.

5.33.3.2 Per QoS Flow per UE QoS Monitoring

SMF may activate the end to end UL/DL packet delay measurement between UE and PSA UPF for a QoS Flow during the PDU Session Establishment or Modification procedure.

The SMF sends a QoS Monitoring request to the PSA UPF via N4 and NG-RAN via N2 signalling to request the QoS monitoring between PSA UPF and NG-RAN. The QoS Monitoring request may contain monitoring parameters determined by SMF based on the authorized QoS Monitoring policy received from the PCF and/or local configuration.

The NG-RAN initiates the RAN part of UL/DL packet delay measurement based on the QoS Monitoring request from SMF. NG-RAN reports the RAN part of UL/DL packet delay result to the PSA UPF in the UL data packet or dummy UL packet.

If the NG-RAN and PSA UPF are time synchronised, the one way packet delay monitoring between NG-RAN and PSA UPF is supported.

If the NG-RAN and PSA UPF are not time synchronised, it is assumed that the UL packet delay and the DL packet delay between NG-RAN and PSA UPF is the same.

For both time synchronised and not time synchronised between NG-RAN and PSA UPF, the PSA UPF creates and sends the monitoring packets to the RAN:

- The PSA UPF encapsulates in the GTP-U header with QFI, QoS Monitoring Packet (QMP) indicator (which indicates the packet is used for UL/DL packet delay measurement) and the local time T1 when the PSA UPF sends out the DL monitoring packets.

- The NG-RAN records the local time T1 received in the GTP-U header and the local time T2 at the reception of the DL monitoring packets. The NG-RAN initiates RAN part of UL/DL packet delay measurement.

- When receiving an UL packet from UE for that QFI or when the NG-RAN sends a dummy UL packet as monitoring response (in case there is no UL service packet for UL packet delay monitoring), the NG-RAN encapsulates QMP indicator, the RAN part of UL/DL packet delay result, the time T1 received in the GTP-U header, the local time T2 at the reception of the DL monitoring packet and the local time T3 when NG-RAN sends out this monitoring response packet to the UPF via N3 interface, in the GTP-U header of the monitoring response packet.

NOTE: When the NG-RAN sends the dummy UL packet as monitoring response to PSA UPF depends on NG-RAN's implementation.

- The PSA UPF records the local time T4 when receiving the monitoring response packets and calculates the round trip (if not time synchronized) or UL/DL packet delay (if time synchronized) between NG-RAN and anchor PSA UPF based on the time information contained in the GTP-U header of the received monitoring responsepacket. The PSA UPF calculates the UL/DL packet delay between the NG-RAN and the PSA UPF based on the (T2-T1+T4-T3)/2. The PSA UPF calculates the UL/DL packet delay between UE and PSA UPF based on the received RAN part of UL/DL packet delay result and the calculated UL/DL packet delay between RAN and PSA UPF. The PSA UPF reports the result to the SMF based on some specific condition, e.g. when threshold for reporting to SMF is reached.

If the redundant transmission on N3/N9 interfaces is activated, the UPF and NG-RAN performs QoS monitoring for both UP paths. The UPF reports the packet delay of the two UP paths respectively to the SMF.

5.33.3.3 GTP-U Path Monitoring

The SMF can request to activate QoS monitoring for the GTP-U path(s) between all UPF(s) and the (R)AN based on locally configured policies. Alternatively, when a QoS monitoring policy is received in a PCC rule and the QoS monitoring is not yet active for the DSCP corresponding to the 5QI in the PCC rule, the SMF activates QoS Monitoring for all UPFs currently in use for this PDU Session and the (R)AN. The SMF sends the QoS monitoring policy to each involved UPF and the (R)AN via N4 interface and via N2 interface respectively.

A GTP-U sender performs an estimation of RTT to a GTP-U receiver on a GTP-U path by sending Echo messages and measuring time that elapses between the transmission of Request message and the reception of Response message. A GTP-U sender computes an accumulated packet delay by adding RTT/2, the processing time and, if available, an accumulated packet delay from an upstream GTP-U sender (i.e. an immediately preceding GTP-U sender in user plane path) thus the measured accumulated delay represents an estimated elapsed time since a user plane packet entered 3GPP domain.

It is expected that a GTP-U sender determines RTT periodically in order to detect changes in transport delays. QoS monitoring is performed by a GTP-U end-point (UP function) that receive and store QoS including a packet delay budget parameter for QoS flow by comparing a received accumulated packet delay with the stored QoS parameter possibly also taking into the account the measured delay of GTP-U path to next GTP-U end-point processing time. If the GTP-U end-point determines that the packet delay exceeds the requested packet delay budget then the node triggers QoS monitoring alert signalling to a control plane network function, e.g. SMF or to an OA&M function.

NOTE: Echo Request message and Echo Response message are sent outside GTP-U tunnels (the messages are using TEID set to 0). If underlying transport is using QoS differentiation (e.g. IP DiffServ) then it is up to the implementation to ensure that the Echo messages are classified correctly and receive similar treatment by the underlaying transport as GTP-U GTP-PDUs carrying QoS flows (user data).

QoS Monitoring can be used to measure the packet delay for transport paths and map the QoS Flows to appropriate network instance, DSCP values as follows:

- Packet delay measurement is performed by using GTP-U Echo Request/Response as defined in the TS 28.552 [108], in the corresponding user plane transport path(s), independent of the corresponding PDU Session and the 5QI for a given QoS flow, for a specific URLLC service.

- RAN measures the RAN part of UL/DL packet delay and calculates UL packet delay of N3 interface. RAN provides the UL packet delay of RAN part and N3 interface towards SMF (via N2).

- The PSA UPF calculates the UL/DL packet delay of N3/N9 interface (N9 is applicable when I-UPF exists).

- UPF and RAN reports QoS Monitoring result to the SMF based on some specific conditions, e.g. first time, periodic, event triggered, when thresholds for reporting towards SMF (via N4) are reached.

- UPF does measurement of network hop delay per transport resources that it will use towards a peer network node identified by an IP destination address (the hop between these two nodes) and port. The network hop measured delay is computed by sending an Echo Request over such transport resource (Ti) and measuring RTT/2 when Echo Response is received.

- UPF maps {network instance, DSCP} into Transport Resource and measures delay per IP destination address and port. Thus, for each IP destination address, the measured delay per (network instance, DSCP) entry is determined.
- The UPF performing the QoS monitoring can provide the corresponding {Network instance, DSCP} along with the measured packet delay for the corresponding transport path to the SMF.
- Based on this, SMF can determine QoS Flow mapping to the appropriate {Network instance, DSCP} considering {5QI, QoS characteristics, ARP} for the given QoS flow.

5.34 Support of deployments topologies with specific SMF Service Areas

5.34.1 General

When the UE is outside of the SMF Service Area, an I-SMF is inserted between the SMF and the AMF. The I-SMF has a N11 interface with the AMF and a N16a interface with the SMF and is responsible of controlling the UPF(s) that the SMF cannot directly control. The exchange of the SM context and forwarding of tunnel information if needed are done between two SMFs directly without involvement of AMF.

Depending on scenario, a PDU Session in non-roaming case or local breakout is either served by a single SMF or served by an SMF and an I-SMF. When a PDU Session is served by both an SMF and an I-SMF, the SMF is the NF instance that has the interfaces towards the PCF and CHF.

In this Release of the specification, deployments topologies with specific SMF Service Areas apply only for 3GPP access.

The SMF shall release or reject the PDU Session if the DNN of the PDU Session corresponds to a LADN and the I-SMF is inserted to the PDU Session.

NOTE 1: This implies that operators need to plan the LADN deployment in such a way that the LADN Service area needs to be within the SMF Service Area, but not across SMFs' Service Areas.

NOTE 2: This is to cover the case where the UE is not in or moves out of SMF Service Area and an I-SMF is inserted to the PDU Session e.g. during PDU Session Establishment, Service Request. If the PDU Session is maintained with I-SMF, the SMF is not be able to enforce the LADN Service control, e.g. SMF is not notified in the case of Service Request.

Independent of whether deployments topologies with specific SMF Service Areas apply, the SMF may trigger the PDU Session re-establishment to the same DN, if the PDU Session is associated with the SSC mode 2 or SSC mode 3.

NOTE 3: SSC mode 2 or SSC mode 3 can be used to optimize SMF location for a PDU Session and/or, depending on deployment, ensure that the UE is always within the service area of the SMF controlling the PDU Session. In this case (when PDU Session continuity over the PLMN is not required) procedures described in this clause are not needed.

In this Release, how TSC (as defined in clauses 5.27 and 5.28) is supported for PDU Sessions involving an I-SMF is not specified.

In this Release, Redundant User Plane Paths as defined in clause 5.33.2.2 is not supported for PDU Sessions involving an I-SMF.

Redundant PDU sessions support as defined in clause 5.33.2.1 is supported for PDU Sessions involving an I-SMF, when different S-NSSAIs are used for the redundant PDU sessions.

Redundant User Plane Paths as defined in clause 5.33.2.3 is supported for PDU Sessions involving an I-SMF only if this PDU session is established for a S-NSSAI referring to network instances requiring redundant transmission at transport layer.

QoS monitoring (as defined in clause 5.33.3) is supported as long as SMF and not I-SMF initiates the QoS monitoring function.

Dynamic CN PDB provisioning (as defined in clause 5.7.3.4) is supported for PDU Sessions involving an I-SMF.

In this Release, no dedicated functionality is specified for I-SMF and N16a in order to support NPN.

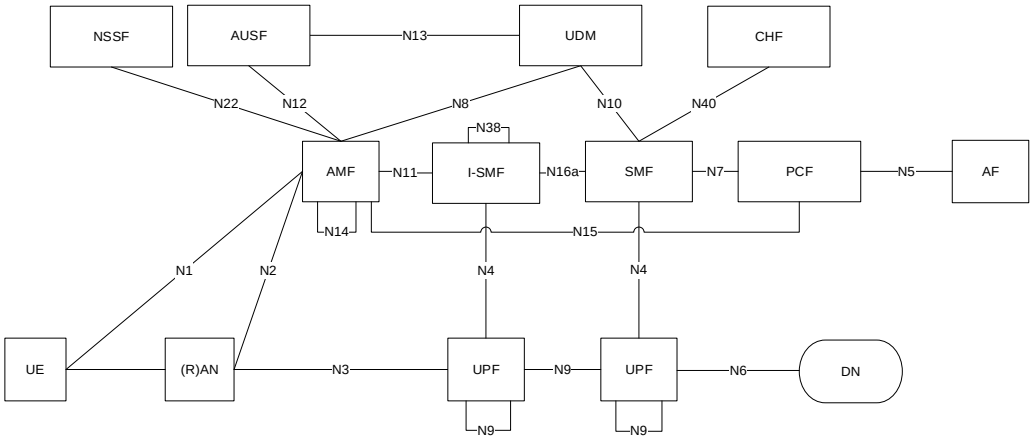
5.34.2 Architecture

5.34.2.1 SBA architecture

In non-roaming case the SBA architecture described in Figure 4.2.3-1 shall apply. In local breakout scenarios the SBA architecture described in Figure 4.2.4-1 shall apply. In Home Routed scenarios the SBA architecture described in Figure 4.2.4-3 shall apply.

5.34.2.2 Non-roaming architecture

Figure 5.34.2.2-1 depicts the non-roaming architecture with an I-SMF insertion to the PDU Session without UL-CL/BP, using reference point representation.



NOTE 1: N16a is the interface between SMF and I-SMF.
NOTE 2: N38 is the interface between I-SMFs.

Figure 5.34.2.2-1: Non-roaming architecture with I-SMF insertion to the PDU Session in reference point representation, with no UL-CL/BP

Figure 5.34.2.2-2 depicts the non-roaming architecture for an I-SMF insertion to the PDU Session with UL-CL/BP, using reference point representation.

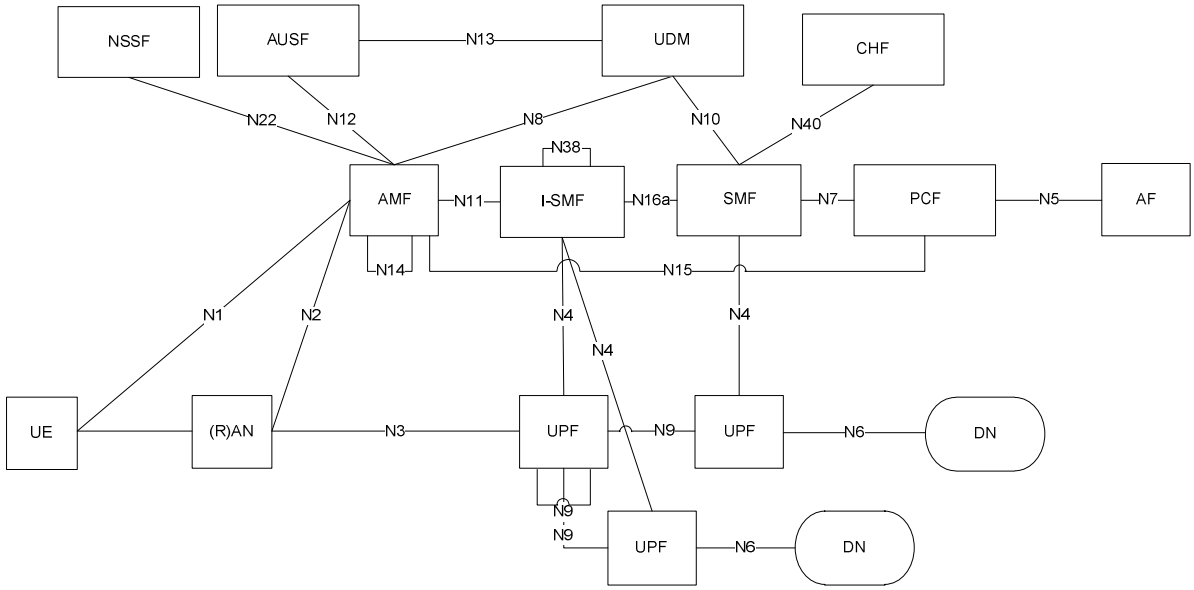


Figure 5.34.2.2-2: Non-roaming architecture with I-SMF insertion to the PDU Session in reference point representation, with UL-CL/BP

5.34.2.3 Roaming architecture

Figure 5.34.2.3-1 depicts 5G System roaming architecture in the case of local break out scenario where the SMF controlling the UPF connecting to NG-(R)AN is separated from the SMF controlling PDU Session anchor, using the reference point representation.

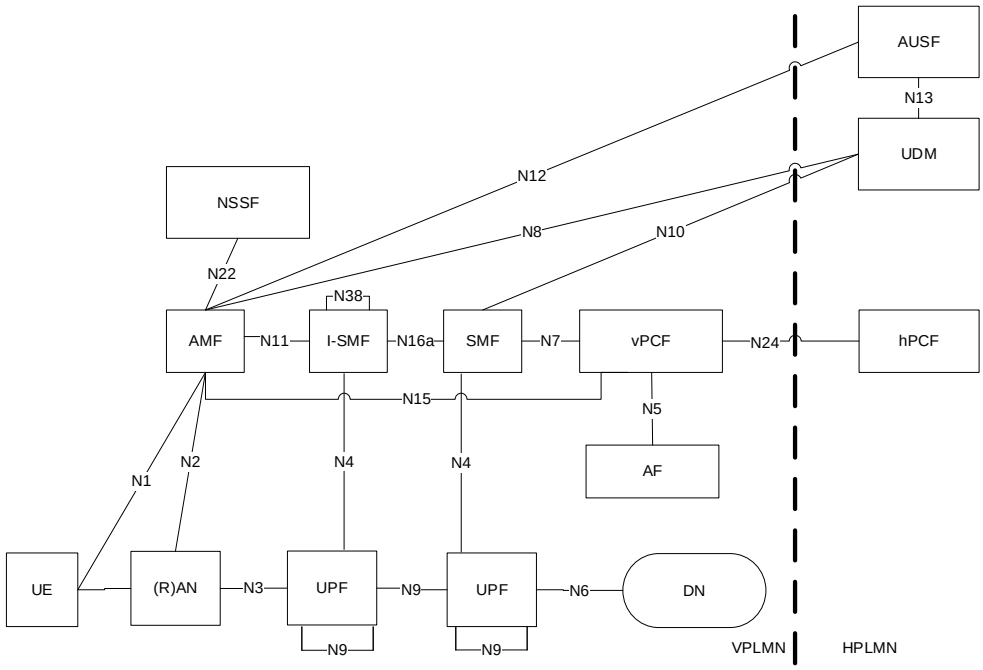


Figure 5.34.2.3-1: Roaming 5G System architecture with SMF/I-SMF - local breakout scenario in reference point representation

For the case of home routed scenario, Figure 4.2.4-6 applies.

5.34.3 I-SMF selection, V-SMF reselection

The AMF is responsible of detecting when to add or to remove an I-SMF or a V-SMF for a PDU Session. For this purpose, the AMF gets from NRF information about the Service Area of SMF(s). During mobility events such as Hand-Over or AMF change, if the service area of the SMF does not include the new UE location, then the AMF selects and inserts an I-SMF which can serve the UE location and the S-NSSAI. Conversely if the AMF detects that an I-SMF is no more needed (as the service area of the SMF includes the new UE location) it removes the I-SMF and interfaces directly with the SMF of the PDU Session. If the AMF detects that the SMF cannot serve the UE location (e.g. due to mobility), then the AMF selects a new I-SMF serving the UE location. If the existing I-SMF (or V-SMF) cannot serve the UE location (e.g. due to mobility) and the service area of the SMF does not include the new UE location (or the PDU Session is Home Routed), then the AMF initiates an I-SMF (or V-SMF) change.

At PDU Session Establishment in non-roaming and roaming with LBO scenarios, if the AMF or SCP cannot select an SMF with a Service Area supporting the current UE location for the selected (DNN, S-NSSAI) and required SMF capabilities, the AMF selects an SMF for the selected (DNN, S-NSSAI) and required capabilities and in addition selects an I-SMF serving the UE location and the S-NSSAI.

Compared to the SMF selection function defined in clause 6.3.2, the following parameters are not applicable for I-SMF selection:

- Data Network Name (DNN).
- Subscription information from UDM.

NOTE 1: All SMF(s) and I-SMF are assumed to be able to control the UPF mapping between EPC bearers and 5GC QoS flows.

If delegated SMF discovery is used at PDU Session establishment:

1. The AMF sends Nsmf_PDUSession_CreateSMContext Request to SCP and includes the parameters as defined in clause 6.3.2 (e.g. the DNN, required SMF capabilities, UE location) as discovery and selection parameters. If the SCP successfully selects an SMF matching all discovery and selection parameters, the SCP forwards the Nsmf_PDUSessionCreateSMContext Request to the selected SMF.
2. If the SCP cannot select an SMF matching all discovery and selection parameters, the SCP returns a dedicated error to AMF. In this case the I-SMF also need be discovered.
3. Upon reception of the error from the SCP that an SMF matching all discovery and selection parameters cannot be found, the AMF performs the discovery and selection of the SMF from NRF (thus not providing the UE location as a discovery parameter). The AMF may indicate the maximum number of SMF instances to be returned from NRF, i.e. SMF selection at NRF.
4. The AMF sends Nsmf_PDUSession_CreateSMContext Request to SCP, which includes the endpoint (e.g. URI) of the selected SMF and the discovery and selection parameters as defined in clause 6.3.2 except the DNN and the required SMF capabilities, i.e. parameter for I-SMF selection. The SCP performs discovery and selection of the I-SMF and forwards the Nsmf_PDUSession_CreateSMContext Request to the selected I-SMF.
5. The I-SMF sends the Nsmf_PDUSession_Create Request towards the SMF via the SCP; the I-SMF uses the received endpoint (e.g. URI) of the selected SMF to construct the target destination to be addressed. The SCP forwards the Nsmf_PDUSession_Create Request to the SMF.
6. The SMF answers to the I-SMF that answers to the AMF; in this answer the AMF receives the I-SMF ID.
7. Upon reception of a response from I-SMF, based on the received I-SMF ID, the AMF may obtain the SMF Service Area of the I-SMF from NRF. The AMF uses the SMF Service Area of the I-SMF to determine the need for I-SMF relocation upon subsequent UE mobility.

If delegated I-SMF discovery is used once the PDU Session establishment has been established, the procedure starts at step 4 above and is further detailed in the messages flows of TS 23.502 [3] clause 23.

If delegated V-SMF discovery is used for V-SMF reselection, clause 6.3.2 applies, but there is no need for discovery and selection of the H-SMF. This is further detailed in the messages flows of TS 23.502 [3] clause 23.

5.34.4 Usage of an UL Classifier for a PDU Session controlled by I-SMF

This clause applies only in the case of non-roaming or LBO roaming as control of UL CL/BP in VPLMN is not supported in HR case.

When I-SMF is involved for a PDU Session, it is possible that the UL CL controlled by I-SMF is inserted into the data path of the PDU Session. The usage of an ULCL controlled by I-SMF in the data path of a PDU Session is depicted in Figure 5.34.4-1.

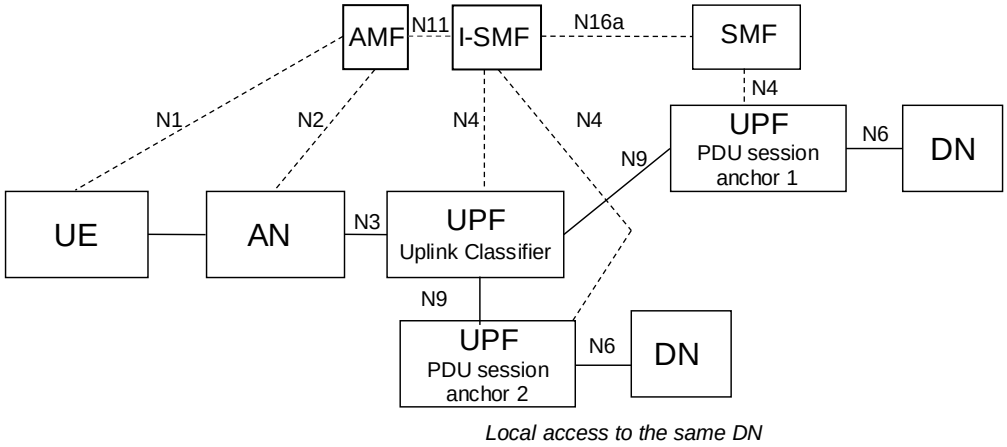


Figure 5.34.4-1: User plane Architecture for the Uplink Classifier controlled by I-SMF

The I-SMF determines whether UL CL will be inserted based on information received from SMF, and the I-SMF selects the UPFs acting as UL CL and/or PDU Session Anchor providing local access to the Data Network.

5.34.5 Usage of IPv6 multi-homing for a PDU Session controlled by I-SMF

This clause applies only in the case of non-roaming or LBO roaming as control of UL CL/BP in VPLMN is not supported in HR case.

When I-SMF is involved for a PDU Session, it is possible that the BP controlled by I-SMF is inserted into the data path of the PDU Session. The usage of a BP controlled by I-SMF in the data path of a PDU Session is depicted in Figure 5.34.5-1.

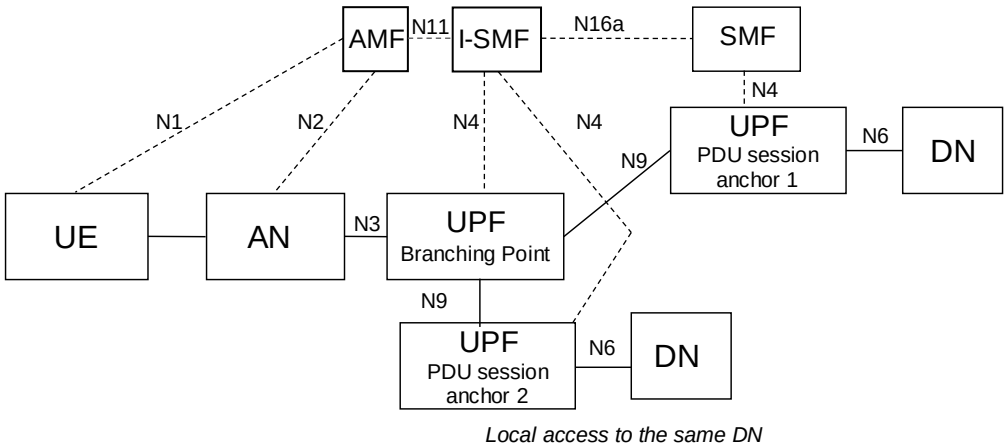


Figure 5.34.5-1: Multi-homed PDU Session: Branching Point controlled by I-SMF

The I-SMF determines whether BP will be inserted based on information received from SMF, and the I-SMF selects the UPFs acting as BP and/or PDU Session Anchor providing local access to the Data Network.

5.34.6 Interaction between I-SMF and SMF for the support of traffic offload by UPF controlled by the I-SMF

5.34.6.1 General

This clause applies only in the case of non-roaming or LBO roaming as control of UL CL/Branching Point in VPLMN is not supported in HR case. It applies for the architectures described in clauses 5.34.4 and 5.34.5

When the I-SMF is inserted into a PDU Session, e.g. during PDU Session establishment or due to UE mobility, the I-SMF may provide the DNAI list it supports to the SMF. Based on the DNAI list information received from I-SMF, the SMF may provide the DNAI(s) of interest for this PDU Session for local traffic steering to the I-SMF e.g. immediately or when a new or updated or removed PCC rule(s) is/are received. The DNAI(s) of interest is derived from PCC rules.

The I-SMF is responsible for the insertion, modification and removal of UPF(s) to ensure local traffic steering. The SMF does not need to have access to local configuration or NRF output related with UPF(s) controlled by I-SMF. Based on the DNAI(s) of interest for this PDU Session for local traffic steering and UE location the I-SMF determines which DNAI(s) are to be selected, selects UPF(s) acting as UL CL/BP and/or PDU Session Anchor based on selected DNAI, and insert these UPF(s) into the data path of the PDU Session.

When a UL CL/BP has been inserted, changed or removed, the I-SMF indicates to the SMF that traffic offload have been inserted, updated or removed for a DNAI, providing also the IPv6 prefix that has been allocated if a new IPv6 prefix has been allocated for the PDU Session.

From now on the SMF and I-SMF interactions entail:

- Notifying the SMF with the new Prefix (multi-Homing case): the SMF is responsible of issuing Router Advertisement message. The SMF constructs a link-local address as the source IP address. The Router Advertisement message includes the IPv6 multi-homed routing rules provided to the UE to select the source IPv6 prefix among the prefixes related with the PDU Session according to RFC 4191 [8]. The SMF sends the Router Advertisement message to the UE via the PSA UPF controlled by the SMF.

- N4 interactions related with traffic offloading. The SMF provide N4 information to the I-SMF for how the traffic shall be detected, enforced, monitored in UPF(s) controlled by the I-SMF: the SMF issues requests to the I-SMF containing N4 information to be used for creating / updating /removing PDR, FAR, QER, URR, etc. The N4 information for local traffic offload provided by the SMF to the I-SMF are described in clause 5.34.6.2.

- Receiving N4 notifications related with traffic usage reporting: the I-SMF forwards to the SMF N4 information corresponding to UPF notifications related with traffic usage reporting; the SMF aggregates and constructs usage reports towards PCF/CHF.

NOTE: How the SMF decides what traffic steering and enforcement actions are enforced in UPF(s) controlled by I-SMF is left for implementation.

The I-SMF is responsible of the N4 interface towards the local UPF(s) including:

- the usage of AN Tunnel Info received from the 5G AN via the AMF in order to build PDR and FAR;

- requesting the allocation of the CN Tunnel Info between local UPFs (if needed);

- to control UPF actions when the UP of the PDU Session becomes INACTIVE.

- provide Trace Requirements on the N4 interface towards the UPF(s) it is controlling, using Trace Requirements received from AMF.

5.34.6.2 N4 information sent from SMF to I-SMF for local traffic offload

The SMF generates N4 information for local traffic offload based on the available DNAI(s) indicated by the I-SMF, PCC rules associated with these DNAI(s) and charging requirement. This N4 information is sent from the SMF to the I-SMF after UL CL/Branching Point insertion/update/removal, and the I-SMF uses this N4 information to derive rules installed in the UPFs controlled by the I-SMF.

The N4 information for local traffic offload corresponds to rules and parameters defined in clause 5.8.2.11, i.e. PDR, FAR, URR and QER. It contains identifiers allowing the SMF to later modify or delete these rules.

N4 information for local traffic offload is generated by the SMF without knowledge of how many local UPF(s) are actually used by the I-SMF. The SMF indicates whether a rule within N4 information is enforced in UL CL/ Branching Point or local PSA. If the rule is applied to the local PSA, the N4 information includes the associated DNAI. The I-SMF generates suitable rules for the UPF(s) based on the N4 information received from SMF.

NOTE: The SMF is not aware of whether there is a single PSA or multiple PSA controlled by I-SMF.

The following parameters are managed by the I-SMF:

- The 5G AN Tunnel Info.
- CN tunnel info between local UPFs.
- Network instance (if needed).

The N4 information exchanged between I-SMF and SMF are not associated with a N4 Session ID but are associated with an N16a association allowing the SMF to modify or delete the N4 information at a later stage.

The I-SMF generates an N4 Session ID and for each rule a Rule ID (unless the ones received from the SMF can be used) and maintains a mapping between the locally generated identifiers and the ones received from the SMF. The I-SMF replaces those IDs in the PDR(s), QER(s), URR(s) and FAR(s) received from the SMF. When the I-SMF receives the N4 information, the Network instance (if needed) included in the rules sent to the UPF is generated by I-SMF.

5.34.7 Event Management

5.34.7.1 UE's Mobility Event Management

When an I-SMF is involved in a PDU Session, the SMF and I-SMF independently subscribe to "UE mobility event notification" service provided by AMF. The AMF treats the SMF's and I-SMF's subscription separately and notifies the event directly to the SMF or I-SMF. If the SMF does not know the serving AMF address, the SMF gets the serving AMF address from the UDM as described in clause 5.2.3.2.4, TS 23.502 [3] and subscribes directly with the serving AMF.

In the case of AMF change (e.g. Inter NG-RAN node N2 based handover), the target AMF receives mobility event subscription information from the source AMF and updates the mobility event subscription information with the SMF and I-SMF independently (i.e. target AMF allocates the Subscription Correlation ID for each event and notifies the respective SMFs and I-SMF as described in clause 5.3.4.4).

In the case of I-SMF change or I-SMF insertion (e.g. at Inter NG-RAN node N2 based handover), the subscription of mobility event (from AMF) is not transferred from the old I-SMF or SMF to the new I-SMF, the new I-SMF triggers a new subscription event if the new I-SMF wants to receive the corresponding mobility event. In the case of I-SMF removal, the subscription of mobility event at the AMF is not transferred from the old I-SMF to the SMF, the SMF triggers a new subscription event if the SMF wants to receive the corresponding mobility event.

The subscription from the old SMF entity (old I-SMF, SMF) is removed via an explicitly request from this old SMF entity.

5.34.7.2 SMF event exposure service

Consumers of SMF events do not need to be aware of the insertion / removal / change of an I-SMF as they always subscribe to the SMF of the PDU Session.

Except for the events documented in the present clause, the I-SMF does not need to support the events defined in TS 23.502 [3] clause 5.2.8.3.1.

For Events "First downlink packet per source of the downlink IP traffic (buffered / discarded / transmitted)", when an I-SMF is involved in the PDU Session, the SMF subscribes / unsubscribes onto I-SMF for the PDU Session ID on behalf of the event consumer (e.g. at I-SMF insertion or when a consumer subscribes or un subscribes while an I-SMF serves the PDU Session) and the I-SMF directly notifies the event consumer. At I-SMF change, the related SMF event subscriptions are not transferred from source I-SMF to the target I-SMF. The SMF may trigger new subscription event to the target I-SMF if the SMF wants to receive the corresponding SMF event. At I-SMF change or removal the corresponding subscription is removed in the source I-SMF when it removes the context associated with the PDU Session Id.

5.34.7.3 AMF implicit subscription about events related with the PDU Session

When creating an association with a SMF or I-SMF for a PDU Session, the AMF implicitly subscribes to SMF / I-SMF about events related with the PDU Session (the AMF provides the relevant notification information to the SMF or the I-SMF respectively). This implicit subscription is implicitly released when the corresponding association with the SMF / I-SMF is removed (e.g. as no more needed due to a I-SMF insertion / change / removal).

5.34.8 Support for Cellular IoT

This clause defines the specific impacts of deployments topologies with specific SMF Service Areas on how 5GS supports Cellular IoT as defined in clause 5.31.

For a PDU Session supporting Control Plane CIoT 5GS Optimisation as defined in clause 5.31.4:

- For a PDU session towards a DNN/S-NSSAI for which the subscription includes a NEF Identity for NIDD (i.e. for a PDU session which will be anchored in NEF), the AMF never inserts an I-SMF.

When an I-SMF is inserted to serve a PDU Session, the I-SMF supports the features that, as specified in clause 5.31, apply to the V-SMF in the case of Home Routed.

NOTE: This can require the SMF to subscribe onto I-SMF about RAT type change for a PDU Session as described in 23.502 [3] clause 4.23.

5.34.9 Support of the Deployment Topologies with specific SMF Service Areas feature within and between PLMN(s)

When Deployments Topologies with specific SMF Service Areas need to be used in a PLMN for a S-NSSAI, all AMF serving this S-NSSAI are configured to support Deployments Topologies with specific SMF Service Areas.

NOTE 1: The specifications do not support AMF selection related with Deployment Topologies with specific SMF Service Areas.

For HR roaming, the AMF discovers at PDU Session establishment whether a H-SMF supports V-SMF change based on feature support indication received from the NRF, possibly via the SCP. When the V-PLMN requires Deployments Topologies with specific SMF Service Areas but no H-SMF can be selected that supports V-SMF change, a H-SMF not supporting V-SMF change may be selected by the VPLMN. In that case, and if a V-SMF serving the full VPLMN is available, AMF should prefer to select such V-SMF.

In this release of the specifications, when an AMF detects the need to change the V-SMF while the H-SMF does not support V-SMF change, the AMF shall not trigger V-SMF change but shall trigger the release of the PDU Session.

NOTE 2: The AMF can determine whether the H-SMF supports V-SMF change based on NRF look up.

5.34.10 Support for 5G LAN-type service

This clause defines how 5GS supports 5G LAN-type service as defined in clause 5.29 in the case of deployments topologies with specific SMF Service Areas.

The UE may be connected with the PSA via an I-UPF which is controlled by the I-SMF. In this case, traffic switching (e.g. UPF local traffic switching) is controlled by the SMF as described in clause 5.29.4 without any specific knowledge or involvement of the I-SMF to support the 5G LAN-type service.

5.35 Support for Integrated access and backhaul (IAB)

5.35.1 IAB architecture and functional entities

Integrated access and backhaul (IAB) enables wireless in-band and out-of-band relaying of NR Uu access traffic via NR Uu backhaul links. The Uu backhaul links can exist between the IAB-node and:

- a gNB referred to as IAB-donor; or

- another IAB-node.

The part of the IAB node that supports the Uu interface towards the IAB-donor or another parent IAB-node (and thus manages the backhaul connectivity with either PLMN or SNPN it is registered with) is referred to as an IAB-UE.

At high level, IAB has the following characteristics:

- IAB uses the CU/DU architecture defined in TS 38.401 [42], and the IAB operation via F1 (between IAB-donor and IAB-node) is invisible to the 5GC;
- IAB performs relaying at layer-2, and therefore does not require a local UPF;
- IAB supports multi-hop backhauling;
- IAB supports dynamic topology update, i.e. the IAB-node can change the parent node, e.g. another IAB-node, or the IAB-donor, during operation, for example in response to backhaul link failure or blockage.

Figure 5.35.1-1 shows the IAB reference architecture with two backhaul hops, when connected to 5GC.

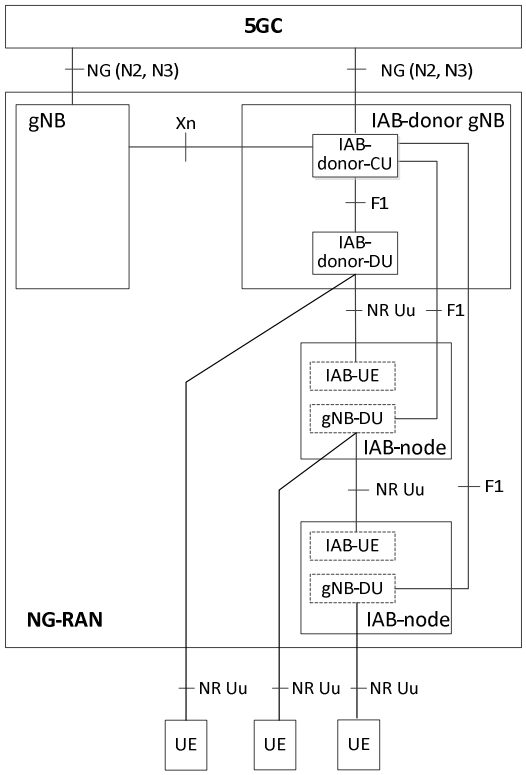


Figure 5.35.1-1: IAB architecture for 5GS

The gNB-DU in the IAB-node is responsible for providing NR Uu access to UEs and child IAB-nodes. The corresponding gNB-CU function resides on the IAB-donor gNB, which controls IAB-node gNB-DU via the F1 interface. IAB-node appears as a normal gNB to UEs and other IAB-nodes and allows them to connect to the 5GC.

The IAB-UE function behaves as a UE, and reuses UE procedures to connect to:

- the gNB-DU on a parent IAB-node or IAB-donor for access and backhauling;
- the gNB-CU on the IAB-donor via RRC for control of the access and backhaul link;
- 5GC, e.g. AMF, via NAS;
- OAM system via a PDU session or PDN connection (based on implementation).

NOTE: The 5GC, e.g. SMF, may detect that a PDU session for the IAB-UE is for the OAM system access, e.g. by checking the DNN and/or configuration. It is up to the operator configuration to choose whether to use 1 or multiple QoS flows for OAM traffic and the appropriate QoS parameters, e.g. using 5QI=6 for software downloading, and 5QI=80 with signalled higher priority or a pre-configured 5QI for alarm or control traffic.

The IAB-UE can connect to 5GC over NR (SA mode) or connect to EPC (EN-DC mode). The UE served by the IAB-node can operate in the same or different modes than the IAB-node as defined in TS 38.401 [42]. The operation mode with both UE and IAB-node connected to EPC is covered in TS 23.401 [26]. Operation modes with UE and IAB-node connected to different core networks are described in clause 5.35.6.

5.35.2 5G System enhancements to support IAB

In IAB operation, the IAB-UE interacts with the 5GC using procedures defined for UE. The IAB-node gNB-DU only interacts with the IAB-donor-CU and follows the CU/DU design defined in TS 38.401 [42].

Editor's note: The following are the expected system enhancements to assist the development of the CRs for IAB. It will be revised and updated based on RAN WG's conclusion.

For the IAB-UE operation, the existing UE authentication methods as defined in TS 33.501 [29] applies. Both USIM based methods and EAP based methods are allowed, and NAI based SUPIs can be used.

Editor's note: Security aspect is being studied by SA WG3, and the above will be revised and aligned after the conclusion of the study.

The following aspects are enhanced to support the IAB operation:

- the Registration procedure as defined in TS 23.502 [3] clause 4.2.2.2 is enhanced to indicate IAB-node's capability to the AMF;
- The IAB-node provides an IAB-indication to the IAB-donor-CU when the the RRC connection is established as defined in TS 38.331 [28]. When the IAB-indication is received, the IAB-donor-CU selects an AMF that supports IAB and includes the IAB-indication in the N2 INITIAL UE MESSAGE as defined in TS 38.413 [34] so that the AMF can perform IAB authorization.
- the UE Subscription data as defined in TS 23.502 [3] clause 5.2.3 is enhanced to include the authorization information for the IAB operation;
- Authorization procedure during the UE Registration procedure is enhanced to perform verification of IAB subscription information;
- UE Context setup/modification procedure is enhanced to provide IAB authorized indication to NG-RAN.

After registered to the 5G system, the IAB-node remains in CM-CONNECTED state. In the case of radio link failure, the IAB-UE uses existing UE procedure to restore the connection with the network. The IAB-UE uses Deregistration Procedure as defined in TS 23.502 [3] clause 4.2.2.3 to disconnect from the network.

5.35.3 Data handling and QoS support with IAB

Control plane and user plane protocol stacks for IAB operation are defined in TS 38.300 [27].

QoS management for IAB can remain transparent to the 5GC. If NG-RAN cannot meet a QoS requirement for a QoS flow to IAB-related resource constraints, the NG-RAN can reject the request using procedures defined in TS 23.502 [3].

The IAB-UE function can establish a PDU session or PDN connection, e.g. for OAM purpose (protocol stack not shown here). In that case, the IAB-UE obtains an IP address/prefix from the core network using normal UE procedures. The IAB-UE's IP address is different from that of the IAB-node's gNB DU IP address.

5.35.4 Mobility support with IAB

For UEs, all existing NR intra-RAT mobility and dual-connectivity procedures are supported when the UE is served by an IAB-node. However, in this release of the specification, there is no system level support of service continuity for a UE served by an IAB-node when the serving IAB-node changes its IAB-donor-CU.

5.35.5 Charging support with IAB

IAB-donor has all the information regarding the UE and the IAB-node and corresponding mapping of the bearers. The PDU sessions for the UE and IAB-node are separate from IAB-node onwards to the core network. Therefore, the existing charging mechanism as defined in clause 5.12 can be used to support IAB.

5.35.6 IAB operation involving EPC

When the IAB-donor gNB has connection to both EPC and 5GC, based on PLMN configuration, there are two possible operation modes:

- the IAB-node connects to a 5GC via the IAB-donor gNB, while the UEs served by the IAB-node connect to EPC with Dual Connectivity as defined in TS 37.340 [31]. In this operation mode, the IAB-donor gNB has connection to an eNB, and the 5GC is restricted for IAB-node access only; and
- the IAB-node connects to an EPC via the IAB-donor gNB with Dual Connectivity as defined in TS 37.340 [31], while the UEs served by the IAB-node connect to the 5GC. In this operation mode, the EPC is restricted for IAB-node access only.

To support the above operation modes, the IAB-UE shall be configured to select only a specific PLMN (as defined in TS 23.122 [17]) and whether it needs to connect to 5GC or EPC.

NOTE: For a particular PLMN, it is expected that only one of the modes would be deployed in a known region.

5.36 RIM Information Transfer

The purpose of RIM Information Transfer is to enable the transfer of RIM information between two RAN nodes via 5GC. The RIM Information Transfer is specified in TS 38.413 [34].

When the source AMF receives RIM information from source NG-RAN towards target NG-RAN, the source AMF forwards the RIM information to the target AMF, as described in TS 38.413 [34], TS 29.518 [71]. The AMF does not interpret the transferred RIM information.

6 Network Functions

6.1 General

Clause 6 provides the functional description of the Network Functions and network entities in the 5GC, and the principles for Network Function and Network Function Service discovery and selection.

6.2 Network Function Functional description

6.2.1 AMF

The Access and Mobility Management function (AMF) includes the following functionality. Some or all of the AMF functionalities may be supported in a single instance of an AMF:

- Termination of RAN CP interface (N2).
- Termination of NAS (N1), NAS ciphering and integrity protection.
- Registration management.
- Connection management.
- Reachability management.
- Mobility Management.

- Lawful intercept (for AMF events and interface to LI System).
- Provide transport for SM messages between UE and SMF.
- Transparent proxy for routing SM messages.
- Access Authentication.
- Access Authorization.
- Provide transport for SMS messages between UE and SMSF.
- Security Anchor Functionality (SEAF) as specified in TS 33.501 [29].
- Location Services management for regulatory services.
- Provide transport for Location Services messages between UE and LMF as well as between RAN and LMF.
- EPS Bearer ID allocation for interworking with EPS.
- UE mobility event notification.
- Support for Control Plane CIoT 5GS Optimisation.
- Support for User Plane CIoT 5GS Optimisation.
- Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters).
- Support for Network Slice-Specific Authentication and Authorization.

NOTE 1: Regardless of the number of Network functions, there is only one NAS interface instance per access network between the UE and the CN, terminated at one of the Network functions that implements at least NAS security and Mobility Management.

In addition to the functionalities of the AMF described above, the AMF may include the following functionality to support non-3GPP access networks:

- Support of N2 interface with N3IWF/TNGF. Over this interface, some information (e.g. 3GPP Cell Identification) and procedures (e.g. Handover related) defined over 3GPP access may not apply, and non-3GPP access specific information may be applied that do not apply to 3GPP accesses.
- Support of NAS signalling with a UE over N3IWF/TNGF. Some procedures supported by NAS signalling over 3GPP access may be not applicable to untrusted non-3GPP (e.g. Paging) access.
- Support of authentication of UEs connected over N3IWF/TNGF.
- Management of mobility, authentication, and separate security context state(s) of a UE connected via a non-3GPP access or connected via a 3GPP access and a non-3GPP access simultaneously.
- Support as described in clause 5.3.2.3 a co-ordinated RM management context valid over a 3GPP access and a Non 3GPP access.
- Support as described in clause 5.3.3.4 dedicated CM management contexts for the UE for connectivity over non-3GPP access.

NOTE 2: Not all of the functionalities are required to be supported in an instance of a Network Slice.

In addition to the functionalities of the AMF described above, the AMF may include policy related functionalities as described in clause 6.2.8 in TS 23.503 [45].

The AMF uses the N14 interface for AMF re-allocation and AMF to AMF information transfer. This interface may be be either intra-PLMN or inter-PLMN (e.g. in the case of inter-PLMN mobility).

In addition to the functionality of the AMF described above, the AMF may include the following functionality to support monitoring in roaming scenarios:

- Normalization of reports according to roaming agreements between VPLMN and HPLMN (e.g. change the location granularity in a report from cell level to a level that is appropriate for the HPLMN); and
- Generation of charging/accounting information for Monitoring Event Reports that are sent to the HPLMN.

6.2.2 SMF

The Session Management function (SMF) includes the following functionality. Some or all of the SMF functionalities may be supported in a single instance of a SMF:

- Session Management e.g. Session Establishment, modify and release, including tunnel maintain between UPF and AN node.
- UE IP address allocation & management (including optional Authorization). The UE IP address may be received from a UPF or from an external data network.
- DHCPv4 (server and client) and DHCPv6 (server and client) functions.
- Functionality to respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests based on local cache information for the Ethernet PDUs. The SMF responds to the ARP and / or the IPv6 Neighbour Solicitation Request by providing the MAC address corresponding to the IP address sent in the request.
- Selection and control of UP function, including controlling the UPF to proxy ARP or IPv6 Neighbour Discovery, or to forward all ARP/IPv6 Neighbour Solicitation traffic to the SMF, for Ethernet PDU Sessions.
- Configures traffic steering at UPF to route traffic to proper destination.
- 5G VN group management, e.g. maintain the topology of the involved PSA UPFs, establish and release the N19 tunnels between PSA UPFs, configure traffic forwarding at UPF to apply local switching, N6-based forwarding or N19-based forwarding.
- Termination of interfaces towards Policy control functions.
- Lawful intercept (for SM events and interface to LI System).
- Charging data collection and support of charging interfaces.
- Control and coordination of charging data collection at UPF.
- Termination of SM parts of NAS messages.
- Downlink Data Notification.
- Initiator of AN specific SM information, sent via AMF over N2 to AN.
- Determine SSC mode of a session.
- Support for Control Plane CIoT 5GS Optimisation.
- Support of header compression.
- Act as I-SMF in deployments where I-SMF can be inserted, removed and relocated.
- Provisioning of external parameters (Expected UE Behaviour parameters or Network Configuration parameters).
- Support P-CSCF discovery for IMS services.
- Roaming functionality:
  - Handle local enforcement to apply QoS SLAs (VPLMN).
  - Charging data collection and charging interface (VPLMN).
  - Lawful intercept (in VPLMN for SM events and interface to LI System).

- Support for interaction with external DN for transport of signalling for PDU Session authentication/authorization by external DN.
- Instructs UPF and NG-RAN to perform redundant transmission on N3/N9 interfaces.

NOTE: Not all of the functionalities are required to be supported in an instance of a Network Slice.

In addition to the functionalities of the SMF described above, the SMF may include policy related functionalities as described in clause 6.2.2 in TS 23.503 [45].

In addition to the functionality of the SMF described above, the SMF may include the following functionality to support monitoring in roaming scenarios:

- Normalization of reports according to roaming agreements between VPLMN and HPLMN; and
- Generation of charging/accounting information for Monitoring Event Reports that are sent to the HPLMN.

6.2.3 UPF

The User plane function (UPF) includes the following functionality. Some or all of the UPF functionalities may be supported in a single instance of a UPF:

- Anchor point for Intra-/Inter-RAT mobility (when applicable).
- Allocation of UE IP address/prefix (if supported) in response to SMF request.
- External PDU Session point of interconnect to Data Network.
- Packet routing & forwarding (e.g. support of Uplink classifier to route traffic flows to an instance of a data network, support of Branching point to support multi-homed PDU Session, support of traffic forwarding within a 5G VN group (UPF local switching, via N6, via N19)).
- Packet inspection (e.g. Application detection based on service data flow template and the optional PFDs received from the SMF in addition).
- User Plane part of policy rule enforcement, e.g. Gating, Redirection, Traffic steering).
- Lawful intercept (UP collection).
- Traffic usage reporting.
- QoS handling for user plane, e.g. UL/DL rate enforcement, Reflective QoS marking in DL.
- Uplink Traffic verification (SDF to QoS Flow mapping).
- Transport level packet marking in the uplink and downlink.
- Downlink packet buffering and downlink data notification triggering.
- Sending and forwarding of one or more "end marker" to the source NG-RAN node.
- Functionality to respond to Address Resolution Protocol (ARP) requests and / or IPv6 Neighbour Solicitation requests based on local cache information for the Ethernet PDUs. The UPF responds to the ARP and / or the IPv6 Neighbour Solicitation Request by providing the MAC address corresponding to the IP address sent in the request.
- Packet duplication in downlink direction and elimination in uplink direction in GTP-U layer.
- TSN Translator (NW-TT) functionality.
- High latency communication, see clause 5.31.8.
- ATSSS Steering functionality to steer the MA PDU Session traffic, refer to clause 5.32.6.

NOTE: Not all of the UPF functionalities are required to be supported in an instance of user plane function of a Network Slice.

- Inter PLMN UP Security (IPUPS) functionality, specified in clause 5.8.2.14.

6.2.4 PCF

The Policy Control Function (PCF) includes the following functionality:

- Supports unified policy framework to govern network behaviour.
- Provides policy rules to Control Plane function(s) to enforce them.
- Accesses subscription information relevant for policy decisions in a Unified Data Repository (UDR).

NOTE: The PCF accesses the UDR located in the same PLMN as the PCF.

The details of the PCF functionality are defined in clause 6.2.1 of TS 23.503 [45].

6.2.5 NEF

The Network Exposure Function (NEF) supports the following independent functionality:

- Exposure of capabilities and events:

  NF capabilities and events may be securely exposed by NEF for e.g. 3rd party, Application Functions, Edge Computing as described in clause 5.13.

  NEF stores/retrieves information as structured data using a standardized interface (Nudr) to the Unified Data Repository (UDR).

- Secure provision of information from external application to 3GPP network:

  It provides a means for the Application Functions to securely provide information to 3GPP network, e.g. Expected UE Behaviour, 5GLAN group information and service specific information. In that case the NEF may authenticate and authorize and assist in throttling the Application Functions.

- Translation of internal-external information:

  It translates between information exchanged with the AF and information exchanged with the internal network function. For example, it translates between an AF-Service-Identifier and internal 5G Core information such as DNN, S-NSSAI, as described in clause 5.6.7.

  In particular, NEF handles masking of network and user sensitive information to external AF's according to the network policy.

- The Network Exposure Function receives information from other network functions (based on exposed capabilities of other network functions). NEF stores the received information as structured data using a standardized interface to a Unified Data Repository (UDR). The stored information can be accessed and "re-exposed" by the NEF to other network functions and Application Functions, and used for other purposes such as analytics.

- A NEF may also support a PFD Function: The PFD Function in the NEF may store and retrieve PFD(s) in the UDR and shall provide PFD(s) to the SMF on the request of SMF (pull mode) or on the request of PFD management from NEF (push mode), as described in TS 23.503 [45].

- A NEF may also support a 5GLAN Group Management Function: The 5GLAN Group Management Function in the NEF may store the 5GLAN group information in the UDR via UDM as described in TS 23.502 [3].

- Exposure of analytics:

  NWDAF analytics may be securely exposed by NEF for external party, as specified in TS 23.288 [86].

- Retrieval of data from external party by NWDAF:

  Data provided by the external party may be collected by NWDAF via NEF for analytics generation purpose. NEF handles and forwards requests and notifications between NWDAF and AF, as specified in TS 23.288 [86].

- Support of Non-IP Data Delivery:

  NEF provides a means for management of NIDD configuration and delivery of MO/MT unstructured data by exposing the NIDD APIs as described in TS 23.502 [3] on the N33/Nnef reference point. See clause 5.31.5.

A specific NEF instance may support one or more of the functionalities described above and consequently an individual NEF may support a subset of the APIs specified for capability exposure.

NOTE: The NEF can access the UDR located in the same PLMN as the NEF.

The services provided by the NEF are specified in clause 7.2.8.

The IP address(es)/port(s) of the NEF may be locally configured in the AF, or the AF may discover the FQDN or IP address(es)/port(s) of the NEF by performing a DNS query using the External Identifier of an individual UE or using the External Group Identifier of a group of UEs, or, if the AF is trusted by the operator, the AF may utilize the NRF to discover the FQDN or IP address(es)/port(s) of the NEF as described in clause 6.3.14.

For external exposure of services related to specific UE(s), the NEF resides in the HPLMN. Depending on operator agreements, the NEF in the HPLMN may have interface(s) with NF(s) in the VPLMN.

When a UE is capable of switching between EPC and 5GC, an SCEF+NEF is used for service exposure. See clause 5.17.5 for a description of the SCEF+NEF.

6.2.5.1 Support for CAPIF

When an NEF is used for external exposure, the CAPIF may be supported. When CAPIF is supported, an NEF that is used for external exposure supports the CAPIF API provider domain functions. The CAPIF and associated API provider domain functions are specified in TS 23.222 [64].

6.2.5a Void

6.2.6 NRF

6.2.6.1 General

The Network Repository Function (NRF) supports the following functionality:

- Supports service discovery function. Receive NF Discovery Request from NF instance or SCP, and provides the information of the discovered NF instances (be discovered) to the NF instance or SCP.
- Supports P-CSCF discovery (specialized case of AF discovery by SMF).
- Maintains the NF profile of available NF instances and their supported services.
- Maintains SCP profile of available SCP instances.
- Supports SCP discovery by SCP instances.
- Notifies about newly registered/updated/ deregistered NF and SCP instances along with its potential NF services to the subscribed NF service consumer or SCP.
- Maintains the health status of NFs and SCP.

In the context of Network Slicing, based on network implementation, multiple NRFs can be deployed at different levels (see clause 5.15.5):

- PLMN level (the NRF is configured with information for the whole PLMN),
- shared-slice level (the NRF is configured with information belonging to a set of Network Slices),
- slice-specific level (the NRF is configured with information belonging to an S-NSSAI).

In the context of roaming, multiple NRFs may be deployed in the different networks (see clause 4.2.4):

- the NRF(s) in the Visited PLMN (known as the vNRF) configured with information for the visited PLMN.
- the NRF(s) in the Home PLMN (known as the hNRF) configured with information for the home PLMN, referenced by the vNRF via the N27 interface.

6.2.6.2 NF profile

NF profile of NF instance maintained in an NRF includes the following information:

- NF instance ID.
- NF type.
- PLMN ID.
- Network Slice related Identifier(s) e.g. S-NSSAI, NSI ID.
- FQDN or IP address of NF.
- NF capacity information.
- NF priority information.

NOTE 1: This parameter is used for AMF selection, if applicable, as specified in clause 6.3.5. See clause 6.1.6.2.2 of TS 29.510 [58] for its detailed use.

- NF Set ID.
- NF Service Set ID of the NF service instance.
- NF Specific Service authorization information.
- if applicable, Names of supported services.
- Endpoint Address(es) of instance(s) of each supported service.
- Identification of stored data/information.

NOTE 2: This is only applicable for a UDR profile. See applicable input parameters for Nnrf_NFManagement_NFRegister service operation in TS 23.502 [3] clause 5.2.7.2.2. This information applicability to other NF profiles is implementation specific.

- Other service parameter, e.g., DNN or DNN list, notification endpoint for each type of notification that the NF service is interested in receiving.
- Location information for the NF instance.

NOTE 3: This information is operator specific. Examples of such information can be geographical location, data center.

- TAI(s).
- NF load information.
- Routing Indicator, for UDM and AUSF.
- One or more GUAMI(s), in the case of AMF.
- SMF area identity(ies) in the case of UPF.
- UDM Group ID, range(s) of SUPIs, range(s) of GPSIs, range(s) of internal group identifiers, range(s) of external group identifiers for UDM.
- UDR Group ID, range(s) of SUPIs, range(s) of GPSIs, range(s) of external group identifiers for UDR.

- AUSF Group ID, range(s) of SUPIs for AUSF.
- PCF Group ID, range(s) of SUPIs for PCF.
- HSS Group ID, set(s) of IMPIs, set(s) of IMPU, for HSS.
- Supported Analytics ID(s), NWDAF Serving Area information (i.e. list of TAIs for which the NWDAF can provide analytics) if available in the case of NWDAF.

NOTE 4: The NWDAF's Serving Area information is common to all its supported Analytics IDs.

- Event ID(s) supported by AFs, in the case of NEF.
- Application ID(s) supported by AFs, in the case of NEF.
- Range(s) of External Identifiers, or range(s) of External Group Identifiers, or the domain names served by the NEF, in the case of NEF.

NOTE 5: This is applicable when NEF exposes AF information for analytics purpose as detailed in TS 23.288 [86].

NOTE 6: It is expected service authorization information is usually provided by OA&M system, and it can also be included in the NF profile in the case that e.g. an NF instance has an exceptional service authorization information.

NOTE 7: The NRF may store a mapping between UDM Group ID and SUPI(s), UDR Group ID and SUPI(s), AUSF Group ID and SUPI(s) and PCF Group ID and SUPI(s), to enable discovery of UDM, UDR, AUSF and PCF using SUPI, SUPI ranges as specified in clause 6.3 or interact with UDR to resolve the UDM Group ID/UDR Group ID/AUSF Group ID/PCF Group ID based on UE identity, e.g. SUPI (see clause 6.3.1 for details).

- IP domain list as described in clause 6.1.6.2.21 of TS 29.510 [58], Range(s) of (UE) IPv4 addresses or Range(s) of (UE) IPv6 prefixes, in the case of BSF.

6.2.6.3 SCP profile

SCP profile maintained in an NRF includes the following information:

- SCP ID.
- FQDN or IP address of SCP.
- Indication that the profile is of an SCP (e.g. NF type parameter set to type SCP).
- SCP capacity information.
- SCP load information.
- SCP priority.
- Location information for the SCP (see locality in 29.510 [58] clause 6.1.6.2.2).
- Served Location(s) (see servingScope in 29.510 [58] clause 6.1.6.2.2).
- Network Slice related Identifier(s) e.g. S-NSSAI, NSI ID.
- Remote PLMNs reachable through SCP.
- Endpoint addresses accessible via the SCP.
- Interconnected SCP IDs.
- Interconnected NF IDs.
- NF sets of NFs served by the SCP.
- SCP Domain the SCP belongs to. If an SCP belongs to more than one SCP Domain, the SCP will be able bridge these domains, i.e. sending messages between these domains.

NOTE: Service definition defines optional and mandatory parameters, see TS 23.502 [3].

6.2.7 UDM

The Unified Data Management (UDM) includes support for the following functionality:

- Generation of 3GPP AKA Authentication Credentials.
- User Identification Handling (e.g. storage and management of SUPI for each subscriber in the 5G system).
- Support of de-concealment of privacy-protected subscription identifier (SUCI).
- Access authorization based on subscription data (e.g. roaming restrictions).
- UE's Serving NF Registration Management (e.g. storing serving AMF for UE, storing serving SMF for UE's PDU Session).
- Support to service/session continuity e.g. by keeping SMF/DNN assignment of ongoing sessions.
- MT-SMS delivery support.
- Lawful Intercept Functionality (especially in outbound roaming case where UDM is the only point of contact for LI).
- Subscription management.
- SMS management.
- 5GLAN group management handling.
- Support of external parameter provisioning (Expected UE Behaviour parameters or Network Configuration parameters).

To provide this functionality, the UDM uses subscription data (including authentication data) that may be stored in UDR, in which case a UDM implements the application logic and does not require an internal user data storage and then several different UDMs may serve the same user in different transactions.

NOTE 1: The interaction between UDM and HSS, when they are deployed as separate network functions, is defined in TS 23.632 [102] and TS 29.563 [103] or it is implementation specific.

NOTE 2: The UDM is located in the HPLMN of the subscribers it serves, and access the information of the UDR located in the same PLMN.

6.2.8 AUSF

The Authentication Server Function (AUSF) supports the following functionality:

- Supports authentication for 3GPP access and untrusted non-3GPP access as specified in TS 33.501 [29].

6.2.9 N3IWF

The functionality of N3IWF in the case of untrusted non-3GPP access includes the following:

- Support of IPsec tunnel establishment with the UE: The N3IWF terminates the IKEv2/IPsec protocols with the UE over NWu and relays over N2 the information needed to authenticate the UE and authorize its access to the 5G Core Network.
- Termination of N2 and N3 interfaces to 5G Core Network for control - plane and user-plane respectively.
- Relaying uplink and downlink control-plane NAS (N1) signalling between the UE and AMF.
- Handling of N2 signalling from SMF (relayed by AMF) related to PDU Sessions and QoS.
- Establishment of IPsec Security Association (IPsec SA) to support PDU Session traffic.

- Relaying uplink and downlink user-plane packets between the UE and UPF. This involves:
  - De-capsulation/ encapsulation of packets for IPSec and N3 tunnelling
- Enforcing QoS corresponding to N3 packet marking, taking into account QoS requirements associated to such marking received over N2
- N3 user-plane packet marking in the uplink.
- Local mobility anchor within untrusted non-3GPP access networks using MOBIKE per IETF RFC 4555 [57].
- Supporting AMF selection.

6.2.9A TNGF

The functionality of TNGF in the case of trusted non-3GPP access includes the following:

- Terminates the N2 and N3 interfaces.
- Terminates the EAP-5G signalling and behaves as authenticator when the UE attempts to register to 5GC via the TNAN.
- Implements the AMF selection procedure.
- Transparently relays NAS messages between the UE and the AMF, via NWt.
- Handles N2 signalling with SMF (relayed by AMF) for supporting PDU sessions and QoS.
- Transparently relays PDU data units between the UE and UPF(s).
- Implements a local mobility anchor within the TNAN.
- Implements a local EAP Re-authentication (ER) server (as per RFC 6696) to facilitate mobility within the TNAN.

6.2.10 AF

The Application Function (AF) interacts with the 3GPP Core Network in order to provide services, for example to support the following:

- Application influence on traffic routing (see clause 5.6.7);
- Accessing Network Exposure Function (see clause 5.20);
- Interacting with the Policy framework for policy control (see clause 5.14);
- IMS interactions with 5GC (see clause 5.16).

Based on operator deployment, Application Functions considered to be trusted by the operator can be allowed to interact directly with relevant Network Functions.

Application Functions not allowed by the operator to access directly the Network Functions shall use the external exposure framework (see clause 7.3) via the NEF to interact with relevant Network Functions.

The functionality and purpose of Application Functions are only defined in this specification with respect to their interaction with the 3GPP Core Network.

6.2.11 UDR

The Unified Data Repository (UDR) supports the following functionality:

- Storage and retrieval of subscription data by the UDM.
- Storage and retrieval of policy data by the PCF.

- Storage and retrieval of structured data for exposure.
- Application data (including Packet Flow Descriptions (PFDs) for application detection, AF request information for multiple UEs, 5GLAN group information for 5GLAN management).
- Storage and retrieval of NF Group ID corresponding to subscriber identifier (e.g. IMPI, IMPU, SUPI).

The Unified Data Repository is located in the same PLMN as the NF service consumers storing in and retrieving data from it using Nudr. Nudr is an intra-PLMN interface.

NOTE 1: Deployments can choose to collocate UDR with UDSF.

6.2.12 UDSF

The UDSF is an optional function that supports the following functionality:

- Storage and retrieval of information as unstructured data by any NF.

NOTE 1: Structured data in this specification refers to data for which the structure is defined in 3GPP specifications. Unstructured data refers to data for which the structure is not defined in 3GPP specifications.

NOTE 2: Deployments can choose to collocate UDSF with UDR.

6.2.13 SMSF

The SMSF supports the following functionality to support SMS over NAS:

- SMS management subscription data checking and conducting SMS delivery accordingly.
- SM-RP/SM-CP with the UE (see TS 24.011 [6]).
- Relay the SM from UE toward SMS-GMSC/IWMSC/SMS-Router.
- Relay the SM from SMS-GMSC/IWMSC/SMS-Router toward the UE.
- SMS related CDR.
- Lawful Interception.
- Interaction with AMF and SMS-GMSC for notification procedure that the UE is unavailable for SMS transfer (i.e, notifies SMS-GMSC to inform UDM when UE is unavailable for SMS).

6.2.14 NSSF

The Network Slice Selection Function (NSSF) supports the following functionality:

- Selecting the set of Network Slice instances serving the UE;
- Determining the Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs;
- Determining the Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs;
- Determining the AMF Set to be used to serve the UE, or, based on configuration, a list of candidate AMF(s), possibly by querying the NRF.

6.2.15 5G-EIR

The 5G-EIR is an optional network function that supports the following functionality:

- Check the status of PEI (e.g. to check that it has not been blacklisted).

6.2.16 LMF

The functionality of LMF is defined in clause 4.3.8 of TS 23.273 [87].

6.2.16A GMLC

The functionality of GMLC is defined in clause 4.3.8 of TS 23.273 [87].

6.2.17 SEPP

The Security Edge Protection Proxy (SEPP) is a non-transparent proxy and supports the following functionality:

- Message filtering and policing on inter-PLMN control plane interfaces.

NOTE: The SEPP protects the connection between Service Consumers and Service Producers from a security perspective, i.e. the SEPP does not duplicate the Service Authorization applied by the Service Producers as specified in clause 7.1.4.

- Topology hiding.

Detailed functionality of SEPP, related flows and the N32 reference point, are specified in TS 33.501 [29].

The SEPP applies the above functionality to every Control Plane message in inter-PLMN signalling, acting as a service relay between the actual Service Producer and the actual Service Consumer. For both Service Producer and Consumer, the result of the service relaying is equivalent to a direct service interaction. Every Control Plane message in inter-PLMN signalling between the SEPPs may pass via IPX entities. More details on SEPPs and the IPX entities are described in TS 29.500 [49] and TS 33.501 [29].

6.2.18 Network Data Analytics Function (NWDAF)

NWDAF represents operator managed network analytics logical function. The NWDAF includes the following functionality:

- Support data collection from NFs and AFs;
- Support data collection from OAM;
- NWDAF service registration and metadata exposure to NFs/AFs;
- Support analytics information provisioning to NFs, AF.

The details of the NWDAF functionality are defined in TS 23.288 [86].

NOTE: NWDAF functionality beyond its support for Nnwdaf is out of scope of 3GPP.

6.2.19 SCP

The Service Communication Proxy (SCP) includes one or more of the following functionalities. Some or all of the SCP functionalities may be supported in a single instance of an SCP:

- Indirect Communication (see clause 7.1.1 for details).
- Delegated Discovery (see clauses 7.1.1 and 6.3.1 for details).
- Message forwarding and routing to destination NF/NF service.
- Message forwarding and routing to a next hop SCP.
- Communication security (e.g. authorization of the NF Service Consumer to access the NF Service Producer API), load balancing, monitoring, overload control, etc.
- Optionally interact with UDR, to resolve the UDM Group ID/UDR Group ID/AUSF Group ID/PCF Group ID/CHF Group ID/HSS Group ID based on UE identity, e.g. SUPI or IMPI/IMPU (see clause 6.3.1 for details).

NOTE 1: Communication security, e.g. authorization of the NF Service Consumer to access the NF Service Producer's API is specified in TS 33.501 [29].

NOTE 2: Load balancing, monitoring, overload control functionality provided by the SCP is left up to implementation.

The SCP may be deployed in a distributed manner.

NOTE 3: More than one SCP can be present in the communication path between NF Services.

SCPs can be deployed at PLMN level, shared-slice level and slice-specific level. It is left to operator deployment to ensure that SCPs can communicate with relevant NRFs.

In order to enable SCPs to route messages through several SCPs (i.e. next SCP hop discovery, see clause 6.3.16), an SCP may register its profile in the NRF. Alternatively, local configuration may be used.

6.2.20 W-AGF

The functionality of W-AGF is specified in TS 23.316 [84].

6.2.21 UE radio Capability Management Function (UCMF)

The UCMF is used for storage of dictionary entries corresponding to either PLMN-assigned or Manufacturer-assigned UE Radio Capability IDs. An AMF may subscribe with the UCMF to obtain from the UCMF new values of UE Radio Capability ID that the UCMF assigns for the purpose of caching them locally.

Provisioning of Manufacturer-assigned UE Radio Capability ID entries in the UCMF is performed from an AF that interacts with the UCMF either directly or via the NEF (or via Network Management) using a procedure defined in TS 23.502 [3]. A UCMF that serves both EPS and 5GS shall require provisioning the UE Radio Capability ID with the TS 36.331 [51] format or TS 38.331 [28] format or both the formats of the UE radio capabilities.

The UCMF also assigns the PLMN-assigned UE Radio Capability ID values.

Each PLMN-assigned UE Radio Capability ID is also associated to the TAC of the UE model(s) that it is related to. When an AMF requests the UCMF to assign a UE Radio Capability ID for a set of UE radio capabilities, it indicates the TAC of the UE that the UE Radio Capability information is related to.

The UCMF stores a Version ID value for the PLMN assigned UE Radio Capability IDs so it is included in the PLMN assigned UE Radio Capability IDs it assigns. This shall be configured in the UCMF.

The UCMF may be provisioned with a dictionary of Manufacturer-assigned UE Radio Capability IDs which include a "Vendor ID" that applies to the Manufacturers of these UE, and a list of TACs for which the PLMN has obtained-Manufacturer-assigned UE Radio Capability IDs.

A PLMN-assigned UE Radio Capability IDs is kept in the UCMF storage as long as it is associated with at least a TAC value. When a TAC value is related to a UE model that is earmarked for operation based on Manufacturer assigned UE Radio Capability IDs, this TAC value is disassociated in the UCMF from any PLMN assigned UE Radio Capability IDs.

For the case that the PLMN is configured to store PLMN assigned IDs in the Manufacturer Assigned operation requested list defined in clause 4.4.1a, the UCMF does not remove from storage any PLMN assigned UE Radio Capability ID no longer used, and rather quarantines it to avoid any future reassignment.

6.2.22 TWIF

The functionality of Trusted WLAN Interworking Function (TWIF) is specified in clause 4.2.8.5.3.

6.2.23 NSSAAF

The Network Slice Specific Authentication and Authorization Function (NSSAAF) supports the following functionality:

- Support for Network Slice-Specific Authentication and Authorization as specified in TS 23.502 [3] with a AAA Server (AAA-S). If the AAA-S belongs to a third party, the NSSAAF may contact the AAA-S via an a AAA proxy (AAA-P).

6.3 Principles for Network Function and Network Function Service discovery and selection

6.3.1 General

The NF discovery and NF service discovery enable Core Network entities (NFs or Service Communication Proxy (SCP)) to discover a set of NF instance(s) and NF service instance(s) for a specific NF service or an NF type. NF service discovery is enabled via the NF discovery procedure, as specified in TS 23.502 [3], clauses 4.17.4, 4.17.5, 4.17.9 and 4.17.10.

Unless the expected NF and NF service information is locally configured on the requester NF, e.g. when the expected NF service or NF is in the same PLMN as the requester NF, the NF and NF service discovery is implemented via the Network Repository Function (NRF). NRF is the logical function that is used to support the functionality of NF and NF service discovery and status notification as specified in clause 6.2.6.

NOTE 1: NRF can be colocated together with SCP e.g. for communication option D, depicted in Annex E.

In order for the requested NF type or NF service to be discovered via the NRF, the NF instance need to be registered in the NRF. This is done by sending a Nnrf_NFManagement_NFRegister containing the NF profile. The NF profile contains information related to the NF instance, such as NF instance ID, supported NF service instances (see clause 6.2.6 for more details regarding the NF profile). The registration may take place e.g. when the producer NF instance and its NF service instance(s) become operative for the first time. The NF service registration procedure is specified in TS 23.502 [3], clause 4.17.1.

In order for the requester NF or SCP to obtain information about the NF and/or NF service(s) registered or configured in a PLMN/slice, based on local configuration the requester NF or SCP may initiate a discovery procedure with the NRF by providing the type of the NF and optionally a list of the specific service(s) it is attempting to discover. The requester NF or SCP may also provide other service parameters e.g. slicing related information. For the detailed service parameter(s) used for specific NF and NF service discovery refer to clause 5.2.7.3.2 of TS 23.502 [3]. The requester NF may also provide NF Set related information to enable reselection of NF instances within the NF set.

For some Network Functions which have access to the subscription data (e.g. HSS, UDM) the NRF may need to resolve the NF Group ID corresponding to a subscriber identifier. If the NRF has no stored configuration mapping identity sets/ranges to NF Group ID locally, the NRF may retrieve the NF Group ID corresponding to a specific subscriber identifier from the UDR using the Nudr_GroupIDmap_Query service operation.

In the case of Indirect Communication, a NF Service Consumer employs an SCP which routes the request to the intended target of the request.

If the requester NF is configured to delegate discovery, the requester NF may omit the discovery procedure with the NRF and instead delegate the discovery to the SCP; the SCP will then act on behalf of the requester NF. In this case, the requester NF adds any necessary discovery and selection parameters to the request in order for the SCP to be able to do discovery and associated selection. The SCP may interact with the NRF to perform discovery and obtain discovery result and it may interact with the NRF or UDR to obtain NF Group ID corresponding to subscriber identifier.

NOTE 2: For delegated discovery of the HSS or the UDM, the SCP can rely on the NRF to discover the group of HSS/UDM instance(s) serving the provided user identity, or in some deployments the SCP can first query the UDR for the HSS/UDM Group ID for the provided user identity. It is expected that the stage 3 defines a single encoding for the user identity provided by the service consumer that can be used for both variants of delegated discovery to avoid that the service consumer needs to be aware of the SCP behaviour.

The NRF provides a list of NF instances and NF service instances relevant for the discovery criteria. The NRF may provide the IP address or the FQDN of NF instance(s) and/or the Endpoint Address(es) of relevant NF service instance(s) to the NF Consumer or SCP. The NRF may also provide NF Set ID and/or NF Service Set ID to the NF Consumer or SCP. The response contains a validity period during which the discovery result is considered valid and can be cached. The result of the NF and NF service discovery procedure is applicable to any subscriber that fulfils the same discovery criteria. The entity that does the discovery may cache the NF profile(s) received from the NF/NF service

discovery procedure. During the validity period, the cached NF profile(s) may be used for NF selection for any subscriber matching the discovery criteria.

NOTE 3: Refer to TS 29.510 [58] for details on using the validity period.

In the case of Direct Communication, the requester NF uses the discovery result to select NF instance and a NF service instance that is able to provide a requested NF Service (e.g., a service instance of the PCF that can provide Policy Authorization).

In the case of Indirect Communication without Delegated Discovery, the requester NF uses the discovery result to select a NF instance while the associated NF service instance selection may be done by the requester NF and/or an SCP on behalf of the requester NF.

In both the cases above, the requester NF may use the information from a valid cached discovery result for subsequent selections (i.e. the requester NF does not need to trigger a new NF discovery procedure to perform the selection).

In the case of Indirect Communication with Delegated Discovery, the SCP will discover and select a suitable NF instance and NF service instance based on discovery and selection parameters provided by the requester NF and optional interaction with the NRF. The NRF to be used may be provided by the NF consumer as part of the discovery parameters, e.g. as a result of a NSSF query. The SCP may use the information from a valid cached discovery result for subsequent selections (i.e. the SCP does not need to trigger a new NF discovery procedure to perform the selection).

NOTE 4: In a given PLMN, Direct Communication, Indirect Communication, or both may apply.

The requester NF or SCP may subscribe to receive notifications from the NRF of a newly updated NF profile of an NF (e.g. NF service instances taken in or out of service), or newly registered de-registered NF instances. The NF/NF service status subscribe/notify procedure is defined in TS 23.502 [3], clauses 4.17.7 and 4.17.8.

For NF and NF service discovery across PLMNs, the NRF in the local PLMN interacts with the NRF in the remote PLMN to retrieve the NF profile(s) of the NF instance(s) in the remote PLMN that matches the discovery criteria. The NRF in the local PLMN reaches the NRF in the remote PLMN by forming a target PLMN specific query using the PLMN ID provided by the requester NF. The NF/NF service discovery procedure across PLMNs is specified in clause 4.17.5 of TS 23.502 [3].

NOTE 5: See TS 29.510 [58] for details on using the target PLMN ID specific query to reach the NRF in the remote PLMN.

For topology hiding, see clause 6.2.17.

6.3.1.0 Principles for Binding, Selection and Reselection

Binding can be used to indicate suitable target NF producer instance(s) for NF service instance selection, reselection and routing of subsequent requests associated with a specific NF producer resource (context) and NF service. This allows the NF producer to indicate that the NF consumer, for a particular context, should be bound to an NF service instance, NF instance, NF service set or NF set depending on local policies and other criteria (e.g. at what point it is in the middle of a certain procedure, considering performance aspects etc).

Binding can also be used by the NF consumer to indicate suitable NF consumer instance(s) for notification target instance reselection and routing of subsequent notification requests associated with a specific notification subscription and for providing Binding Indication for service(s) that the NF consumer produces for the same data context and the NF service producer is subsequently likely to invoke.

The Binding Indication contains the information in Table 6.3.1.0-1.

The Routing Binding Indication may be included in Request, Subscribe or Notification messages (see clause 7.1.2). It can be used in the case of indirect communication by the SCP to route the message. The Routing Binding Indication is a copy of the information in the Binding Indication and also contains the information in Table 6.3.1.0-1.

NOTE 1: Subscription request messages can contain both a Binding Indication and a Routing Binding Indication.

The NF service producer may provide a Binding Indication to the NF service consumer as part of the Direct or Indirect Communication procedures, to be used in subsequent related service requests. The level of Binding Indication provided by the NF service producer to the NF consumer indicates if the resource in the NF service producer is either bound to NF service instance, NF instance, NF Service Set or NF set as specified in Table 6.3.1.0-1. The Binding Indication may include NF Service Set ID, NF Set ID, NF instance ID, or NF service instance ID, for use by the NF consumer or SCP

for NF Service Producer (re-)selection. If the resource is created in the NF Service Producer, the NF Service Producer provides resource information which includes the endpoint address of the NF service producer. For indirect communication, the NF service consumer copies the Binding Indication into the Routing Binding Indication in Request or Subscribe message.

During explicit or implicit notification subscription, a Binding Indication may be provided by the NF service consumer to NF service producer; the NF service consumer will also provide a Notification Endpoint. The NF service consumer may also provide a Binding Indication in response to notification requests. The level of Binding Indication provided by the NF service consumer to the NF service provider indicates if the Notification Endpoint is either bound to NF service instance, NF instance, NF Service Set or NF set as specified in Table 6.3.1.0-1. The Binding Indication shall include at least one of NF Set ID, NF instance ID, NF Service Set ID and/or NF service instance ID, and may also include the service name. The NF Service Set ID, NF service instance ID, and service name relate to the service of the NF service consumer that will handle the notification.

NOTE 2: The NF service can either be a standardised service as per this specification or a custom service. The custom service can be used for the sole purpose of registering endpoint address(es) to receive notifications at the NRF.

The Binding Indication is used by the NF service producer as notification sender to reselect an endpoint address and construct the Notification Endpoint, i.e. the URI where the notification is to be sent, e.g. if the provided Notification Endpoint of the NF service consumer included in the subscription cannot be reached, according to the following:

- If the service name in the Binding Indication is omitted and the binding for notification is on NF Set or NF Instance level, the endpoint address registered in the NRF at NF Profile level of the NF(s) selected according to the Binding Indication shall be used to construct a new Notification Endpoint.

- If the service name is included in the Binding Indication, an endpoint address registered in the NRF for that service in the NF profile(s) selected according to the Binding Indication shall be used to construct a new Notification Endpoint.

For indirect communication, the NF service producer copies the Binding Indication into the Routing Binding Indication that is included in the Notification request, to be used by the SCP to discover an alternative endpoint address and construct a Notification Endpoint e.g. if the Notification Endpoint that the request targets cannot be reached, according to the following:

- If the service name in the Routing Binding Indication is omitted and the binding for notification is on NF Set or NF Instance level, the endpoint address registered in the NRF at NF Profile level of the NF(s) selected according to the Binding Indication shall be used to construct a new Notification Endpoint.

- If the service name is included in the Routing Binding Indication, an endpoint address registered in the NRF for that service in the NF profile(s) selected according to the Binding Indication shall be used to construct a new Notification Endpoint.

For subscription to notifications via another network function, a separate Binding Indication for subscription related events may be provided by the NF service consumer (see clause 4.17.12.4 of TS 23.502 [3]) and if provided shall be associated with an applicability indicating notification for subscription related events.

If the NF as an NF consumer provides a Binding Indication for services that the NF produces in service requests, the Binding Indication shall be associated with an applicability indicating other service and may contain the related service name(s), in addition to the other parameters listed in Table 6.3.1.0-1. If no service name(s) are provided, the Binding Indication relates to all services that the NF produces.

For NF Set or NF Instance level of binding, a Binding Indication for notifications and other services may be combined if it relates to the same service, and that combined Binding Indication shall then be associated with an applicability indicating all scenarios that the Binding Indication relates to (For this purpose, the applicability can indicate a combination of values).

If no applicability is indicated in a request or subscribe messages, a Binding Indication in that messages is applicable for notification to all events except for the subscription related event (see clause 4.17.12.4 of TS 23.502 [3]).

NOTE 3: Such a request message can be used for implicit subscription.

NOTE 4: Request messages can contain both the Binding Indications for services and for notifications, and in addition, the Routing Binding Indication in the case of indirect communication.

Table 6.3.1.0-1 defines the selection and reselection behaviour of NF services consumers and SCPs depending on the Binding Indication provided by an NF service producer. The detailed procedures refer to clause 4.17.11 and 4.17.12 of TS 23.502 [3]

Table 6.3.1.0-1: Binding, selection and reselection

Level of Binding Indication	The NF Consumer / Notification sender / SCP selects	The NF Consumer / Notification sender / SCP can reselect e.g. when selected producer is not available	Binding information for selection and re-selection
NF Service Instance	The indicated NF Service Instance	An equivalent NF Service instance: - within the NF Service Set (if applicable) - within the NF instance - within the NF Set (if applicable)	NF Service Instance ID, NF Service Set ID, NF Instance ID, NF Set ID, Service name (NOTE 4)
NF Service Set	Any NF Service instance within the indicated NF Service Set	Any NF Service instance within an equivalent NF Service Set within the NF Set (if applicable) (Note 2)	NF Service Set ID, NF Instance ID, NF Set ID, Service name (NOTE 4)
NF Instance	Any equivalent NF Service instance within the NF instance.	Any equivalent NF Service instance within a different NF instance within the NF Set (if applicable)	NF Instance ID, NF Set ID, Service name (NOTE 4)
NF Set	Any equivalent NF Service instance within the indicated NF Set	Any equivalent NF Service instance within the NF Set	NF Set ID, Service name (NOTE 4)
NOTE 1: if the Binding Indication is not available, the NF Consumer routes the service request to the target based on routing information available. NOTE 2: NF Service Sets in different NFs are considered equivalent if they include same type and variant (e.g. identical NF Service Set ID) of NF Services. NOTE 3: If a Routing Binding Indication is not available, the SCP routes the service request to the target based on available routing information. NOTE 4: The service name is only applicable if the Binding Indication relates to a notification target or If the NF as a NF consumer provides a Binding Indication for services that the NF produces.			

6.3.1.1 NF Discovery and Selection aspects relevant with indirect communication

For indirect communication shown in Annex E, the SCP performs the following functionalities regarding Network Function and Network Function Service discovery and selection:

- If the request includes a Routing Binding Indication, the SCP shall route the service request to the requested target as specified in Table 6.3.1.0-1. If the Routing Binding Indication does not exist, the SCP may get the NF Set ID from the NRF or local configuration (if available).

- If the request recipient had previously provided a Binding Indication, then the request sender shall include a Routing Binding Indication with the same contents in subsequent related requests.

6.3.1.2 Location information

The location information describes the network location of the NF instance. It can consist of one or more levels. Each level describes one location aspect, such as geographic location, data centre, cluster, etc. An NF instance has only one location.

The location information may be used to select the NF service instance or NF instance from a particular network location based on local configuration.

NOTE: The location information in TS 29.510 [58] specifies the granularity of location information. It is up to each deployment to determine the granularity of location information to be used.

6.3.2 SMF discovery and selection

The SMF selection functionality is supported by the AMF and SCP and is used to allocate an SMF that shall manage the PDU Session. The SMF selection procedures are described in clause 4.3.2.2.3 of TS 23.502 [3].

The SMF discovery and selection functionality follows the principles stated in clause 6.3.1.

If the AMF does discovery, the AMF shall utilize the NRF to discover SMF instance(s) unless SMF information is available by other means, e.g. locally configured on AMF. The AMF provides UE location information to the NRF when trying to discover SMF instance(s). The NRF provides NF profile(s) of SMF instance(s) to the AMF. In addition, the NRF also provides the SMF service area of SMF instance(s) to the AMF. The SMF selection functionality in the AMF selects an SMF instance and an SMF service instance based on the available SMF instances obtained from NRF or on the configured SMF information in the AMF.

NOTE 1: Protocol aspects of the access to NRF are specified in TS 29.510 [58].

The SMF selection functionality is applicable to both 3GPP access and non-3GPP access.

The SMF selection for Emergency services is described in clause 5.16.4.5.

The following factors may be considered during the SMF selection:

a) Selected Data Network Name (DNN). In the case of the home routed roaming, the DNN is not applied for the V-SMF selection.

b) S-NSSAI of the HPLMN (for non-roaming and home-routed roaming scenarios), and S-NSSAI of the VPLMN (for roaming with local breakout and home-routed roaming scenarios).

c) NSI-ID.

NOTE 2: The use of NSI -ID in the network is optional and depends on the deployment choices of the operator. If used, the NSI ID is associated with S-NSSAI.

d) Access technology being used by the UE.

e) Support for Control Plane CIoT 5GS Optimisation.

f) Subscription information from UDM, e.g.

- per DNN: whether LBO roaming is allowed.
- per S-NSSAI: the subscribed DNN(s).
- per (S-NSSAI, subscribed DNN): whether LBO roaming is allowed.
- per (S-NSSAI, subscribed DNN): whether EPC interworking is supported.
- per (S-NSSAI, subscribed DNN): whether selecting the same SMF for all PDU sessions to the same S-NSSAI and DNN is required.

g) Void.

h) Local operator policies.

NOTE 3: These policies can take into account whether the SMF to be selected is an I-SMF or a V-SMF or a SMF.

i) Load conditions of the candidate SMFs.

j) Analytics (i.e. statistics or predictions) for candidate SMFs' load as received from NWDAF (see TS 23.288 [86]), if NWDAF is deployed.

k) UE location (i.e. TA).

l) Service Area of the candidate SMFs.

m) Capability of the SMF to support a MA PDU Session.

n) If interworking with EPS is required.

To support the allocation of a static IPv4 address and/or a static IPv6 prefix as specified in clause 5.8.2.2.1, a dedicated SMF may be deployed for the indicated combination of DNN and S-NSSAI and registered to the NRF, or provided by the UDM as part of the subscription data.

In the case of delegated discovery, the AMF, shall send all the available factors a)-d), k) and n) to the SCP.

In addition, the AMF may indicate to the SCP which NRF to use (in the case of NRF dedicated to the target slice).

If there is an existing PDU Session and the UE requests to establish another PDU Session to the same DNN and S-NSSAI of the HPLMN, and the UE subscription data indicates the support for interworking with EPS for this DNN and S-NSSAI of the HPLMN or UE subscription data indicates the same SMF shall be selected for all PDU sessions to the same S-NSSAI, DNN, the same SMF in non roaming and LBO case or the same H-SMF in home routed roaming case, shall be selected. In addition, if the UE Context in the AMF provides a SMF ID for an existing PDU session to the same DNN, S-NSSAI, the AMF uses the stored SMF ID for the additional PDU Session. In any such a case where the AMF can determine which SMF should be selected, if delegated discovery is used, the AMF shall indicate a desired NF Instance ID so that the SCP is able to route the message to the relevant SMF. Otherwise, if UE subscription data does not indicate the support for interworking with EPS for this DNN and S-NSSAI, a different SMF in non roaming and LBO case or a different H-SMF in home routed roaming case, may be selected. For example, to support a SMF load balancing or to support a graceful SMF shutdown (e.g., a SMF starts to no more take new PDU Sessions).

In the home-routed roaming case, the SMF selection functionality selects an SMF in VPLMN based on the S-NSSAI of the VPLMN, as well as an SMF in HPLMN based on the S-NSSAI of the HPLMN. This is specified in clause 4.3.2.2.3.3 of TS 23.502 [3].

When the UE requests to establish a PDU Session to a DNN and an S-NSSAI of the HPLMN, if the UE MM Core Network Capability indicates the UE supports EPC NAS and optionally, if the UE subscription indicates the support for interworking with EPS for this DNN and S-NSSAI of the HPLMN, the selection functionality (in AMF or SCP) selects a combined SMF+PGW-C. Otherwise, a standalone SMF may be selected.

If the UDM provides a subscription context that allows for handling the PDU Session in the VPLMN (i.e. using LBO) for this DNN and S-NSSAI of the HPLMN and, optionally, the AMF is configured to know that the VPLMN has a suitable roaming agreement with the HPLMN of the UE, the following applies:

- If the AMF does discovery, the SMF selection functionality in AMF selects an SMF from the VPLMN.
- If delegated discovery is used, the SCP selects an SMF from the VPLMN.

If an SMF in the VPLMN cannot be derived for the DNN and S-NSSAI of the VPLMN, or if the subscription does not allow for handling the PDU Session in the VPLMN using LBO, then the following applies:

- If the AMF does discovery, both an SMF in VPLMN and an SMF in HPLMN are selected, and the DNN and S-NSSAI of the HPLMN is used to derive an SMF identifier from the HPLMN.
- If delegated discovery is used:
    - The AMF performs discovery and selection of H-SMF from NRF. The AMF may indicate the maximum number of H-SMF instances to be returned from NRF, i.e. SMF selection at NRF.
    - The AMF sends Nsmf_PDUSession_CreateSMContext Request to SCP, which includes the endpoint (e.g. URI) of the selected H-SMF, and the discovery and selection parameters as defined in this clause, i.e. parameter for V-SMF selection. The SCP performs discovery and selection of the V-SMF and forwards the request to the selected V-SMF.
    - The V-SMF sends the Nsmf_PDUSession_Create Request towards the H-SMF via the SCP; the V-SMF uses the received endpoint (e.g. URI) of the selected H-SMF to construct the target destination to be addressed. The SCP forwards the request to the H-SMF.
    - Upon reception of a response from V-SMF, based on the received V-SMF ID the AMF obtains the Service Area of the V-SMF from NRF. The AMF uses the Service Area of the V-SMF to determine the need for V-SMF relocation upon subsequent UE mobility.

If the initially selected SMF in VPLMN (for roaming with LBO) detects it does not understand information in the UE request, it may reject the N11 message (related with a PDU Session Establishment Request message) with a proper N11

cause triggering the AMF to select both a new SMF in the VPLMN and a SMF in the HPLMN (for home routed roaming).

The AMF selects SMF(s) considering support for CIoT 5GS optimisations (e.g. Control Plane CIoT 5GS Optimisation).

Additional details of AMF selection of an I-SMF are described in clause 5.34.

In the case of home routed scenario, the AMF selects a new V-SMF if it determines that the current V-SMF cannot serve the UE location. The selection/relocation is same as an I-SMF selection/relocation as described in clause 5.34.

6.3.3 User Plane Function Selection

6.3.3.1 Overview

The selection and reselection of the UPF are performed by the SMF by considering UPF deployment scenarios such as centrally located UPF and distributed UPF located close to or at the Access Network site. The selection of the UPF shall also enable deployment of UPF with different capabilities, e.g. UPFs supporting no or a subset of optional functionalities.

For home routed roaming case, the UPF(s) in home PLMN is selected by SMF(s) in HPLMN, and the UPF(s) in the VPLMN is selected by SMF(s) in VPLMN. The exact set of parameters used for the selection mechanism is deployment specific and controlled by the operator configuration.

The UPF selection involves:

- a step of SMF Provisioning of available UPF(s). This step may take place while there is no PDU Session to establish and may be followed by N4 Node Level procedures defined in clause 4.4.3 of TS 23.502 [3] where the UPF and the SMF may exchange information such as the support of optional functionalities and capabilities.

- A step of selection of an UPF for a particular PDU Session; it is followed by N4 session management procedures defined in clause 4.4.1 of TS 23.502 [3].

6.3.3.2 SMF Provisioning of available UPF(s)

SMF may be locally configured with the information about the available UPFs, e.g. by OA&M system when UPF is instantiated or removed.

NOTE 1: UPF information can be updated e.g. by OA&M system any time after the initial provisioning, or UPF itself updates its information to the SMF any time after the node level interaction is established.

The UPF selection functionality in the SMF may optionally utilize the NRF to discover UPF instance(s). In this case, the SMF issues a request to the NRF that may include following parameters: DNN, S-NSSAI, SMF Area Identity, ATSSS steering capabilities. In its answer, the NRF provides the NF profile(s) that include(s) the IP address(es) or the FQDN of the N4 interface of corresponding UPF instance(s) to the SMF.

UPFs may be associated with an SMF Area Identity in the NRF. This allows limiting the SMF provisioning of UPF(s) using NRF to those UPF(s) associated with a certain SMF Area Identity. This can e.g. be used in the case that an SMF is only allowed to control UPF(s) configured in NRF as belonging to a certain SMF Area Identity.

The NRF may be configured by OAM with information on the available UPF(s) or the UPF instance(s) may register its/their NF profile(s) in the NRF. This is further defined in TS 23.502 [3] clause 4.17.

6.3.3.3 Selection of an UPF for a particular PDU Session

If there is an existing PDU Session, and the SMF receives another PDU Session request to the same DNN and S-NSSAI, and if the SMF determines that interworking with EPC is supported for this PDU Session as specified in clause 4.11.5 of TS 23.502 [3], the SMF should select the same UPF, otherwise, if the SMF determines that interworking with EPC is not supported for the new PDU Session, a different UPF may be selected.

For the same DNN and S-NSSAI if different UPF are selected at 5GC, when the UE is moved to EPC network, there is no requirement to enforce APN-AMBR. Whether and how to apply APN-AMBR for the PDN Connection associated with this DNN/APN is implementation dependent, e.g. possibly only AMBR enforcement per PDU Session applies.

The following parameter(s) and information may be considered by the SMF for UPF selection and re-selection:

- UPF's dynamic load.
- Analytics (i.e. statistics or predictions) for UPF load and UE related analytics (UE mobility, UE communication, and expected UE behavioural parameters) as received from NWDAF (see TS 23.288 [86]), if NWDAF is deployed.
- UPF's relative static capacity among UPFs supporting the same DNN.
- UPF location available at the SMF.
- UE location information.
- Capability of the UPF and the functionality required for the particular UE session: An appropriate UPF can be selected by matching the functionality and features required for an UE.
- Data Network Name (DNN).
- PDU Session Type (i.e. IPv4, IPv6, IPv4v6, Ethernet Type or Unstructured Type) and if applicable, the static IP address/prefix.
- SSC mode selected for the PDU Session.
- UE subscription profile in UDM.
- DNAI as included in the PCC Rules and described in clause 5.6.7.
- Local operator policies.
- S-NSSAI.
- Access technology being used by the UE.
- Information related to user plane topology and user plane terminations, that may be deduced from:
  - 5G-AN-provided identities (e.g. CellID, TAI), available UPF(s) and DNAI(s);
- Identifiers (i.e. a FQDN and/or IP address(es)) of N3 terminations provided by a W-AGF or a TNGF or a TWIF;
- Information regarding the user plane interfaces of UPF(s). This information may be acquired by the SMF using N4;
- Information regarding the N3 User Plane termination(s) of the AN serving the UE. This may be deduced from 5G-AN-provided identities (e.g. CellID, TAI);
- Information regarding the N9 User Plane termination(s) of UPF(s) if needed;
- Information regarding the User plane termination(s) corresponding to DNAI(s).
- RSN, support for redundant GTP-U path or support for redundant transport path in the transport layer (as in clause 5.33.2) when redundant UP handling is applicable.
- Information regarding the ATSSS Steering Capability of the UE session (ATSSS-LL capability, MPTCP capability, or both) and information on the UPF support of RTT measurements without PMF.
- Support for UPF allocation of IP address/prefix.
- Support of the IPUPS functionality, specified in clause 5.8.2.14.
- Support for High latency communication (see clause 5.31.8).

NOTE 1: How the SMF determines information about the user plane network topology from information listed above, and what information is considered by the SMF, is based on operator configuration.

NOTE 2: In this release the SMF uses no additional parameters for UPF selection for a PDU Session serving TSC. If a PDU Session of a specific DS-TT needs to connect to a specific UPF hosting a specific TSN 5GS bridge, this can be achieved e.g. by using a dedicated DNN/S-NSSAI combination.

A W-AGF or a TNGF may provide Identifiers of its N3 terminations when forwarding over N2 uplink NAS signalling to the 5GC. The AMF may relay this information to the SMF, as part of session management signalling for a new PDU Session.

6.3.4 AUSF discovery and selection

In the case of NF consumer based discovery and selection, the following applies:

- The AMF performs AUSF selection to allocate an AUSF Instance that performs authentication between the UE and 5G CN in the HPLMN. The AMF shall utilize the NRF to discover the AUSF instance(s) unless AUSF information is available by other means, e.g. locally configured on AMF. The AUSF selection function in the AMF selects an AUSF instance based on the available AUSF instances (obtained from the NRF or locally configured in the AMF).

- The UDM shall utilize the NRF to discover the AUSF instance(s) unless AUSF information is available by other means, e.g. locally configured on UDM. The UDM selects an AUSF instance based on the available AUSF instance(s) obtained from the NRF or based on locally configured information, and information stored (by the UDM) from a previously successful authentication.

AUSF selection is applicable to both 3GPP access and non-3GPP access.

The AUSF selection function in AUSF NF consumers or in SCP should consider one of the following factors when available:

1. Home Network Identifier (e.g., MNC and MCC) of SUCI/SUPI (by an NF consumer in the Serving network) along with NID (provided by the NG-RAN) in the case of SNPN and Routing Indicator.

NOTE 1: The UE provides the Routing Indicator to the AMF as part of the SUCI as defined in TS 23.003 [19] during initial registration. The AMF can provide the UE's Routing Indicator to other AMFs as described in TS 23.502 [3].

NOTE 2: In the case of SNPN, the AMF uses the selected NID provided by the NG-RAN together with the selected PLMN ID (from SUCI/SUPI) as the SUCI/SUPI does not always include the NID.

When the UE's Routing Indicator is set to its default value as defined in TS 23.003 [19], the AUSF NF consumer can select any AUSF instance within the home network for the UE.

2. AUSF Group ID the UE's SUPI belongs to.

NOTE 3: The AMF can infer the AUSF Group ID the UE's SUPI belongs to, based on the results of AUSF discovery procedures with NRF. The AMF provides the AUSF Group ID the SUPI belongs to other AMFs as described in TS 23.502 [3].

3. SUPI; e.g. the AMF selects an AUSF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for AUSF discovery.

In the case of delegated discovery and selection in SCP, the AUSF NF consumer shall send all available factors to the SCP.

6.3.5 AMF discovery and selection

The AMF discovery and selection functionality is applicable to both 3GPP access and non-3GPP access.

The AMF selection functionality can be supported by the 5G-AN (e.g. RAN, N3IWF) and is used to select an AMF instance for a given UE. An AMF supports the AMF selection functionality to select an AMF for relocation or because the initially selected AMF was not an appropriate AMF to serve the UE (e.g. due to change of Allowed NSSAI). Other CP NF(s), e.g. SMF, supports the AMF selection functionality to select an AMF from the AMF set when the original AMF serving a UE is unavailable.

5G-AN selects an AMF Set and an AMF from the AMF Set under the following circumstances:

1) When the UE provides no 5G-S-TMSI nor the GUAMI to the 5G-AN.

2) When the UE provides 5G-S-TMSI or GUAMI but the routing information (i.e. AMF identified based on AMF Set ID, AMF pointer) present in the 5G-S-TMSI or GUAMI is not sufficient and/or not usable (e.g. UE provides GUAMI with an AMF region ID from a different region).

3) AMF has instructed AN that the AMF (identified by GUAMI(s)) is unavailable and no target AMF is identified and/or AN has detected that the AMF has failed.

In the case of NF Service Consumer based discovery and selection, the CP NF selects an AMF from the AMF Set under the following circumstances:

- When the AMF has instructed CP NF that a certain AMF identified by GUAMI(s) is unavailable and the CP NF was not notified of target AMF; and/or

- CP NF has detected that the AMF has failed; and/or

- When the selected AMF does not support the UE's Preferred Network Behaviour.

In the case of delegated discovery and associated selection, the SCP selects an AMF from the corresponding AMF Set under the following circumstances:

- The SCP gets an indication "select new AMF within SET" from the CP NF; and/or

- SCP has detected that the AMF has failed.

The AMF selection functionality in the 5G-AN may consider the following factors for selecting the AMF Set:

- AMF Region ID and AMF Set ID derived from GUAMI;

- Requested NSSAI;

- Local operator policies;

- 5G CIoT features indicated in RRC signalling by the UE;

- IAB-indication;

- NB-IoT RAT Type; and

- Category M Indication.

AMF selection functionality in the 5G-AN or CP NFs or SCP considers the following factors for selecting an AMF from AMF Set:

- Availability of candidate AMF(s).

- Load balancing across candidate AMF(s) (e.g. considering weight factors of candidate AMFs in the AMF Set).

- In 5G-AN, 5G CIoT features indicated in RRC signalling by the UE.

When the UE accesses the 5G-AN with a 5G-S-TMSI or GUAMI that identifies more than one AMF (as configured during N2 setup procedure), the 5G-AN selects the AMF considering the weight factors.

When 5G-S-TMSI or GUAMI provided by the UE to the 5G-AN contains an AMF Set ID that is usable, and the AMF identified by AMF pointer that is not usable (e.g. AN detects that the AMF has failed) or the corresponding AMF indicates it is unavailable (e.g. out of operation) then the 5G-AN uses the AMF Set ID for selecting another AMF from the AMF set considering the factors above.

The discovery and selection of AMF in the CP NFs or SCP follows the principle in clause 6.3.1

In the case of NF Service Consumer based discovery and selection, the AMF or other CP NFs shall utilize the NRF to discover the AMF instance(s) unless AMF information is available by other means, e.g. locally configured on AMF or other CP NFs. The NRF provides the NF profile(s) of AMF instance(s) to the AMF or other CP NFs. The AMF selection function in the AMF or other CP NFs selects an AMF instance as described below:

When NF Service Consumer performs discovery and selection the following applies:

- In the case of AMF discovery and selection functionality in AMF or other CP NFs use GUAMI or TAI to discover the AMF instance(s), the NRF provides the NF profile of the associated AMF instance(s). If an associated AMF is unavailable due to AMF planned removal, the NF profile of the backup AMF used for planned removal is provided by the NRF. If an associated AMF is unavailable due to AMF failure, the NF profile of the backup AMF used for failure is provided by the NRF. If AMF pointer value in the GUAMI is associated with more than one AMF, the NRF provides all the AMFs associated with this AMF pointer value. If no AMF instances related to the indicated GUAMI can be found, the NRF may provide a list of NF profiles of candidate AMF instances in the same AMF Set. The other CP NF or AMF may select any AMF instance from the list of candidate AMF instances. If no NF profiles of AMF is returned in the discovery result, the other CP NF or AMF may discover an AMF using the AMF Set as below.

- In the case of AMF discovery and selection functionality in AMF use AMF Set to discover AMF instance(s), the NRF provides a list of NF profiles of AMF instances in the same AMF Set.

- At intra-PLMN mobility, the AMF discovery and selection functionality in AMF may use AMF Set ID, AMF Region ID, the target location information, S-NSSAI(s) of Allowed NSSAI to discover target AMF instance(s). The NRF provides the target NF profiles matching the discovery.

- At inter PLMN mobility, the source AMF selects an AMF instance(s) in the target PLMN by querying target PLMN level NRF via the source PLMN level NRF with target PLMN ID. The target PLMN level NRF returns an AMF instance address based on the target operator configuration. After the Handover procedure the AMF may select a different AMF instance as specified in clause 4.2.2.2.3 in TS 23.502 [3].

In the context of Network Slicing, the AMF selection is described in clause 5.15.5.2.1.

When delegated discovery and associated selection is used, the following applies:

- If the CP NF includes GUAMI or TAI in the request, the SCP selects an AMF instance associated with the GUAMI or TAI and sends the request to a selected AMF service instance if it is available. The following also applies:

  - If none of the associated AMF service instances are available due to AMF planned removal, an AMF service instance from the backup AMF used for planned removal is selected by the SCP;

  - If none of the associated AMF service instances are available due to AMF failure, an AMF service instance from the backup AMF used for failure is selected by the SCP;

  - If no AMF service instances related to the indicated GUAMI can be found the SCP selects an AMF instance from the AMF Set; or

  - AMF Pointer value used by more than one AMF, SCP selects one of the AMF instances associated with the AMF Pointer.

- If the CP NF includes AMF Set ID in the request, the SCP selects AMF/AMF service instances in the provided AMF Set.

- At intra-PLMN mobility, if a target AMF instance needs to be selected, the AMF provides the source AMF Set ID, source AMF Region ID, and the target location information, S-NSSAI(s) of Allowed NSSAI in the request, optionally NRF to use. The SCP will select a target AMF instance belonging to the target AMF set in target AMF Region which can be the mapping of the source AMF set in source AMF region.

- At inter PLMN mobility, the source AMF selects indicates "roaming" to the SCP. The SCP interacts with the NRF in source PLMN so that the NRF in source PLMN can discover an AMF in the target PLMN via target PLMN NRF.

6.3.6 N3IWF selection

6.3.6.1 General

When the UE supports connectivity with N3IWF but does not support connectivity with ePDG, as specified in TS 23.402 [43], the UE shall perform the procedure in clause 6.3.6.2 for selecting an N3IWF.

When the UE supports connectivity with N3IWF, as well as with ePDG, as specified in TS 23.402 [43], the UE shall perform the procedure in clause 6.3.6.3 for selecting either an N3IWF or an ePDG, i.e. for selecting a non-3GPP access node.

In both cases above the UE can be configured by the HPLMN with the same information that includes:

1) ePDG identifier configuration: It contains the FQDN or IP address of the ePDG in the HPLMN, as specified in TS 23.402 [43], clause 4.5.4.3. This is used only when the UE supports connectivity with ePDG and attempts to select an ePDG. It is ignored in all other cases.

2) N3IWF identifier configuration: It contains the FQDN or IP address of the N3IWF in the HPLMN.

3) Non-3GPP access node selection information: It contains a prioritized list of PLMNs and for each PLMN it includes (i) a "Preference" parameter which indicates if ePDG or N3IWF is preferred in this PLMN and (ii) an FQDN parameter which indicates if the Tracking/Location Area Identity FQDN or the Operator Identifier FQDN (as specified in TS 23.402 [43], clause 4.5.4.4) should be used when discovering the address of an ePDG or N3IWF in this PLMN. The list of PLMNs shall include the HPLMN and shall include an "any PLMN" entry, which matches any PLMN the UE is connected to except the HPLMN.

The ePDG identifier configuration and the N3IWF identifier configuration are optional parameters, while the Non-3GPP access node selection information is required and shall include at least the HPLMN and the "any PLMN" entry.

If the ePDG identifier configuration is configured in the UE, then, when the UE decides to select an ePDG in the HPLMN (according to the procedure in clause 6.3.6.3), the UE shall use the ePDG identifier configuration to find the IP address of the ePDG in the HPLMN and shall ignore the FQDN parameter of the HPLMN in the Non-3GPP access node selection information.

If the N3IWF identifier configuration is configured in the UE, then, when the UE decides to select an N3IWF in the HPLMN (according to the procedure in clause 6.3.6.3 for combined N3IWF/ePDG selection and the procedure in clause 6.3.6.2 for Stand-alone N3IWF selection), the UE shall use the N3IWF identifier configuration to find the IP address of the N3IWF in the HPLMN and shall ignore the FQDN parameter of the HPLMN in the Non-3GPP access node selection information.

6.3.6.2 Stand-alone N3IWF selection

The UE performs N3IWF selection based on the ePDG selection procedure as specified in the TS 23.402 [43] clause 4.5.4 except for the following differences:

- The Tracking/Location Area Identifier FQDN shall be constructed by the UE based only on the Tracking Area wherein the UE is located. The N3IWF Tracking/Location Area Identifier FQDN may use the 5GS TAI when the UE is registered to the 5GS, or the EPS TAI when the UE is registered to EPS. The Location Area is not applicable on the 3GPP access.

- The ePDG Operator Identifier (OI) FQDN format is substituted by with N3IWF OI FQDN format as specified in TS 23.003 [19].

- The ePDG identifier configuration and the ePDG selection information are substituted by the N3IWF identifier configuration and the Non-3GPP access node selection information respectively. The UE shall give preference to the N3IWF in all PLMNs in the Non-3GPP access node selection information independent of the "Preference" parameter.

Network slice information cannot be used for N3IWF selection in this Release of the specification.

Accessing a standalone non-public network service via a PLMN, the UE uses a configured N3IWF FQDN to select an N3IWF deployed in the NPN.

6.3.6.3 Combined N3IWF/ePDG Selection

When the UE wants to select a non-3GPP access node (either an N3IWF or an ePDG), the UE shall perform the following procedure:

The UE shall first select a PLMN in which the non-3GPP access node should be selected by using the procedure specified in TS 23.402 [43], clause 4.5.4.4 with the following modifications:

- Instead of using the ePDG selection information the UE uses the Non-3GPP access node selection information.

In the selected PLMN the UE shall attempt to select a non-3GPP access node as follows:

1. The UE shall determine if the non-3GPP access node selection is required for an IMS service or for a non-IMS service. The means of that determination are implementation-specific.

2. When the selection is required for an IMS service, the UE shall choose a non-3GPP access node type (i.e. ePDG or N3IWF) based on the "Preference" parameter specified in clause 6.3.6.1, unless the UE has its 5GS capability disabled in which case it shall choose an ePDG independent of the "Preference" parameter setting.

   If the "Preference" parameter for the selected PLMN indicates that ePDG is preferred, the UE shall attempt to select an ePDG. If the "Preference" parameter for the selected PLMN indicates that N3IWF is preferred, the UE shall attempt to select an N3IWF.

   If the selection fails, including the case when, during the registration performed over either 3GPP or non-3GPP access, the UE receives the IMS Voice over PS session Not Supported over Non-3GPP Access indication (specified in clause 5.16.3.2a), the UE shall attempt selecting the other non-3GPP access node type in the selected PLMN, if any. If that selection fails too, or it is not possible, then the UE shall select another PLMN, according to the procedure specified in TS 23.402 [43], clause 4.5.4.5.

3. When the selection is required for a non-IMS service, the UE shall perform the selection by giving preference to the N3IWF independent of the "Preference" parameter setting. If the N3IWF selection fails, or it is not possible, the UE should select another PLMN based on the procedure specified in TS 23.402 [43], clause 4.5.4.4, and shall attempt to select an N3IWF in this PLMN. If the UE fails to select an N3IWF in any PLMN, the UE may attempt to select an ePDG according to the procedure specified in TS 23.402 [43], clause 4.5.4.5.

In the above procedure, when the UE attempts to construct a Tracking/Location Area Identifier FQDN either for ePDG selection or for N3IWF selection, the UE shall use the Tracking Area wherein the UE is located and shall construct either:

- an ePDG or N3IWF TAI FQDN based on the 5GS TAI, when the UE is registered to the 5GS; or

- an ePDG or N3IWF TAI FQDN based on the EPS TAI, when the UE is registered to EPS.

NOTE: A UE performing both a selection for an IMS service and a selection for a non-IMS service could get simultaneously attached to a N3IWF and to an ePDG in the same PLMN or in different PLMNs.

6.3.6.4 PLMN Selection for emergency services

UE initiates PLMN selection for emergency services when it detects a user request for emergency session and determines that untrusted non-3GPP access shall be used for the emergency access.

Unless the UE is attached to 5GC via an N3IWF or to EPC via an ePDG that has indicated support for the emergency services and is located in the same country the UE is currently located in, the UE deregisters from the 5G Core non-3GPP access or terminates the existing ePDG connection, if any, and performs PLMN selection for emergency services. Otherwise, the UE should reuse the existing N3IWF or ePDG connection.

PLMN selection for emergency services is performed as follows:

- The UE determines whether it is located in the home country or a visited country;

- If the UE is located in the home country, and the UE is equipped with a UICC, then the UE selects the PLMN for emergency services based on the configured Operator Identifier Emergency FQDN;

- If the UE is located in a visited country, the UE performs a DNS query using the Visited Country Emergency FQDN, as specified in TS 23.003 [19] to discover the regulatory requirements and to determine which PLMNs in the visited country support emergency services in non-3GPP access.

  - If the DNS response contains one or more records, the UE selects a PLMN that supports emergency services in non-3GPP access for the UE. Each record in the DNS response shall contain the identity of a PLMN in the visited country supporting emergency services in non-3GPP access.

- The UE shall consider these PLMNs based on their priorities in the Non-3GPP Access Node Selection Information. If the UE cannot select a PLMN in the Non-3GPP Access Node Selection Information, it shall attempt to select any PLMN in the list of PLMNs returned in the DNS response.

- If the DNS response does not contain any record, or if the DNS response contains one or more records but the UE fails to select a PLMN that supports emergency services in non-3GPP access, or if the Emergency Registration procedure has failed for all PLMNs supporting emergency services in non-3GPP access, the UE notifies the user that emergency session cannot be established.

When a PLMN has been selected, the UE determines whether to proceed with N3IWF selection or with ePDG selection in that PLMN according to the Non-3GPP Access Node Selection Information for that PLMN. For ePDG selection, the UE shall use the Operator Identifier Emergency FQDN and the Tracking/Location Area Identity Emergency FQDN as specified in TS 23.401 [26] clause 4.5.4a.2.

If the UE is not equipped with a UICC, the UE shall perform the emergency ePDG/N3IWF selection procedure without using the Non-3GPP Access Node Selection Information, i.e., the UE may construct the Operator Identifier FQDN format based on a PLMN ID obtained via implementation specific means.

When a N3IWF has been selected, the UE initiates an Emergency Registration. If the Emergency Registration fails, the UE shall attempt to select an ePDG before selecting another PLMN supporting emergency services in non-3GPP access. When an ePDG has been selected, the UE initiates an Emergency Registration. If the Emergency Registration fails, the UE shall attempt to select a N3IWF before selecting another PLMN supporting emergency services in non-3GPP access.

6.3.7 PCF discovery and selection

6.3.7.0 General principles

Clause 6.3.7.0 describes the underlying principles for PCF selection and discovery:

- There may be multiple and separately addressable PCFs in a PLMN.

- The PCF must be able to correlate the AF service session established over N5 or Rx with the associated PDU Session (Session binding) handled over N7.

- It shall be possible to deploy a network so that the PCF may serve only specific DN(s). For example, Policy Control may be enabled on a per DNN basis.

- Unique identification of a PDU Session in the PCF shall be possible based on the (UE ID, DNN)-tuple, the (UE (IP or MAC) Address(es), DNN)-tuple and the (UE ID, UE (IP or MAC) Address(es), DNN).

6.3.7.1 PCF discovery and selection for a UE or a PDU Session

PCF discovery and selection functionality is implemented in AMF, SMF and SCP, and follows the principles in clause 6.3.1. The AMF uses the PCF services for a UE and the SMF uses the PCF services for a PDU Session.

When the NF service consumer performs discovery and selection for a UE, the following applies:

- The AMF may utilize the NRF to discover the candidate PCF instance(s) for a UE. In addition, PCF information may also be locally configured in the AMF. The AMF selects a PCF instance based on the available PCF instances obtained from the NRF or locally configured information in the AMF, depending on operator's policies.

In the non roaming case, the AMF selects a PCF instance for AM policy association and selects the same PCF instance for UE policy association. In the roaming case, the AMF selects a V-PCF instance for AM policy association and selects the same V-PCF instance for UE policy association. The following factors may be considered at PCF discovery and selection for Access and Mobility policies and UE policies:

- SUPI; the AMF selects a PCF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for PCF discovery.

- S-NSSAI(s). In the roaming case, the AMF selects the V-PCF instance based on the S-NSSAI(s) of the VPLMN and selects the H-PCF instance based on the S-NSSAI(s) of the HPLMN.

- PCF Set ID.
- PCF Group ID of the UE's SUPI.

NOTE 1: The AMF can infer the PCF Group ID the UE's SUPI belongs to, based on the results of PCF discovery procedures with NRF. The AMF provides the PCF Group ID the SUPI belongs to to other PCF NF consumers as described in TS 23.502 [3].

- DNN replacement capability of the PCF.

When the NF service consumer performs discovery and selection for a PDU Session, the following applies:

- The SMF may utilize the NRF to discover the candidate PCF instance(s) for a PDU Session. In addition, PCF information may also be locally configured in the SMF. The SMF selects a PCF instance based on the available PCF instances obtained from the NRF or locally configured information in the SMF, depending on operator's policies.

  The following factors may be considered at PCF discovery and selection for a PDU session:

  a) Local operator policies.

  b) Selected Data Network Name (DNN).

  c) S-NSSAI of the PDU Session. In the LBO roaming case, the SMF selects the PCF instance based on the S-NSSAI of the VPLMN. In the home routed roaming case, the H-SMF selects the H-PCF instance based on the S-NSSAI of the HPLMN.

  d) SUPI; the SMF selects a PCF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for PCF discovery.

  e) PCF selected by the AMF for the UE.

  f) MA PDU Session capability of the PCF, for an MA PDU session.

  g) The PCF Group ID provided by the AMF to the SMF.

  h) PCF Set ID.

In the case of delegated discovery and selection in SCP, the SMF includes the factors b) - h), if available, in the first request.

The selected PCF instance for serving the UE and the selected PCF instance for serving a PDU session of this UE may be the same or may be different.

In the following scenarios, information about the PCF instance that has been selected i.e. the PCF ID and if available PCF Group ID may be forwarded to another NF. If the NF service consumer performs discovery and selection, this NF may use this PCF instance. In the case of delegated discovery and selection, this NF may include PCF ID and if available PCF Group ID in the request and the SCP may use this information to select the PCF instance (discovery may still be needed depending on what level of information is sent by the AMF, e.g. the address of the PCF instance may not be present):

When NF service consumer performs discovery and selection, the following applies:

- During AMF relocation, the target AMF may receive a PCF ID and if available the PCF Group ID from the source AMF to enable the usage of the same PCF by the target AMF, and the target AMF may decide based on operator policy either to use the same PCF or select a new PCF.
- The AMF may, based on operator policies, forward the selected PCF to SMF instance(s) during the PDU Session Establishment procedure(s) to enable the usage of the same PCF for the AMF and the SMF instance(s). The SMF may decide based on operator policy either to use the same PCF or select a new PCF.
- In the roaming case, the AMF may, based on operator policies, e.g. roaming agreement, select the H-PCF in addition to the V-PCF for a UE by performing the PCF discovery and selection as described above. The AMF sends the H-PCF ID of the selected H-PCF instance to the V-PCF during the policy association establishment procedure.

When the SMF receives a a redirection indication with PCF ID from the PCF for the PDU session, the SMF shall terminate the current SM Policy Control association and reselects a PCF based on the received PCF ID. The SMF shall then establish an SM Policy Control association with the reselected PCF.

In the case of delegated discovery and selection in the SCP, the following applies:

- The selected PCF instance may include the PCF Group ID in the response to the AMF.

NOTE 2: The selected (V-)PCF instance can include the binding indication, including the (V-)PCF ID and possibly PCF Set ID in the response to the AMF as described in clause 6.3.1.0.

- The AMF first establishes an AM policy association; when forwarding the related request message the SCP discovers and selects a PCF instance. Unless binding information is provided in the response to that request the SCP adds the NF function producer ID it selected, i.e. PCF ID, into the response and the AMF uses the received PCF ID and available binding information as discovery and selection parameters for the request to establish the UE policy association towards the SCP. The SCP selects the (V-)PCF instance for UE policy association based on the received discovery and selection parameters.

- During AMF relocation, the AMF may receive a PCF ID and if available a PCF Group ID from the source AMF to enable the usage of the same PCF instance by the AMF. The AMF may decide based on operator policy either to use the old PCF instance or select another PCF instance. If the AMF decides to use the old PCF, the AMF includes the PCF ID, and if available the PCF Group ID as received from the source AMF in the AM policy update request to the SCP.

- The AMF may, based on operator policies, forward the selected PCF ID and if available the PCF Group ID to the SMF during the PDU Session Establishment procedure to enable the usage of the same PCF for the AMF and the SMF. The SMF may include that information in the request in discovery and selection parameters to the SCP. The SCP may decide based on operator policy either to use the indicated PCF instance or select another PCF instance.

- In the roaming case, the AMF performs discovery and selection of the H-PCF from NRF as described in this clause. The AMF may indicate the maximum number of H-PCF instances to be returned from NRF, i.e. H-PCF selection at NRF. The AMF uses the received V-PCF ID and available binding information received during the AM policy association procedure to send the UE policy association establishment request, which also includes the H-PCF ID, to the SCP. The SCP discovers and selects the V-PCF. The V-PCF sends an UE policy association establishment request towards the HPLMN, which includes the H-PCF ID as a discovery and selection parameter to SCP.

6.3.7.2 Providing policy requirements that apply to multiple UE and hence to multiple PCF

An authorized Application Function may, via the NEF, provide policy requirements that apply to multiple UE(s) (which, for example, belong to group of UE(s) defined by subscription or to any UE). Such policy requirements shall apply to any existing or future PDU Sessions that match the parameters in the AF request, and they may apply to multiple PCF instance(s).

NOTE: Application Function influence on traffic routing described in clause 5.6.7 is an example of such requirement.

After relevant validation of the AF request (and possible parameter mapping), the NEF stores this request received from the AF into the selected UDR instance as the Data Subset of the Application data. The possible parameter mapping includes mapping UE (group) identifiers provided by the AF to identifiers used within the 5GC, e.g. from GPSI to SUPI and/or from External Group Identifier to Internal-Group Identifier. Parameter mapping may also include mapping from the identifier of the Application Function towards internal identifiers such as the DNN and/or the S-NSSAI.

PCF(s) that need to receive AF requests that targets a DNN (and slice), and/or a group of UEs subscribe to receive notifications from the UDR about such AF request information. The PCF(s) can be configured (e.g. by OAM) to subscribe to receive notification of such AF request information from the UDR(s). The PCF(s) take(s) the received AF request information into account when making policy decisions for existing and future relevant PDU Sessions. In the case of existing PDU Sessions, the policy decision of the PCF instance(s) may trigger a PCC rule(s) change from the PCF to the SMF.

The PCF subscription to notifications of AF requests described above may take place during PDU Session Establishment or PDU Session Modification, when the PCF(s) receive request(s) from the SMF for policy information

related to the DNN (and slice), and/or the Internal-Group Identifier of UEs. For the PCF(s) that have subscribed to such notifications, the UDR(s) notify the PCF(s) of any AF request update.

The NEF associates the AF request with information allowing to later modify or delete the AF request in the UDR; it associates the AF request with:

- When the AF request targets PDU Sessions established by "any UE": the DNN, the slicing information target of the AF request,
- When the request targets PDU Sessions established by UE(s) belonging to an Internal-Group: the DNN, the slicing information and the Internal-Group Identifier target of the application request.
- The AF transaction identifier in the AF request.

6.3.7.3 Binding an AF request targeting a UE address to the relevant PCF

Binding an AF request to the relevant PCF instance is described in TS 23.503 [45].

6.3.8 UDM discovery and selection

The NF consumer or the SCP performs UDM discovery to discover a UDM instance that manages the user subscriptions.

If the NF consumer performs discovery and selection, the NF consumers shall utilize the NRF to discover the UDM instance(s) unless UDM information is available by other means, e.g. locally configured on NF consumers. The UDM selection function in NF consumers selects a UDM instance based on the available UDM instances (obtained from the NRF or locally configured).

The UDM selection functionality is applicable to both 3GPP access and non-3GPP access.

The UDM selection functionality in NF consumer or in SCP should consider one of the following factors:

1. Home Network Identifier (e.g. MNC and MCC) of SUCI/SUPI, along with NID (provided by the NG-RAN) in the case of SNPN, and UE's Routing Indicator.

NOTE 1: The UE provides the Routing Indicator to the AMF as part of the SUCI as defined in TS 23.003 [19] during initial registration. The AMF provides the UE's Routing Indicator to other NF consumers (of UDM) as described in TS 23.502 [3].

NOTE 2: In the case of SNPN, the AMF uses the selected NID provided by the NG-RAN together with the selected PLMN ID (from SUCI/SUPI) as the SUCI/SUPI does not always include the NID.

When the UE's Routing Indicator is set to its default value as defined in TS 23.003 [19], the UDM NF consumer can select any UDM instance within the home network of the SUCI/SUPI.

2. UDM Group ID of the UE's SUPI.

NOTE 3: The AMF can infer the UDM Group ID the UE's SUPI belongs to, based on the results of UDM discovery procedures with NRF. The AMF provides the UDM Group ID the SUPI belongs to other UDM NF consumers as described in TS 23.502 [3].

3. SUPI or Internal Group ID; the UDM NF consumer selects a UDM instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI or Internal Group ID as input for UDM discovery.

4. GPSI or External Group ID; UDM NF consumers which manage network signalling not based on SUPI/SUCI (e.g. the NEF) select a UDM instance based on the GPSI or External Group ID range the UE's GPSI or External Group ID belongs to or based on the results of a discovery procedure with NRF using the UE's GPSI or External Group ID as input for UDM discovery.

In the case of delegated discovery and selection in SCP, NF consumer shall include one of these factors in the request towards SCP.

6.3.9 UDR discovery and selection

Multiple instances of UDR may be deployed, each one storing specific data or providing service to a specific set of NF consumers as described in clause 4.2.5.

If the NF service consumer performs discovery and selection, the NF consumer shall utilize the NRF to discover the appropriate UDR instance(s) unless UDR instance information is available by other means, e.g. locally configured on NF consumer. The UDR selection function in NF consumers is applicable to both 3GPP access and non-3GPP access. The NF consumer or the SCP shall select a UDR instance that contains relevant information for the NF consumer, e.g. UDM/SCP selects a UDR instance that contains subscription data, while NEF/SCP (when used to access data for exposure) selects a UDR that contains data for exposure; or PCF/SCP selects a UDR that contains Policy Data and/or Application Data.

The UDR selection function in UDR NF consumers considers the Data Set Identifier of the data to be managed in UDR (see UDR service definition in TS 23.502 [3] clause 5.2.12). Additionally, the UDR selection function in UDR NF consumers should consider one of the following factors when available to the UDR NF consumer:

1. UDR Group ID the UE's SUPI belongs to.
2. SUPI; e.g. the UDR NF consumer selects a UDR instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for UDR discovery.
3. GPSI or External Group ID; e.g. UDR NF consumers select a UDR instance based on the GPSI or External Group ID range the UE's GPSI or External Group ID belongs to or based on the results of a discovery procedure with NRF using the UE's GPSI or External Group ID as input for UDR discovery.

In the case of delegated discovery and selection, the NF consumer shall include the available factors in the request towards SCP.

6.3.10 SMSF discovery and selection

The SMSF selection function is supported by the AMF and is used to allocate an SMSF instance that shall manage the SMS.

If the "SMS supported" indication is included in the Registration Request by the UE, the AMF checks SMS subscription from the UDM for the UE on whether the SMS is allowed for the UE.

If the SMS is allowed and the UE Context stored in AMF includes an SMSF address, the AMF uses the SMSF address included in UE Context (according to Table 5.2.2.2.2-1 of TS 23.502 [3]).

If the SMS is allowed and the UE Context stored in AMF does not include an SMSF address, the AMF discovers and selects an SMSF to serve the UE.

The SMSF selection may be based on the following methods:

- SMSF instance(s) address(es) preconfigured in the AMF (i.e., SMSF FQDN or IP addresses); or
- SMSF information available in the serving PLMN if received from an old AMF or the UDM; or
- The AMF invokes Nnrf_NFDiscovery service operation from NRF to discover SMSF instance as described in clause 5.2.7.3.2 of TS 23.502 [3].

For roaming scenario, the AMF discovers and selects an SMSF in VPLMN.

If the NF consumer performs discovery and selection via NRF, the SMSF selection function in the NF consumer selects a SMSF instance based on the available SMSF instances obtained from the NRF.

In the case of delegated discovery and selection in SCP, the NF consumer shall include all available factors in the request towards SCP.

6.3.11 CHF discovery and selection

The CHF discovery and selection function is supported by the SMF, the AMF, the SMSF and the PCF. It is used by the SMF to select a CHF that manages the online charging or offline charging for a PDU Session of a subscriber. It is used

by the AMF to select a CHF that manages the online charging or offline charging for 5G connection and mobility of a subscriber. It is used by the SMSF to select a CHF that manages the online charging or offline charging for the SMS over NAS transactions of a subscriber. It is used by the PCF to select a CHF that manages the spending limits for a PDU Session of a subscriber.

For the PCF to select the CHF, the address(es) of the CHF, including the Primary CHF address and the Secondary CHF address, may be:

- stored in the UDR as part of the PDU Session policy control subscription information as defined in clause 6.2.1.3 of TS 23.503 [45].
- locally configured in the PCF based on operator policies.
- discovered using NRF as described in in clause 6.1 of TS 32.290 [67].

The address(es) of the CHF shall be applicable for all services provided by the CHF.

The CHF address(es) that a stored in the UDR or configured in the PCF may be complemented by the associated CHF instance ID(s) and CHF set ID(s) (see clause 6.3.1.0) stored or configured in the same location.

The CHF address(es) retrieved from the UDR and possible associated CHF instance ID(s) and CHF set ID(s) take precendence over the locally configured CHF address(es) and possible associated CHF instance ID(s) and CHF set ID(s), and over the CHF address(es) discoverred by the NRF. If no CHF address(es) is received from the UDR, the PCF selects, based on operator policies, either the CHF addresse(es) provided by NRF, or the locally configured CHF address(es) and possible associated CHF instance ID(s) and CHF set ID(s).

If the PCF has a CHF set ID but no CHF instance ID associated to the CHF address(es) in the same location, the CHF instance within the CHF set may change. If the PCF is not able to reach the CHF address(es), it should query the NRF for other CHF instances within the CHF set.

If the PCF received a CHF set ID and a CHF instance ID associated to the CHF address(es) in the same location, the CHF service instance within the CHF may change. If an PCF is not able to reach the CHF address(es), it should query the NRF for other CHF service instances within the CHF.

To enable the SMF to select the same CHF that is selected by the PCF for a PDU Session, the PCF provides the selected CHF address(es) and, if available, the associated CHF instance ID(s) and/or CHF set ID(s) in the PDU Session related policy information to the SMF as described in Table 6.4-1 of TS 23.503 [45] and the SMF applies them as defined in clause 5.1.8 of TS 32.255 [68]. Otherwise, the SMF selection of the CHF as defined in clause 5.1.8 of TS 32.255 [68] applies.

How the CHF is selected by the AMF is defined in clause 5.1.3 of TS 32.256 [114].

How the CHF is selected by the SMSF is defined in clause 5.4 of TS 32.274 [118].

If the NF consumer performs discovery and selection via NRF, the CHF selection function in NF consumers selects a CHF instance based on the available CHF instances obtained from the NRF.

The CHF selection functionality in NF consumer or in SCP should consider one of the following factors:

1. CHF Group ID of the UE's SUPI.

NOTE: The NF Consumer can infer the CHF Group ID the UE's SUPI belongs to, based on the results of CHF discovery procedures with NRF.

2. SUPI; the NF consumer selects a CHF instance based on the SUPI range the UE's SUPI belongs to or based on the results of a discovery procedure with NRF using the UE's SUPI as input for CHF discovery.

In the case of delegated discovery and selection in SCP, the NF consumer shall include all available factors in the request towards SCP.

6.3.12 Trusted Non-3GPP Access Network selection

6.3.12.1 General

Clause 6.3.12 specifies how a UE, which wants to establish connectivity via trusted non-3GPP access, selects a PLMN and a trusted non-3GPP access network (TNAN) to connect to. How the UE decides to use trusted non-3GPP access is not specified in this document. As an example, a UE may decide to use trusted non-3GPP access for connecting to 5GC in a specific PLMN based on:

- the UE implementation-specific criteria; or
- the UE configuration, e.g. the UE may be configured to try first the trusted non-3GPP access procedures; or
- the UE capabilities, e.g. the UE may support only the trusted non-3GPP access procedures; or
- the advertised capabilities of the discovered non-3GPP access networks, e.g. one or more available non-3GPP access networks advertise support of trusted connectivity to 5GC in a specific PLMN.

An example deployment scenario is schematically illustrated in Figure 6.3.12.1-1 below. In this scenario, the UE has discovered five non-3GPP access networks, which are WLAN access networks. These WLANs advertise information about the PLMNs they interwork with, e.g., by using the ANQP protocol, as defined in the HS2.0 specification [85]. Each WLAN may support "S2a connectivity" and/or "5G connectivity" to one or more PLMNs. Before establishing connectivity via trusted non-3GPP access, the UE needs to select (a) a PLMN, (b) a non-3GPP access network that provide trusted connectivity this this PLMN, and (c) a connectivity type, i.e. either "5G connectivity" or "S2a connectivity".

Each non-3GPP access network may advertise one or more of the following PLMN lists:

1) A PLMN List-1, which includes PLMNs with which "AAA connectivity" is supported. A non-3GPP access network supports "AAA connectivity" with a PLMN when it deploys an AAA function that can connect with a 3GPP AAA Server/Proxy in this PLMN, via an STa interface (trusted WLAN to EPC), or via an SWa interface (untrusted WLAN to EPC); see TS 23.402 [43].

2) A PLMN List-2, which includes PLMNs with which "S2a connectivity" is supported. A non-3GPP access network supports "S2a connectivity" with a PLMN when it deploys a TWAG function that can connect with a PGW in this PLMN, via an S2a interface; see TS 23.402 [43], clause 16.

3) A PLMN List-3, which includes PLMNs with which "5G connectivity" is supported. A non-3GPP access network supports "5G connectivity" with a PLMN when it deploys a TNGF function that can connect with an AMF function and an UPF function in this PLMN via N2 and N3 interfaces, respectively; see clause 4.2.8.

When the UE wants to discover the PLMN List(s) supported by a non-3GPP access network and the non-3GPP access network supports ANQP, the UE shall send an ANQP query to the non-3GPP access network requesting "3GPP Cellular Network" information. If the non-3GPP access network supports interworking with one or more PLMNs, the response received by the UE includes a "3GPP Cellular Network" information element containing one or more of the above three PLMN Lists. The PLMN List-1 and the PLMN List-2 are specified in TS 23.402 [43] and indicate support of interworking with EPC in one or more PLMNs. The PLMN List-3 is a list used to indicate support of interworking with 5GC in one or more PLMNs. When the non-3GPP access network does not support ANQP, how the UE discovers the PLMN List(s) supported by the non-3GPP access network is not defined in the present specification.

The UE determines if a non-3GPP access network supports "trusted connectivity" to a specific PLMN by receiving the PLMN List-2 and the PLMN List-3 advertised by this access network. If this PLMN is not included in any of these lists, then the non-3GPP access network can only support connectivity to an ePDG or N3IWF in the PLMN (i.e. "untrusted connectivity").

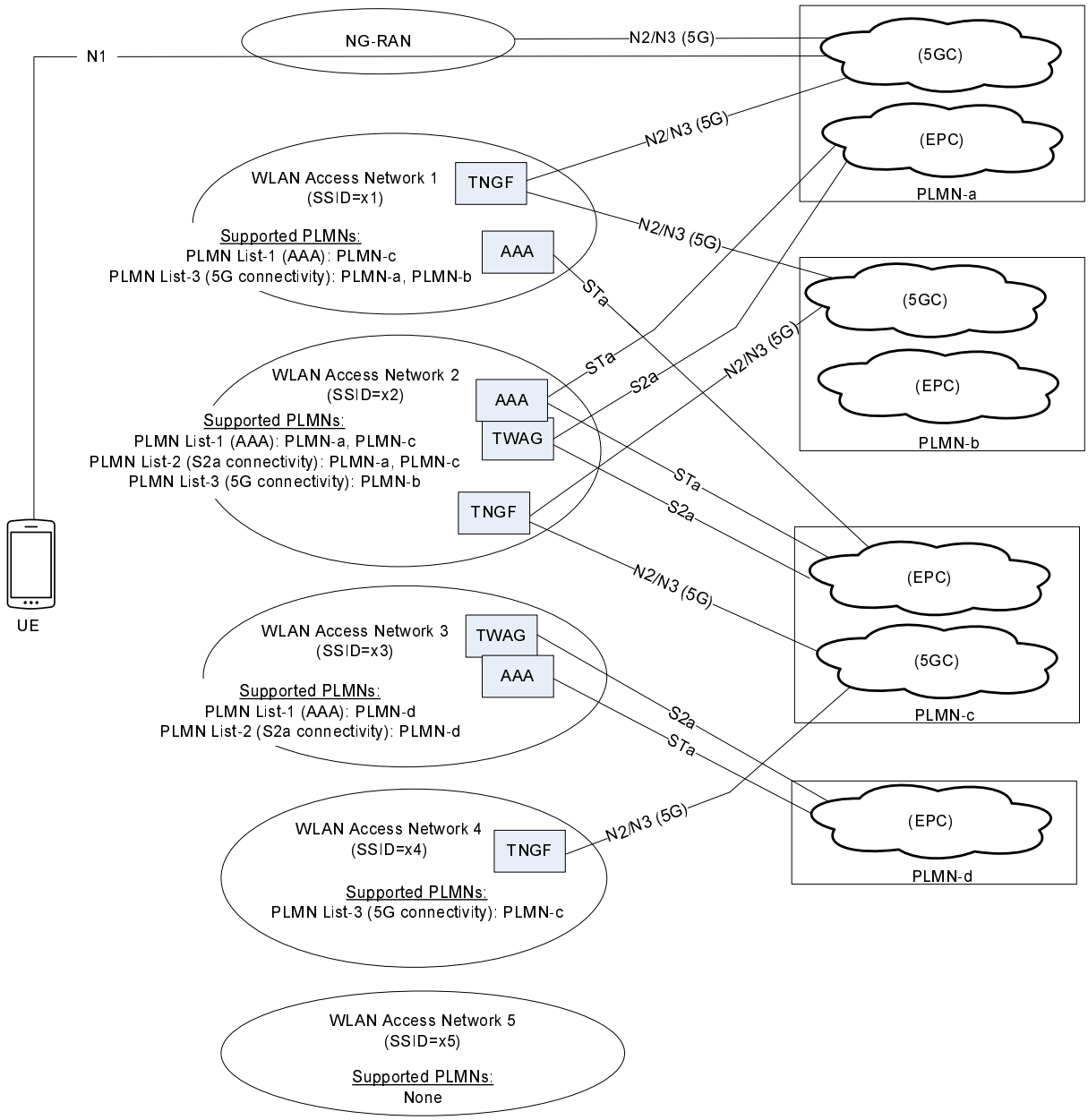


Figure 6.3.12.1-1: Example deployment scenario for trusted Non-3GPP access network selection

6.3.12.2 Access Network Selection Procedure

The steps below specify the steps executed by the UE when the UE wants to select and connect to a PLMN over trusted non-3GPP access. Note that the UE executes these steps before connecting to a trusted non-3GPP access network. This is different from the untrusted non-3GPP access (see clause 6.3.6, "N3IWF selection"), where the UE first connects to a non-3GPP access network, it obtains IP configuration and then proceeds to PLMN selection and ePDG/N3IWF selection. In the case of trusted non-3GPP access, the UE uses 3GPP-based authentication for connecting to a non-3GPP access, so it must first select a PLMN and then attempt to connect to a non-3GPP access.

Step 1: The UE constructs a list of available PLMNs, with which trusted connectivity is supported. This list contains the PLMNs included in the PLMN List-2 and PLMN List-3, advertised by all discovered non-3GPP access networks. For each PLMN the supported type(s) of trusted connectivity is also included.

a. In the example shown in Figure 6.3.12.1-1, the list of available PLMNs includes:

- PLMN-a: "S2a connectivity", "5G connectivity"
- PLMN-b: "5G connectivity"

- PLMN-c: "S2a connectivity", "5G connectivity"
- PLMN-d: "S2a connectivity"

Step 2:The UE selects a PLMN that is included in the list of available PLMNs, as follows:

a. If the UE is connected to a PLMN via 3GPP access and this PLMN is included in the list of available PLMNs, the UE selects this PLMN. If this PLMN is not included in the list of available PLMNs, but it is included in the "Non-3GPP access node selection information" in the UE (see clause 6.3.6.1), the UE selects this PLMN and executes the combined ePDG/N3IWF selection procedure specified in clause 6.3.6.3.

b. Otherwise (the UE is not connected to a PLMN via 3GPP access, or the UE is connected to a PLMN via 3GPP access but this PLMN is neither in the list of available PLMNs nor in the "Non-3GPP access node selection information"), the UE determines the country it is located in by using implementation specific means.

   i) If the UE determines to be located in its home country, then:

      - The UE selects the HPLMN, if included in the list of available PLMNs. Otherwise, the UE selects an E-HPLMN (Equivalent HPLMN), if an E-HPLMN is included in the list of available PLMNs. If the list of available PLMNs does not include the HPLMN and does not include an E-HPLMN, the UE stops the procedure and may attempt to connect via untrusted non-3GPP access (i.e. it may execute the N3IWF selection procedure specified in clause 6.3.6).

   ii) If the UE determines to be located in a visited country, then:

      - The UE determines if it is mandatory to select a PLMN in the visited country, as follows:

        - If the UE has IP connectivity (e.g. the UE is connected via 3GPP access), the UE sends a DNS query and receives a DNS response that indicates if a PLMN must be selected in the visited country. The DNS response includes also a lifetime that denotes how long the DNS response can be cached for. The FQDN in the DNS query shall be different from the Visited Country FQDN (see TS 23.003 [19]) that is used for ePDG/N3IWF selection. The DNS response shall not include a list of PLMNs that support trusted connectivity in the visited country, but shall only include an indication of whether a PLMN must be selected in the visited country or not.

        - If the UE has no IP connectivity (e.g. the UE is not connected via 3GPP access), then the UE may use a cached DNS response that was received in the past, or may use local configuration that indicates which visited countries mandate a PLMN selection in the visited country.

      - If the UE determines that it is not mandatory to select a PLMN in the visited country, and the HPLMN or an E-HPLMN is included in the list of available PLMNs, then the UE selects the HPLMN or an E-HPLMN, whichever is included in the list of available PLMNs.

      - Otherwise, the UE selects a PLMN in the visited country by considering, in priority order, the PLMNs, first, in the User Controlled PLMN Selector list and, next, in the Operator Controlled PLMN Selector list (see TS 23.122 [17]). The UE selects the highest priority PLMN in a PLMN Selector list that is also included in the list of available PLMNs;

        - If the list of available PLMNs does not include a PLMN that is also included in a PLMN Selector list, the UE stops the procedure and may attempt to connect via untrusted non-3GPP access.

c. In the example shown in Figure 6.3.12.1-1, the UE may select PLMN-c, for which "S2a connectivity" and "5G connectivity" is supported.

Step 3:The UE selects the type of trusted connectivity ("S2a connectivity" or "5G connectivity") for connecting to the selected PLMN, as follows:

a. If the list of available PLMNs indicates that both "S2a connectivity" and "5G connectivity" is supported for the selected PLMN, then the UE shall select "5G connectivity" because it is the preferred type of trusted access.

b. Otherwise, if the list of available PLMNs indicates that only one type of trusted connectivity (either "S2a connectivity" or "5G connectivity") is supported for the selected PLMN, the UE selects this type of trusted connectivity.

c. In the example shown in Figure 6.3.12.1-1, the UE may select PLMN-c and "5G connectivity". There are two non-3GPP access networks that support "5G connectivity" to PLMN-c: the WLAN access network 2 and the WLAN access network 4.

Step 4: Finally, the UE selects a non-3GPP access network to connect to, as follows:

a. The UE puts the available non-3GPP access networks in priority order. For WLAN access, the UE constructs this prioritized list by using the WLANSP rules (if provided). For other types of non-3GPP access, the UE may use access specific information to construct this prioritized list.

b. From the prioritized list of non-3GPP access networks, the UE selects the highest priority non-3GPP access network that supports the selected type of trusted connectivity to the selected PLMN.

c. In the example shown in Figure 6.3.12.1-1, the UE selects either the WLAN access network 2 or the WLAN access network 4, whichever has the highest priority in the prioritized list of non-3GPP access networks.

d. Over the selected non-3GPP access network, the UE starts the 5GC registration procedure specified in TS 23.502, clause 4.12a.2.2.

6.3.12a Access Network selection for devices that do not support 5GC NAS over WLAN

6.3.12a.1 General

As specified in clause 4.2.8.5, devices that do not support 5GC NAS signalling over WLAN access (referred to as "Non-5G-Capable over WLAN" devices, or N5CW devices for short), may access 5GC in a PLMN via a trusted WLAN access network that supports a TWIF function. The following clause specifies (a) how a N5CW device selects a PLMN and (b) how it selects a trusted WLAN access network that can provide "5G connectivity-without-NAS" to the selected PLMN. This selection procedure is called access network selection.

Each WLAN access network that provides "5G connectivity-without-NAS" advertises with ANQP a list of PLMNs with which "5G connectivity-without-NAS" is supported. This list is called PLMN List-4, and is different from the PLMN List-1, PLMN List-2 and PLMN List-3 defined in clause 6.3.12. A WLAN advertises the PLMN List-4, when the WLAN supports a TWIF function.

6.3.12a.2 Access Network Selection Procedure

The steps executed by a N5CW device for access network selection are specified below and are very similar with the corresponding steps executed by a UE that supports NAS; see clause 6.3.12.2.

Step 1: The N5CW device constructs a list of available PLMNs. This list contains the PLMNs included in the PLMN List-4 advertised by all discovered WLAN access networks.

a. The N5CW device discovers the PLMN List-4 advertised by all discovered WLAN access networks by sending an ANQP query to each discovered WLAN access network. The ANQP query shall request "3GPP Cellular Network" information. If a WLAN access network supports interworking with one or more PLMNs, the ANQP response received by the N5CW device includes a "3GPP Cellular Network" information element containing one or more of the following lists: PLMN List-1, PLMN List-2, PLMN List-3 and PLMN List-4. The PLMN List-1, PLMN List-2 and PLMN List-3 are defined in clause 6.3.12. The PLMN List-4 includes the PLMNs with which "5G connectivity-without-NAS" is supported.

Step 2: The N5CW device selects a PLMN that is included in the list of available PLMNs as follows.

a. If the N5CW device is connected to a PLMN via 3GPP access and this PLMN is included in the list of available PLMNs, then the N5CW device selects this PLMN.

b. Otherwise (the N5CW device is not connected to a PLMN via 3GPP access, or the N5CW device is connected to a PLMN via 3GPP access but this PLMN is not in the list of available PLMNs):

i) If the N5CW device determines to be located in its home country, then:

- The N5CW device selects the HPLMN if the N5CW device has a USIM or is pre-configured with an HPLMN, if the HPLMN is included in the list of available PLMNs. Otherwise, the N5CW device

selects an E-HPLMN (Equivalent HPLMN), if an E-HPLMN is included in the list of available PLMNs. If the list of available PLMNs does not include the HPLMN and does not include an E-HPLMN, the N5CW device stops the access network selection procedure.

ii) If the N5CW device determines to be located in its visited country, then:

- The N5CW device determines if it is mandatory to select a PLMN in the visited country, as follows:
  - If the N5CW device has IP connectivity (e.g. it is connected via 3GPP access), the N5CW device sends a DNS query and receives a DNS response that indicates if a PLMN must be selected in the visited country. The DNS response includes a lifetime that denotes how long the DNS response can be cached.
  - If the N5CW device has no IP connectivity (e.g. it is not connected via 3GPP access), then the N5CW device may use a cached DNS response that was received in the past, or may use local configuration that indicates which visited countries mandate a PLMN selection in the visited country.
- If the N5CW device determines that it is not mandatory to select a PLMN in the visited country, and the HPLMN or an E-HPLMN is included in the list of available PLMNs, then the N5CW device selects the HPLMN or an E-HPLMN, whichever is included in the list of available PLMNs.
- Otherwise, the N5CW device selects a PLMN in the visited country as follows:
  - If the N5CW device has a USIM, the UE selects a PLMN in the visited country by considering, in priority order, the PLMNs, first, in the User Controlled PLMN Selector list and, next, in the Operator Controlled PLMN Selector list (see TS 23.122 [17]).
  - If the N5CW device does not have a USIM, the N5CW device selects the highest priority PLMN in a pre-configured list, which is also included in the list of available PLMNs.
  - If the list of available PLMNs does not include a PLMN that is also included in the pre-configured list(s), the N5CW device either stops the access network selection procedure, or may select a PLMN based on its own implementation.

Step 3:Finally, the N5CW device selects a WLAN access network (e.g. an SSID) to connect to, as follows:

a. The N5CW device puts the available WLAN access networks in priority order. The N5CW device constructs this prioritized list by using the WLANSP rules (if they have been received via 3GPP access), or any other implementation specific means.

b. From the prioritized list of WLAN access networks, the N5CW device selects the highest priority WLAN access network that supports "5G connectivity-without-NAS" to the PLMN selected in step 2.

After the N5CW device completes the above access network selection procedure, the N5CW device initiates the "Initial Registration and PDU Session Establishment" procedure specified in TS 23.502, clause 4.12b.2.

6.3.13 NWDAF discovery and selection

Multiple instances of NWDAF may be deployed in a network.

The NF consumers shall utilize the NRF to discover NWDAF instance(s) unless NWDAF information is available by other means, e.g. locally configured on NF consumers. The NWDAF selection function in NF consumers selects an NWDAF instance based on the available NWDAF instances.

The following factors may be considered by the NF consumer for NWDAF selection:

- S-NSSAI.
- Analytics ID(s).
- NWDAF Serving Area information, i.e. list of TAIs for which the NWDAF can provide analytics.

6.3.14 NEF Discovery

The NF consumers may utilize the NRF to discover NEF instance(s) unless NEF information is available by other means, e.g. locally configured in NF consumers. The NRF provides NF profile(s) of NEF instance(s) to the NF consumers.

NOTE: The NEF discovery and selection procedures described in this clause are intended to be applied by NF consumers deployed within the operator's domain.

The following factors may be considered for NEF selection:

- S-NSSAI(s).
- Event ID(s) supported by AF (see clause 6.2.6, TS 23.288 [86] clause 6.2.2.3 and TS 23.502 [3] clause 5.2.19).
- AF Instance ID, Application ID.
- External Identifier, External Group Identifier, or domain name.

6.3.15 UCMF Discovery and Selection

The AMF, MME, NEF, AF, SCEF, SCS/AS may utilize the NRF to discover UCMF instance(s) unless UCMF information is available by other means, e.g. locally configured in UCMF services consumers.

In the case of delegated discovery and selection in SCP, the NF consumer shall forward the request towards SCP.

6.3.16 SCP discovery and selection

An NF is configured with its serving SCP(s).

In a deployment where several SCPs are deployed, a message may traverse several SCP instances until reaching its final destination. A SCP may discover and select a next hop SCP by querying the Nnrf_NFDiscovery Service of the NRF or it may be configured with next SCP in the message path.

An SCP may use the SCP profile parameters in clause 6.2.6.3 as discovery parameters in Nnrf_NFDiscovery. The parameter(s) to be used depend(s) on network deployment. The NRF returns a list SCP Profiles as per the provided discovery parameters.

If an SCP receives a Routing Binding Indication within a service or notification request and decides to forward that request to a next-hop SCP, it shall include the Routing Binding Indication in the forwarded request.

NOTE: It is up to SCP implementation, deployment specific configuration and operator policies as to how the SCP will use information retrieved from the NRF to resolve the optimal route to a producer.

Based on SCP configuration, an SCP deciding to address a next-hop SCP for a service request may then delegate the NF (instance) and/or service (instance) selection to subsequent SCPs and provide discovery and selection parameters to the next-hop SCP.

6.3.17 NSSAAF discovery and selection

In the case of NF consumer based discovery and selection, the following applies:

- The AMF performs NSSAAF selection to select an NSSAAF Instance that supports network slice specific authentication between the UE and the AAA-S associated with the HPLMN. The AMF shall utilize the NRF to discover the NSSAAF instance(s) unless NSSAAF information is available by other means, e.g. locally configured on AMF. The NSSAAF selection function in the AMF selects an NSSAAF instance based on the available NSSAAF instances (obtained from the NRF or locally configured in the AMF).

NSSAAF selection is applicable to both 3GPP access and non-3GPP access.

The NSSAAF selection function in NSSAAF NF consumers or in SCP should consider the following factor when it is available:

1. For roaming subscribers, Home Network Identifier (e.g., MNC and MCC) of SUPI (by an NF consumer in the Serving network).

In the case of delegated discovery and selection in SCP, the NSSAAF NF consumer shall send all available factors to the SCP.

7 Network Function Services and descriptions

7.1 Network Function Service Framework

7.1.1 General

Service Framework functionalities include e.g. service registration/de-registration, consumer authorization, service discovery, and inter service communication, which include selection and message passing. Four communication options are listed in Annex E and can all co-exist within one and the same network.

An NF service is one type of capability exposed by an NF (NF Service Producer) to other authorized NF (NF Service Consumer) through a service-based interface. A Network Function may expose one or more NF services. Following are criteria for specifying NF services:

- NF services are derived from the system procedures that describe end-to-end functionality, where applicable (see TS 23.502 [3], Annex B drafting rules). Services may also be defined based on information flows from other 3GPP specifications.

- System procedures can be described by a sequence of NF service invocations.

NF services may communicate directly between NF Service consumers and NF Service Producers, or indirectly via an SCP. Direct and Indirect Communication are illustrated in Figure 7.1.1-1. For more information, see Annex E and clauses 6.3.1 and 7.1.2. Whether a NF Service Consumer (e.g. in the case of requests or subscriptions) or NF Service Producer (e.g. in the case of notifications) uses Direct Communication or Indirect Communication by using an SCP is based on the local configuration of the NF Service Consumer/NF Service Producer. An NF may not use SCP for all its communication based on the local configuration.

NOTE: The SCP can be deployed in a distributed manner.

In Direct Communication, the NF Service consumer performs discovery of the target NF Service producer by local configuration or via NRF. The NF Service consumer communicates with the target NF Service producer directly.

In Indirect Communication, the NF Service consumer communicates with the target NF Service producer via a SCP. The NF Service consumer may be configured to perform discovery of the target NF Service producer directly, or delegate the discovery of the target NF Service Producer to the SCP used for Indirect Communication. In the latter case, the SCP uses the parameters provided by NF Service consumer to perform discovery and/or selection of the target NF Service producer. The SCP address may be locally configured in NF Service consumer.

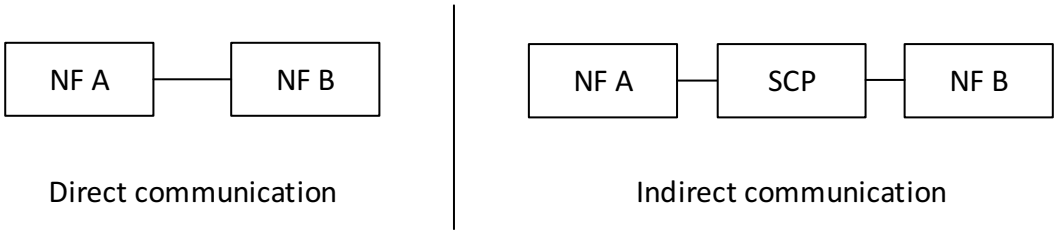


Figure 7.1.1-1: NF/NF service inter communication

7.1.2 NF Service Consumer - NF Service Producer interactions

The end-to-end interaction between two Network Functions (Consumer and Producer) within this NF service framework follows two mechanisms, irrespective of whether Direct Communication or Indirect Communication is used:

- "Request-response": A Control Plane NF_B (NF Service Producer) is requested by another Control Plane NF_A (NF Service Consumer) to provide a certain NF service, which either performs an action or provides information or both. NF_B provides an NF service based on the request by NF_A. In order to fulfil the request, NF_B may in turn consume NF services from other NFs. In Request-response mechanism, communication is one to one between two NFs (consumer and producer) and a one-time response from the producer to a request from the consumer is expected within a certain timeframe. The NF Service Producer may also add a Binding Indication (see clause 6.3.1.0) in the Response, which may be used by the NF Service Consumer to select suitable NF service producer instance(s) for subsequent requests. For indirect communication, the NF Service Consumer copies the Binding Indication into the Routing Binding indication, that is included in subsequent requests, to be used by the SCP to discover a suitable NF service producer instance(s).

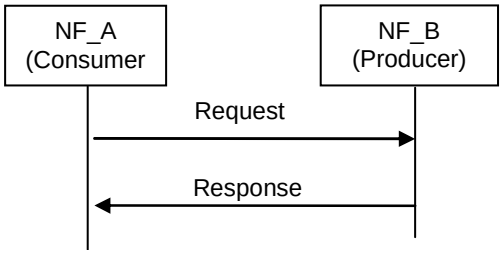


Figure 7.1.2-1: "Request-response" NF Service illustration

- "Subscribe-Notify": A Control Plane NF_A (NF Service Consumer) subscribes to NF Service offered by another Control Plane NF_B (NF Service Producer). Multiple Control Plane NFs may subscribe to the same Control Plane NF Service. NF_B notifies the results of this NF service to the interested NF(s) that subscribed to this NF service. The subscription request shall include the notification endpoint, i.e. Notification Target Address) and a Notification Correlation ID (e.g. the notification URL) of the NF Service Consumer to which the event notification from the NF Service Producer should be sent to.

NOTE 1: The notification endpoint URL can contain both the notification endpoint and the Notification Correlation ID.

The NF Service Consumer may add a Binding Indication (see clause 6.3.1.0) in the subscribe request, which may be used by the NF Service Producer to discover a suitable notification endpoint. For indirect communication, the NF Service Producer copies the Binding Indication into the Routing Binding Indication, that is included in the response, to be used by the SCP to discover a suitable notification target. The NF Service Producer may also add a Binding Indication (see clause 6.3.1.0) in the subscribe response, which may be used by the NF Service Consumer (or SCP) to select suitable NF service producer instance(s) or NF producer service instance. In addition, the subscription request may include notification request for periodic updates or notification triggered through certain events (e.g., the information requested gets changed, reaches certain threshold etc.). The subscription for notification can be done through one of the following ways:

- Explicit subscription: A separate request/response exchange between the NF Service Consumer and the NF Service Producer; or

- Implicit subscription: The subscription for notification is included as part of another NF service operation of the same NF Service; or

- Default notification endpoint: Registration of a notification endpoint for each type of notification the NF consumer is interested to receive, as a NF service parameter with the NRF during the NF and NF service Registration procedure as specified in TS 23.502 [3] clause 4.17.1.

The NF Service Consumer may also add a Binding Indication (see clause 6.3.1.0) in the response to the notification request, which may be used by the NF Service Producer to discover a suitable notification endpoint. For indirect communication, the NF Service Producer copies the Binding Indication into the Routing Binding indication that is included in subsequent notfication requests. The binding indication is then used by the SCP to discover a suitable notification target.

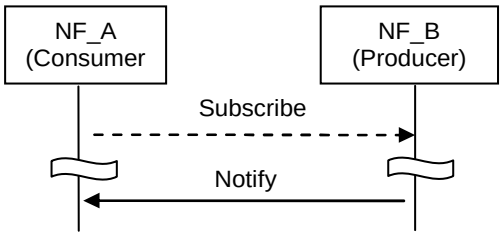


Figure 7.1.2-2: "Subscribe-Notify" NF Service illustration 1

A Control Plane NF_A may also subscribe to NF Service offered by Control Plane NF_B on behalf of Control Plane NF_C, i.e. it requests the NF Service Producer to send the event notification to another consumer(s). In this case, NF_A includes the notification endpoint, i.e. Notification Target Address) and a Notification Correlation ID, of the NF_C in the subscription request. NF_A may also additionally include the notification endpoint and a Notification Correlation ID of NF A associated with subscription change related Event ID(s), e.g. Subscription Correlation ID Change, in the subscription request, so that NF_A can receive the notification of the subscription change related event. The NF_A may add Binding Indication (see clause 6.3.1.0) in the subscribe request.

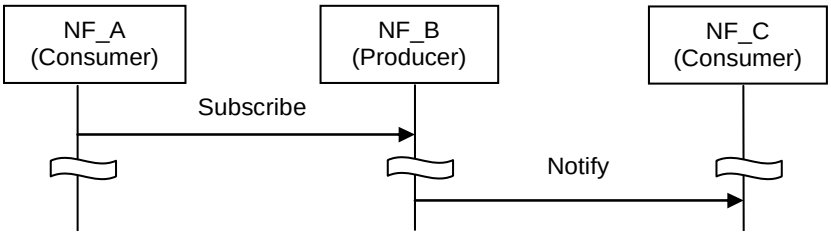


Figure 7.1.2-3: "Subscribe-Notify" NF Service illustration 2

Routing of the messages for the NF interaction mechanisms above may be direct, as shown in the figures 7.1.2-1 to 7.1.2-3, or indirect. In the case of Indirect Communication, an SCP is employed by the NF service consumer. The SCP routes messages between NF service consumers and NF service producers based on the Routing Binding Indication if available, and may do discovery and associated selection of the NF service producer on behalf of a NF service consumer. Figure 7.1.2-4 shows the principle for a request-response interaction and figure 7.1.2-5 shows an example of a subscribe-notify interaction.

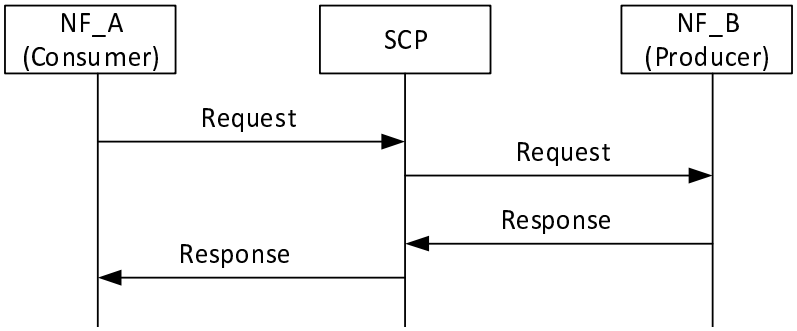


Figure 7.1.2-4: Request response using Indirect Communication

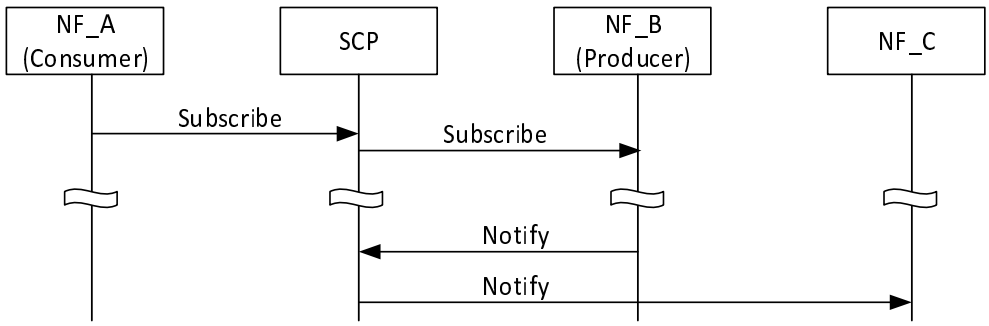


Figure 7.1.2-5: Subscribe-Notify using Indirect Communication

NOTE: The subscribe request and notify request can be routed by different SCPs.

7.1.3 Network Function Service discovery

A Control Plane Network function (NF) within the 5G Core network may expose its capabilities as services via its service based interface, which can be re-used by Control Plane CN NFs.

The NF service discovery enables a CN NF or SCP to discover NF instance(s) that provide the expected NF service(s). The NF service discovery is implemented via the NF discovery functionality.

For more detail NF discovery refer to clause 6.3.1.

7.1.4 Network Function Service Authorization

NF service authorization shall ensure the NF Service Consumer is authorized to access the NF service provided by the NF Service Provider, according to e.g. the policy of NF, the policy from the serving operator, the inter-operator agreement.

Service authorization information shall be configured as one of the components in NF profile of the NF Service Producer. It shall include the NF type (s) and NF realms/origins allowed to consume NF Service(s) of NF Service Producer.

Due to roaming agreements and operator policies, a NF Service Consumer shall be authorised based on UE/subscriber/roaming information and NF type, the Service authorization may entail two steps:

- Check whether the NF Service Consumer is permitted to discover the requested NF Service Producer instance during the NF service discovery procedure. This is performed on a per NF granularity by NRF.

NOTE 1: When NF discovery is performed based on local configuration, it is assumed that locally configured NFs are authorized.

- Check whether the NF Service Consumer is permitted to access the requested NF Service Producer for consuming the NF service, with a request type granularity. This is performed on a per UE, subscription or roaming agreements granularity. This type of NF Service authorization shall be embedded in the related NF service logic.

NOTE 2: The security of the connection between NF Service Consumer and NF Service Producer is specified in TS 33.501 [29].

NOTE 3: It is expected that an NF authorization framework exists in order to perform consumer NF authorization considering UE, subscription or roaming agreements granularity. This authorization is assumed to be performed without configuration of the NRF regarding UE, subscription or roaming information.

7.1.5 Network Function and Network Function Service registration and de-registration

For the NRF to properly maintain the information of available NF instances and their supported services, each NF instance informs the NRF of the list of NF services that it supports.

NOTE: The NF informs the appropriate NRF based on configuration.

The NF instance may make this information available to NRF when the NF instance becomes operative for the first time (registration operation) or upon individual NF service instance activation/de-activation within the NF instance (update operation) e.g. triggered after a scaling operation. The NF instance while registering the list of NF services it supports, for each NF service, may provide a notification endpoint information for each type of notification service that the NF service is prepared to consume, to the NRF during the NF instance registration. The NF instance may also update or delete the NF service related parameters (e.g. to delete the notification endpoint information). Alternatively, another authorised entity (such as an OA&M function) may inform the NRF on behalf of an NF instance triggered by an NF service instance lifecycle event (register or de-registration operation depending on instance instantiation, termination, activation, or de-activation). Registration with the NRF includes capacity and configuration information at time of instantiation.

The NF instance may also de-registers from the NRF when it is about to gracefully shut down or disconnect from the network in a controlled way. If an NF instance become unavailable or unreachable due to unplanned errors (e.g. NF crashes or there are network issues), an authorised entity shall de-register the NF instance with the NRF.

7.2 Network Function Services

7.2.1 General

In the context of this specification, an NF service is offering a capability to authorised consumers.

Network Functions may offer different capabilities and thus, different NF services to distinct consumers. Each of the NF services offered by a Network Function shall be self-contained, reusable and use management schemes independently of other NF services offered by the same Network Function (e.g. for scaling, healing, etc).

The discovery of the NF instance and NF service instance is specified in clause 6.3.1.

NOTE 1: There can be dependencies between NF services within the same Network Function due to sharing some common resources, e.g. context data. This does not preclude that NF services offered by a single Network Function are managed independently of each other.

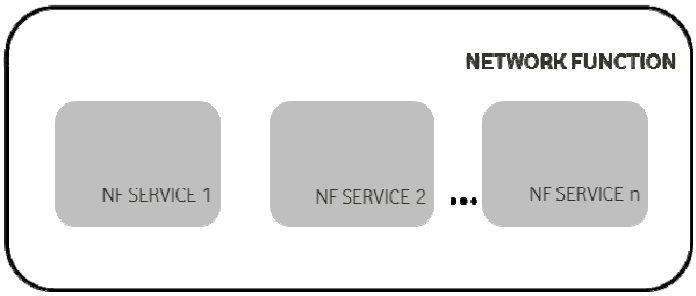


Figure 7.2.1-1: Network Function and NF Service

Each NF service shall be accessible by means of an interface. An interface may consist of one or several operations.

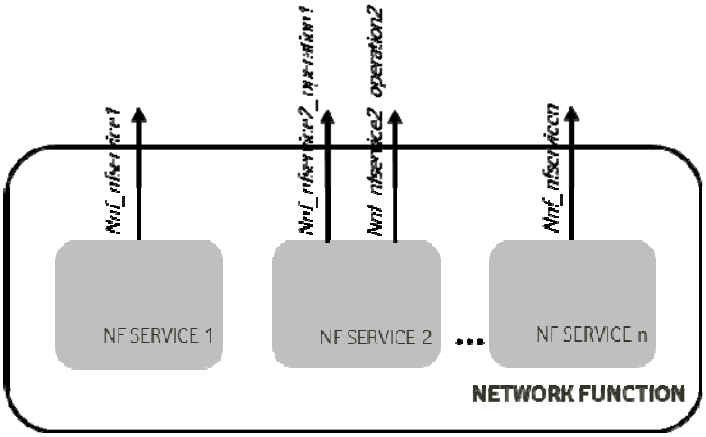


Figure 7.2.1-2: Network Function, NF Service and NF Service Operation

System procedures, as specified in TS 23.502 [3] can be built by invocation of a number of NF services. The following figure shows an illustrative example on how a procedure can be built; it is not expected that system procedures depict the details of the NF Services within each Network Function.

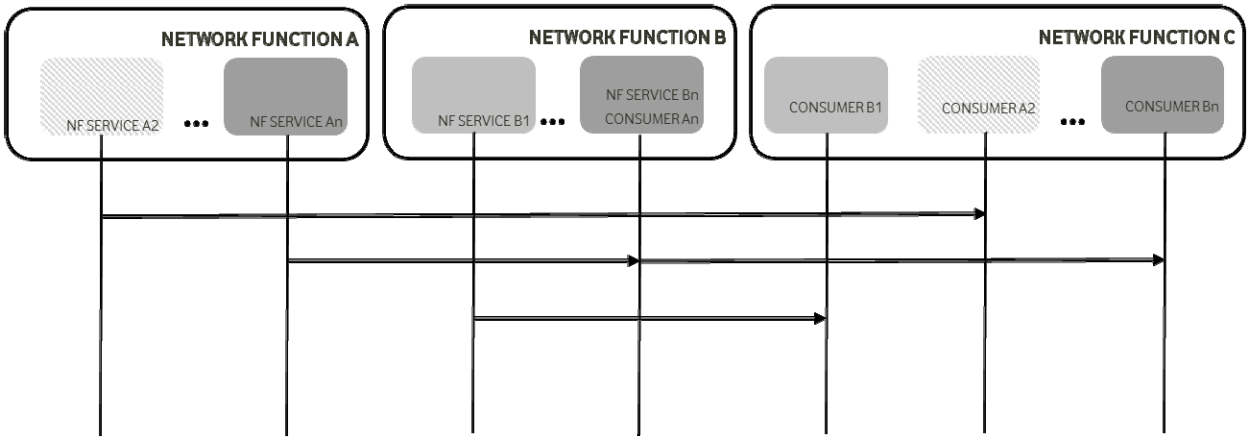


Figure 7.2.1-3: System Procedures and NF Services

NOTE 2: The SCP can be used for indirect communication between NF/NF service instances. For simplicity the SCP is not shown in the procedure.

The following clauses provide for each NF the NF services it exposes through its service based interfaces.

7.2.2 AMF Services

The following NF services are specified for AMF:

Table 7.2.2-1: NF Services provided by AMF

Service Name	Description	Reference in TS 23.502 [3]
Namf_Communication	Enables an NF consumer to communicate with the UE and/or the AN through the AMF. This service enables SMF to request EBI allocation to support interworking with EPS. This service also supports PWS functionality as described in TS 23.041 [46].	5.2.2.2
Namf_EventExposure	Enables other NF consumers to subscribe or get notified of the mobility related events and statistics.	5.2.2.3
Namf_MT	Enables an NF consumer to make sure UE is reachable.	5.2.2.4
Namf_Location	Enables an NF consumer to request location information for a target UE.	5.2.2.5

7.2.3 SMF Services

The following NF services are specified for SMF:

Table 7.2.3-1: NF Services provided by SMF

Service Name	Description	Reference in TS 23.502 [3]
Nsmf_PDUSession	This service manages the PDU Sessions and uses the policy and charging rules received from the PCF. The service operations exposed by this NF service allows the consumer NFs to handle the PDU Sessions.	5.2.8.2
Nsmf_EventExposure	This service exposes the events happening on the PDU Sessions to the consumer NFs.	5.2.8.3
Nsmf_NIDD	This service is used for NIDD transfer between SMF and another NF.	5.2.8.4

7.2.4 PCF Services

The following NF services are specified for PCF:

Table 7.2.4-1: NF Services provided by PCF

Service Name	Description	Reference in TS 23.502 [3]
Npcf_AMPolicyControl	This PCF service provides Access Control, network selection and Mobility Management related policies, UE Route Selection Policies to the NF consumers.	5.2.5.2
Npcf_SMPolicyControl	This PCF service provides session related policies to the NF consumers.	5.2.5.4
Npcf_PolicyAuthorization	This PCF service authorises an AF request and creates policies as requested by the authorised AF for the PDU Session to which the AF session is bound to. This service allows the NF consumer to subscribe/unsubscribe to the notification of Access Type and RAT type, PLMN identifier, access network information, usage report etc.	5.2.5.3
Npcf_BDTPolicyControl	This PCF service provides background data transfer policy negotiation and optionally notification for the renegotiation to the NF consumers.	5.2.5.5
Npcf_UEPolicyControl	This PCF service provides the management of UE Policy Association to the NF consumers.	5.2.5.6
Npcf_EventExposure	This PCF service provide the support for event exposure.	5.2.5.7

7.2.5 UDM Services

The following NF services are specified for UDM:

Table 7.2.5-1: NF Services provided by UDM

Service Name	Description	Reference in TS 23.502 [3]
Nudm_UECM	1. Provide the NF consumer of the information related to UE's transaction information, e.g. UE's serving NF identifier, UE status, etc. 2. Allow the NF consumer to register and deregister its information for the serving UE in the UDM. 3. Allow the NF consumer to update some UE context information in the UDM.	5.2.3.2
Nudm_SDM	1. Allow NF consumer to retrieve user subscription data when necessary. 2. Provide updated user subscriber data to the subscribed NF consumer.	5.2.3.3
Nudm_UEAuthentication	1. Provide updated authentication related subscriber data to the subscribed NF consumer. 2. For AKA based authentication, this operation can be also used to recover from security context synchronization failure situations. 3. Used for being informed about the result of an authentication procedure with a UE.	5.2.3.4
Nudm_EventExposure	1. Allow NF consumer to subscribe to receive an event. 2. Provide monitoring indication of the event to the subscribed NF consumer.	5.2.3.5
Nudm_ParameterProvision	1. To provision information which can be used for the UE in 5GS.	5.2.3.6
Nudm_NIDDAuthorisation	1. To authorise an NIDD configuration request for the received External Group Identifier or GPSI.	5.2.3.7

7.2.6 NRF Services

The following NF services are specified for NRF:

Table 7.2.6-1: NF Services provided by NRF

Service Name	Description	Reference in TS 23.502 [3]
Nnrf_NFManagement	Provides support for register, deregister and update service to NF, NF services, SCP. Provide consumers and SCP with notifications of newly registered/updated/deregistered NF along with its NF services.	5.2.7.2
Nnrf_NFDiscovery	Enables one NF service consumer or SCP to discover a set of NF instances with specific NF service or a target NF type. Also enables one NF service consumer or SCP to discover a specific NF service. Also enables a SCP to discover a next hop SCP.	5.2.7.3
Nnrf_AccessToken	Provides OAuth2 2.0 Access Tokens for NF to NF authorization as defined in TS 33.501 [29].	5.2.7.4

7.2.7 AUSF Services

The following NF services are specified for AUSF:

Table 7.2.7-1: NF Services provided by AUSF

Service Name	Description	Reference in TS 23.502 [3]
Nausf UEauthentication	The AUSF provides UE authentication service to requester NF. For AKA based authentication, this operation can also be used to recover from security context synchronization failure situations.	5.2.10.2
Nausf_SoRProtection	The AUSF provides protection of Steering of Roaming information service to the requester NF.	5.2.10.3

7.2.8 NEF Services

The following NF services are specified for NEF:

Table 7.2.8-1: NF Services provided by NEF

Service Name	Description	Reference in TS 23.502 [3]
Nnef_EventExposure	Provides support for event exposure.	5.2.6.2
Nnef_PFDManagement	Provides support for PFDs management.	5.2.6.3
Nnef_ParameterProvision	Provides support to provision information which can be used for the UE in 5GS.	5.2.6.4
Nnef_Trigger	Provides support for device triggering.	5.2.6.5
Nnef_BDTPNegotiation	Provides support for background data transfer policy negotiation and optionally notification for the renegotiation.	5.2.6.6
Nnef_TrafficInfluence	Provide the ability to influence traffic routing.	5.2.6.7
Nnef_ChargeableParty	Requests to become the chargeable party for a data session for a UE.	5.2.6.8
Nnef_AFsessionWithQoS	Requests the network to provide a specific QoS for an AS session.	5.2.6.9
Nnef_MSISDN-less_MO_SMS	Used by the NEF to send MSISDN-less MO SM to the AF.	5.2.6.10
Nnef_ServiceParameter	Provides support to provision service specific information.	5.2.6.11
Nnef_APISupportCapability	Provides support for awareness on availability or expected level of a service API.	5.2.6.12
Nnef_NIDDConfiguration	Used for configuring necessary information for data delivery via the NIDD API.	5.2.6.13
Nnef_NIDD	Used for NEF anchored MO and MT unstructured data transport.	5.2.6.14
Nnef_SMContext	Provides the capability to create, update or release the SMF-NEF Connection.	5.2.6.15
Nnef_AnalyticsExposure	Provides support for exposure of network analytics.	5.2.6.16
Nnef_UCMFProvisioning	Provides the ability to configure the UCMF with dictionary entries consisting of UE manufacturer-assigned UE Radio Capability IDs, the corresponding UE radio capabilities and the (list of) associated IMEI/TAC value(s) via the NEF. The UE radio capabilities the NEF provides for a UE radio Capability ID can be in TS 36.331 [51] format, TS 38.331 [28] format or both formats. Also used for deletion (e.g. as no longer used) or update (e.g. to add or remove a (list of) IMEI/TAC value(s) associated to an entry) of dictionary entries in the UCMF.	5.2.6.17
Nnef_ECRestriction	Provides support for queuing status of enhanced coverage restriction, or enable/disable enhanced coverage restriction per individual UEs.	5.2.6.18
Nnef_ApplyPolicy	Provides the capability to apply a previously negotiated Background Data Transfer Policy to a UE or a group of UEs.	5.2.6.19
Nnef_Location	Provides the capability to deliver UE location to AF.	5.2.6.21

7.2.8A Void

7.2.9 SMSF Services

The following NF services are specified for SMSF:

Table 7.2.9-1: NF Services provided by SMSF

Service Name	Description	Reference in TS 23.502 [3]
Nsmsf_SMService	This service allows AMF to authorize SMS and activate SMS for the served user on SMSF.	5.2.9.2

7.2.10 UDR Services

The following NF services are specified for UDR:

Table 7.2.10-1: NF Services provided by UDR

Service Name	Description	Reference in TS 23.502 [3]
Nudr_DM	Allows NF consumers to retrieve, create, update, subscribe for change notifications, unsubscribe for change notifications and delete data stored in the UDR, based on the set of data applicable to the consumer. This service may also be used to manage operator specific data.	5.2.12.2
Nudr_GroupIDmap	Allows NF consumers to retrieve a NF group ID corresponding to a subscriber identifier.	5.2.12.9

7.2.11 5G-EIR Services

The following NF services are specified for 5G-EIR:

Table 7.2.11-1: NF Services provided by 5G-EIR

Service Name	Description	Reference in TS 23.502 [3]
N5g-eir_Equipment Identity Check	This service enables the 5G-EIR to check the PEI and check whether the PEI is in the black list or not.	5.2.4.2

7.2.12 NWDAF Services

The following NF services are specified for NWDAF:

Table 7.2.12-1: NF Services provided by NWDAF

Service Name	Description	Reference in TS 23.288 [86]
Nnwdaf_AnalyticsSubscription	This service enables the NF service consumers to subscribe/unsubscribe for different type of analytics from NWDAF.	7.2
Nnwdaf_AnalyticsInfo	This service enables the NF service consumers to request and get different type of analytics information from NWDAF.	7.3

7.2.13 UDSF Services

The following NF services are specified for UDSF:

Table 7.2.13-1: NF Services provided by UDSF

Service Name	Description	Reference in TS 23.502 [3]
Nudsf_UnstructuredData Management	Allows NF consumers to retrieve, create, update, and delete data stored in the UDSF.	5.2.14.2

7.2.14 NSSF Services

The following NF services are specified for NSSF:

Table 7.2.14-1: NF Services provided by NSSF

Service Name	Description	Reference in TS 23.502 [3]
Nnssf_NSSelection	Provides the requested Network Slice information to the Requester.	5.2.16.2
Nnssf_NSSAIAvailability	Provides NF consumer on the availability of S-NSSAIs on a per TA basis.	5.2.16.3

7.2.15 BSF Services

The following NF services are specified for BSF as described in TS 23.503 [45]:

Table 7.2.15-1: NF Services provided by BSF

Service Name	Description	Reference in TS 23.502 [3]
Nbsf_Management	Allows a PCF to register/deregister itself and to be discoverable by NF service consumers.	5.2.13.2

7.2.16 LMF Services

The following NF services are specified for LMF:

Table 7.2.16-1: NF Services provided by LMF

Service Name	Description	Reference in TS 23.273 [87]
Nlmf_Location	This service enables an NF to request location determination for a target UE for the Immediate Location Request and to subscribe / get notified of the location determination for a Deferred Location Request. It allow NFs to request or subscribe the current geodetic and optionally civic location of a target UE.	8.3

7.2.16A GMLC Services

The following NF services are specified for GMLC:

Table 7.2.16A-1: NF Services provided by GMLC

Service Name	Description	Reference in TS 23.273 [87]
Ngmlc_Location	This service enables an NF to request location determination for a target UE.	8.4

7.2.17 CHF Services

The following NF services are specified for CHF.

Table 7.2.17-1: NF Service provided by CHF

Service Name	Description	Reference in TS 23.502 [3]
Nchf_SpendingLimitControl	This service enables transfer of policy counter status information relating to subscriber spending limits from CHF to NF consumer	5.2.17.2
Nchf_Converged_Charging	This service is described in TS 32.290 [67].	
Nchf_OfflineOnlyCharging	This service is described for offline only charging as described in TS 32.290 [67].	

7.2.18 UCMF Services

The following NF services are specified for UCMF:

Table 7.2.18-1: NF Services provided by UCMF

Service Name	Description	Reference in TS 23.502 [3]
Nucmf_Provisioning	Allows the NF consumer to provision a dictionary entry in the UCMF consisting of a Manufacturer-assigned UE Radio Capability ID and the corresponding UE radio capabilities and the (list of) associated IMEI/TAC value(s). The UE radio capabilities the NEF provides for a UE radio Capability ID can be in TS 36.331 [51] format, TS 38.331 [28] format or both formats. Also used for deletion (e.g. as no longer used) or update (e.g. to add or remove a (list of) IMEI/TAC value(s) associated to an entry) of dictionary entries in the UCMF.	5.2.18.2
Nucmf_UECapabilityManagement	Allows the NF consumer to resolve UE Radio Capability ID (either Manufacturer-assigned or PLMN-assigned) into the corresponding UE radio capabilities. The consumer shall indicate whether it requests a TS 36.331 [51] format or a TS 38.331 [28] format to be provided. Allows the NF consumer to obtain a PLMN-assigned UE Radio Capability ID for a specific UE radio capabilities. The consumer shall indicate whether the UE radio capabilities sent to UCMF are in TS 36.331 [51] format, TS 38.331 [28], or both. Allows the NF consumer to subscribe or unsubscribe for notifications of UCMF dictionary entries. Allows the NF consumer to be notified about creation and deletion of UCMF dictionary entries.	5.2.18.3

7.2.19 AF Services

The following NF services are specified for AF:

Table 7.2.19-1: NF Services provided by AF

Service Name	Description	Reference in TS 23.502 [3]
Naf_EventExposure	This service enables consumer NF(s) to subscribe or get notified of the event as described in TS 23.288 [86].	5.2.19.2

7.2.20 NSSAAF Services

The following NF services are specified for NSSAAF:

Table 7.2.20 -1: NF Services provided by NSSAAF

Service Name	Description	Reference in TS 23.502 [3]
Nnssaaf_NSSAA	The NSSAAF provides NSSAA service to the requester NF by relaying EAP messages towards a AAA-S or AAA-P and performing related protocol conversion as needed. It also provides notification to the current AMF where the UE is of the need to re-authenticate and re-authorize the UE or to revoke the UE authorization.	5.2.10.5

7.3 Exposure

Network exposure is described in clause 5.20 and in TS 23.502 [3] clause 4.15.

8 Control and User Plane Protocol Stacks

8.1 General

Clause 8 specifies the overall protocol stacks between 5GS entities, e.g. between the UE and the 5GC Network Functions, between the 5G-AN and the 5GC Network Functions, or between the 5GC Network Functions.

8.2 Control Plane Protocol Stacks

8.2.1 Control Plane Protocol Stacks between the 5G-AN and the 5G Core: N2

8.2.1.1 General

NOTE 1: N2 maps to NG-C as defined in TS 38.413 [34].

Following procedures are defined over N2:

- Procedures related with N2 Interface Management and that are not related to an individual UE, such as for Configuration or Reset of the N2 interface. These procedures are intended to be applicable to any access but may correspond to messages that carry some information only on some access (such as information on the default Paging DRX used only for 3GPP access).

- Procedures related with an individual UE:

- Procedures related with NAS Transport. These procedures are intended to be applicable to any access but may correspond to messages that for UL NAS transport carry some access dependent information such as User Location Information (e.g. Cell-Id over 3GPP access or other kind of User Location Information for Non-3GPP access).

- Procedures related with UE context management. These procedures are intended to be applicable to any access. The corresponding messages may carry:

  - some information only on some access (such as Mobility Restriction List used only for 3GPP access).

  - some information (related e.g. with N3 addressing and with QoS requirements) that is to be transparently forwarded by AMF between the 5G-AN and the SMF.

- Procedures related with resources for PDU Sessions. These procedures are intended to be applicable to any access. They may correspond to messages that carry information (related e.g. with N3 addressing and with QoS requirements) that is to be transparently forwarded by AMF between the 5G-AN and the SMF.

- Procedures related with Hand-Over management. These procedures are intended for 3GPP access only.

The Control Plane interface between the 5G-AN and the 5G Core supports:

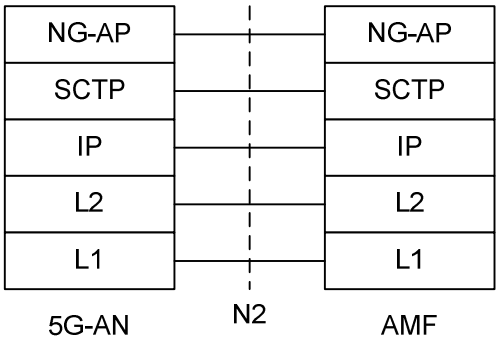
- The connection of multiple different kinds of 5G-AN (e.g. 3GPP RAN, N3IWF for Un-trusted access to 5GC) to the 5GC via a unique Control Plane protocol: A single NGAP protocol is used for both the 3GPP access and non-3GPP access;

- There is a unique N2 termination point in AMF per access for a given UE regardless of the number (possibly zero) of PDU Sessions of the UE;

- The decoupling between AMF and other functions such as SMF that may need to control the services supported by 5G-AN(s) (e.g. control of the UP resources in the 5G-AN for a PDU Session). For this purpose, NGAP may support information that the AMF is just responsible to relay between the 5G-AN and the SMF. The information can be referred as N2 SM information in TS 23.502 [3] and this specification.

NOTE 2: The N2 SM information is exchanged between the SMF and the 5G-AN transparently to the AMF.

8.2.1.2 5G-AN - AMF

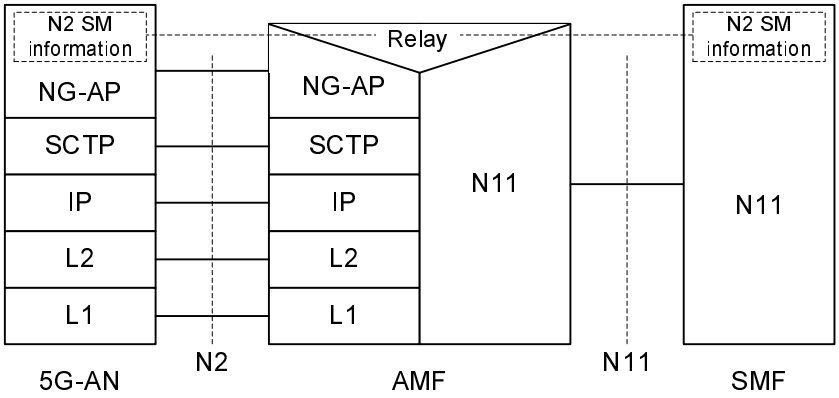


Legend:

- **NG Application Protocol (NG-AP):** Application Layer Protocol between the 5G-AN node and the AMF. NG-AP is defined in TS 38.413 [34].
- **Stream Control Transmission Protocol (SCTP):** This protocol guarantees delivery of signalling messages between AMF and 5G-AN node (N2). SCTP is defined in RFC 4960 [44].

Figure 8.2.1.2-1: Control Plane between the 5G-AN and the AMF

8.2.1.3 5G-AN - SMF



Legend:

- **N2 SM information:** This is the subset of NG-AP information that the AMF transparently relays between the 5G-AN and the SMF, and is included in the NG-AP messages and the N11 related messages.

Figure 8.2.1.3-1: Control Plane between the 5G-AN and the SMF

NOTE 1: From the 5G-AN perspective, there is a single termination of N2 i.e. the AMF.

NOTE 2: For the protocol stack between the AMF and the SMF, see clause 8.2.3.

8.2.2 Control Plane Protocol Stacks between the UE and the 5GC

8.2.2.1 General

A single N1 NAS signalling connection is used for each access to which the UE is connected. The single N1 termination point is located in AMF. The single N1 NAS signalling connection is used for both Registration Management and Connection Management (RM/CM) and for SM-related messages and procedures for a UE.

The NAS protocol on N1 comprises a NAS-MM and a NAS-SM components.

There are multiple cases of protocols between the UE and a core network function (excluding the AMF) that need to be transported over N1 via NAS-MM protocol. Such cases include:

- Session Management Signalling.
- SMS.
- UE Policy.
- LCS.

RM/CM NAS messages in NAS-MM and other types of NAS messages (e.g. SM), as well as the corresponding procedures, are decoupled.

The NAS-MM supports generic capabilities:

- NAS procedures that terminate at the AMF. This includes:
  - Handles Registration Management and Connection Management state machines and procedures with the UE, including NAS transport; the AMF supports following capabilities:
    - Decide whether to accept the RM/CM part of N1 signalling during the RM/CM procedures without considering possibly combined other non NAS-MM messages (e.g., SM) in the same NAS signalling contents;
    - Know if one NAS message should be routed to another NF (e.g., SMF), or locally processed with the NAS routing capabilities inside during the RM/CM procedures;

- Provide a secure NAS signalling connection (integrity protection, ciphering) between the UE and the AMF, including for the transport of payload;
- Provide access control if it applies;

- It is possible to transmit the other type of NAS message (e.g., NAS SM) together with an RM/CM NAS message by supporting NAS transport of different types of payload or messages that do not terminate at the AMF, i.e. NAS-SM, SMS, UE Policy and LCS between the UE and the AMF. This includes:
  - Information about the Payload type;
  - Additional Information for forwarding purposes
  - The Payload (e.g. the SM message in the case of SM signalling);
- There is a Single NAS protocol that applies on both 3GPP and non-3GPP access. When an UE is served by a single AMF while the UE is connected over multiple (3GPP/Non 3GPP) accesses, there is a N1 NAS signalling connection per access.

Security of the NAS messages is provided based on the security context established between the UE and the AMF.

Figure 8.2.2.1-1 depicts NAS transport of SM signalling, SMS, UE Policy and LCS.

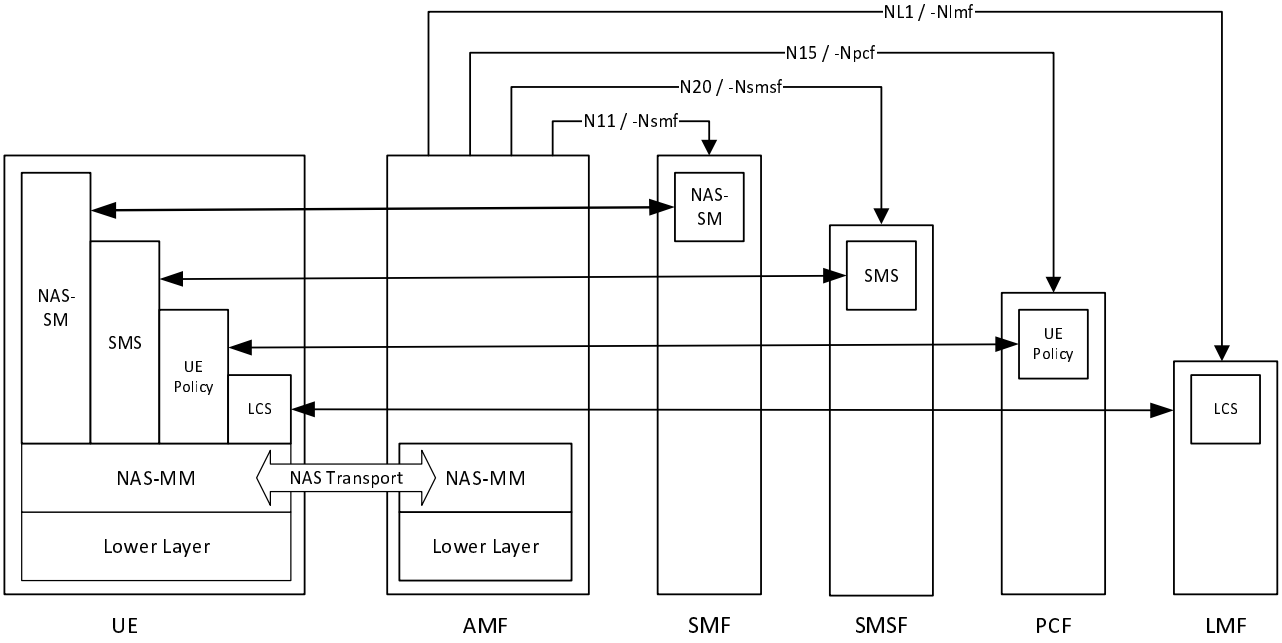
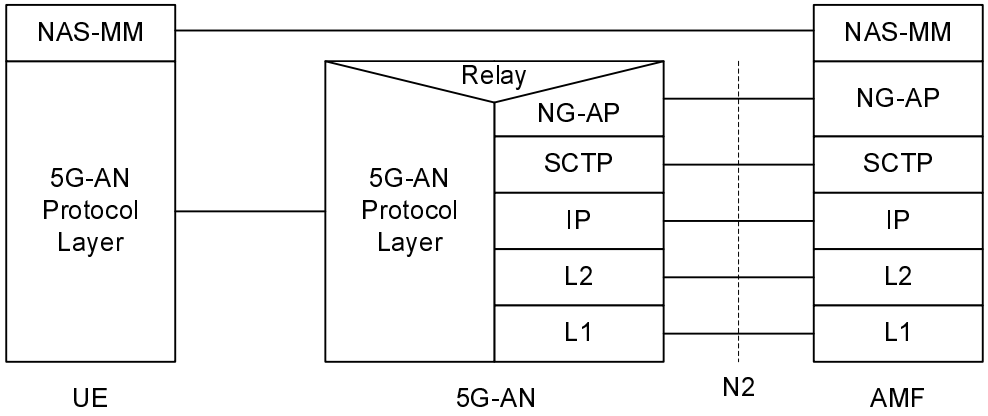


Figure 8.2.2.1-1 NAS transport for SM, SMS, UE Policy and LCS

8.2.2.2 UE - AMF



Legend:

- **NAS-MM:** The NAS protocol for MM functionality supports registration management functionality, connection management functionality and user plane connection activation and deactivation. It is also responsible of ciphering and integrity protection of NAS signalling. 5G NAS protocol is defined in TS 24.501 [47]
- **5G-AN Protocol layer:** This set of protocols/layers depends on the 5G-AN. In the case of NG-RAN, the radio protocol between the UE and the NG-RAN node (eNodeB or gNodeB) is specified in TS 36.300 [30] and TS 38.300 [27]. In the case of non-3GPP access, see clause 8.2.4.

Figure 8.2.2.2-1: Control Plane between the UE and the AMF

8.2.2.3 UE – SMF

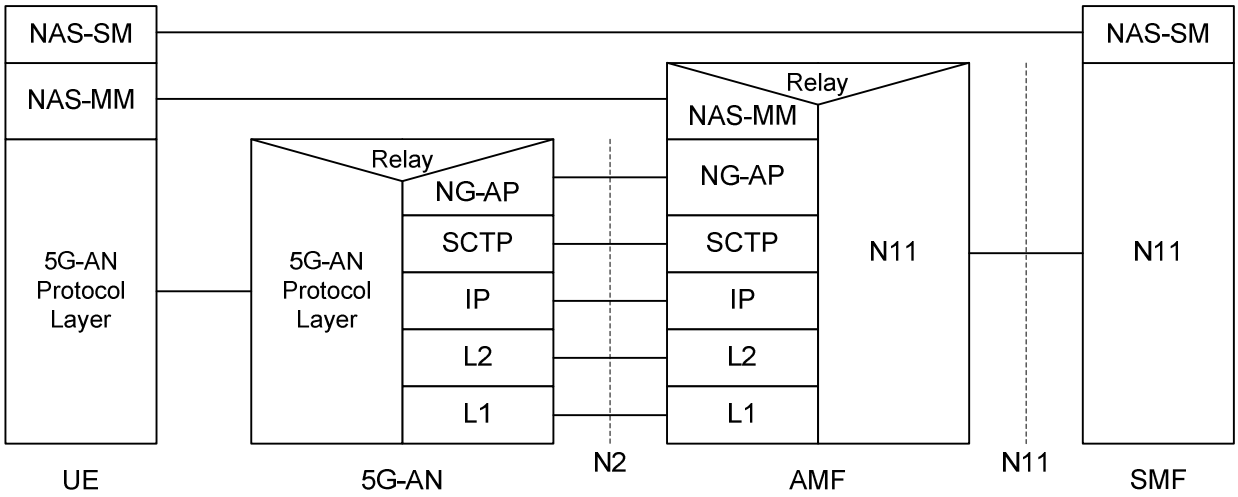
The NAS-SM supports the handling of Session Management between the UE and the SMF.

The SM signalling message is handled, i.e. created and processed, in the NAS-SM layer of UE and the SMF. The content of the SM signalling message is not interpreted by the AMF.

The NAS-MM layer handles the SM signalling is as follows:

- For transmission of SM signalling:
  - The NAS-MM layer creates a NAS-MM message, including security header, indicating NAS transport of SM signalling, additional information for the receiving NAS-MM to derive how and where to forward the SM signalling message.
- For reception of SM signalling:
  - The receiving NAS-MM processes the NAS-MM part of the message, i.e. performs integrity check, and interprets the additional information to derive how and where to derive the SM signalling message.

The SM message part shall include the PDU Session ID.



Legend:

- **NAS-SM:** The NAS protocol for SM functionality supports user plane PDU Session Establishment, modification and release. It is transferred via the AMF, and transparent to the AMF. 5G NAS protocol is defined in TS 24.501 [47]

Figure 8.2.2.3-1: Control Plane protocol stack between the UE and the SMF

8.2.3 Control Plane Protocol Stacks between the network functions in 5GC

8.2.3.1 The Control Plane Protocol Stack for the service based interface

The control plane protocol(s) for the service-based interfaces listed in clause 4.2.6 is defined in the TS 29.500 [49]

8.2.3.2 The Control Plane protocol stack for the N4 interface between SMF and UPF

The control plane protocol for SMF-UPF (i.e. N4 reference point) is defined in TS 29.244 [65].

8.2.4 Control Plane for untrusted non 3GPP Access

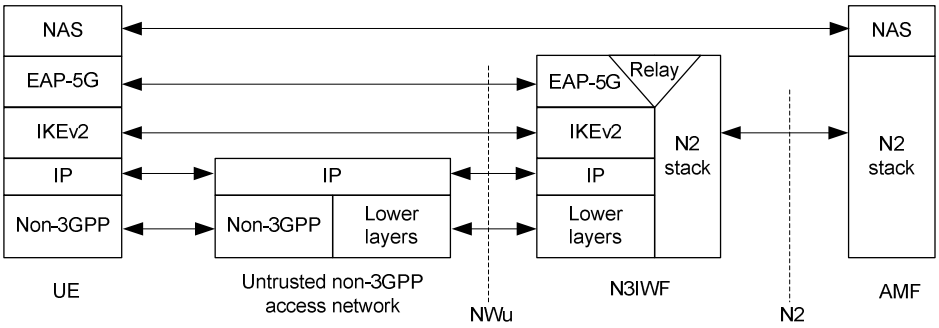


Figure 8.2.4-1: Control Plane before the signalling IPsec SA is established between UE and N3IWF

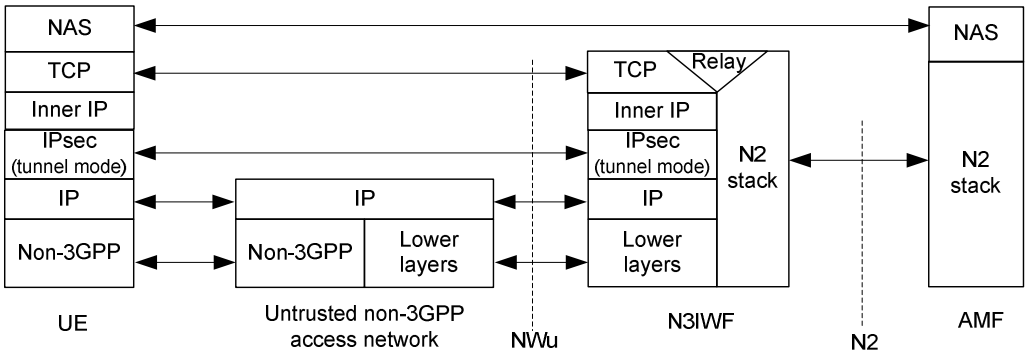


Figure 8.2.4-2: Control Plane after the signalling IPsec SA is established between UE and N3IWF

Large NAS messages may be fragmented by the "inner IP" layer or by TCP.

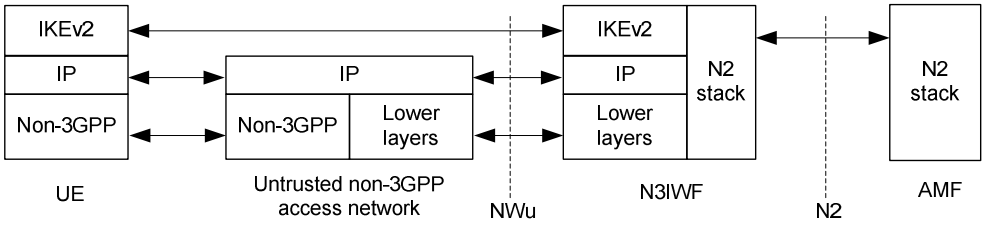


Figure 8.2.4-3: Control Plane for establishment of user-plane via N3IWF

In the above figures 8.2.4-1, 8.2.4-2 and 8.2.4-3, the UDP protocol may be used between the UE and N3IWF to enable NAT traversal for IKEv2 and IPsec traffic.

The "signalling IPsec SA" is defined in TS 23.502 [3], clause 4.12.2.

8.2.5 Control Plane for trusted non-3GPP Access

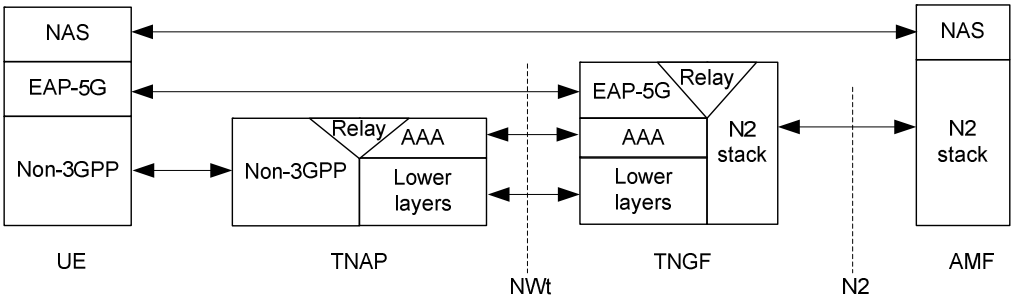


Figure 8.2.5-1: Control Plane before the NWt connection is established between UE and TNGF

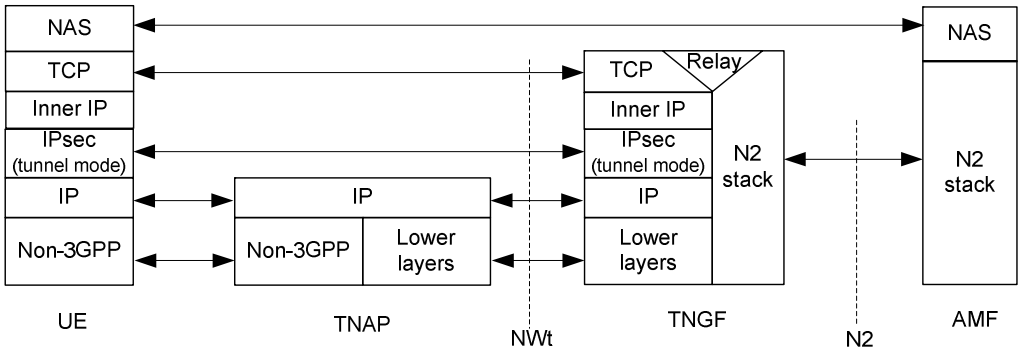


Figure 8.2.5-2: Control Plane after the NWt connection is established between UE and TNGF

Large NAS messages may be fragmented by the "inner IP" layer or by TCP.

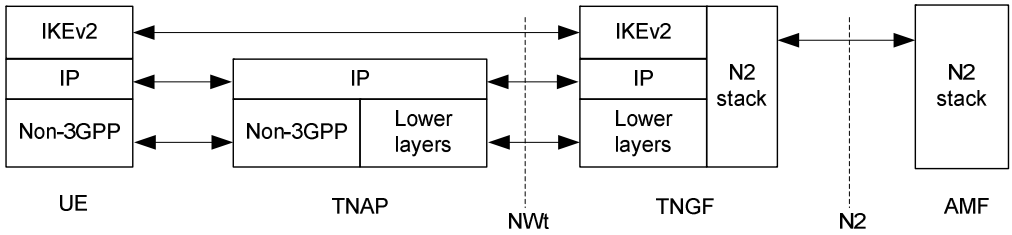


Figure 8.2.5-3: Control Plane for establishment of user-plane via TNGF

In the above figures 8.2.5-2 and 8.2.5-3, the UDP protocol may be used between the UE and TNGF to enable NAT traversal for IKEv2 and IPsec traffic.

The NWt connection is defined in clause 4.2.8.3 and in clause 4.12a.2.2 of TS 23.502 [3].

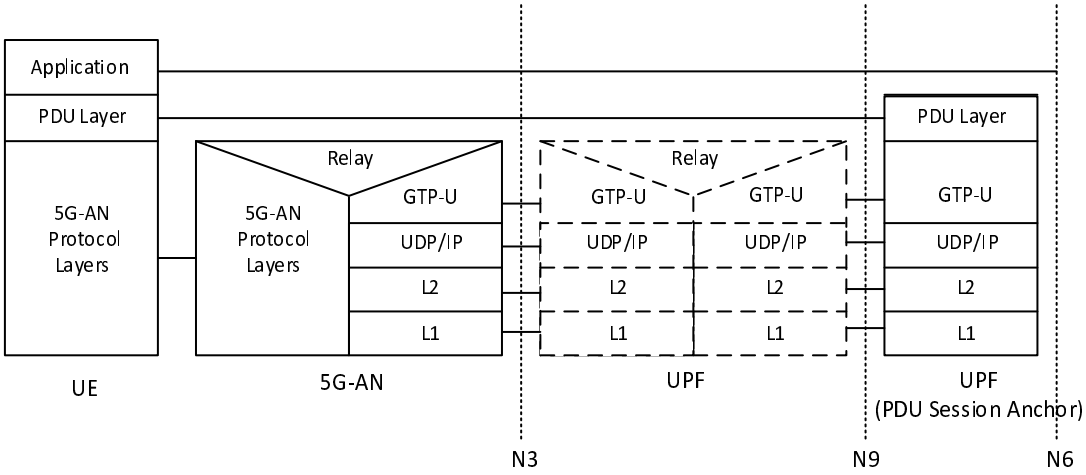
8.2.6 Control Plane for W-5GAN Access

The control plane for W-5GAN is defined in clause 6 of TS 23.316 [84].

8.3 User Plane Protocol Stacks

8.3.1 User Plane Protocol Stack for a PDU Session

This clause illustrates the protocol stack for the User plane transport related with a PDU Session.



Legend:

- **PDU layer:** This layer corresponds to the PDU carried between the UE and the DN over the PDU Session. When the PDU Session Type is IPv4 or IPv6 or IPv4v6, it corresponds to IPv4 packets or IPv6 packets or both of them; When the PDU Session Type is Ethernet, it corresponds to Ethernet frames; etc.
- **GPRS Tunnelling Protocol for the user plane (GTP-U):** This protocol supports tunnelling user data over N3 (i.e. between the 5G-AN node and the UPF) and N9 (i.e. between different UPFs of the 5GC) in the backbone network, details see TS 29.281 [75]. GTP shall encapsulate all end user PDUs. It provides encapsulation on a per PDU Session level. This layer carries also the marking associated with a QoS Flow defined in clause 5.7. This protocol is also used on N4 interface as defined in TS 29.244 [65].

Figure 8.3.1-1: User Plane Protocol Stack

- **5G-AN protocol stack**: This set of protocols/layers depends on the AN:
  - When the 5G-AN is a 3GPP NG-RAN, these protocols/layers are defined in TS 38.401 [42]. The radio protocol between the UE and the 5G-AN node (eNodeB or gNodeB) is specified in TS 36.300 [30] and TS 38.300 [27].
  - When the AN is an Untrusted non 3GPP access to 5GC the 5G-AN interfaces with the 5GC at a N3IWF defined in clause 4.3.2 and the 5G-AN protocol stack is defined in clause 8.3.2.
- **UDP/IP:** These are the backbone network protocols.

NOTE 1: The number of UPF in the data path is not constrained by 3GPP specifications: there may be in the data path of a PDU Session 0, 1 or multiple UPF that do not support a PDU Session Anchor functionality for this PDU Session.

NOTE 2: The "non PDU Session Anchor" UPF depicted in the Figure 8.3.1-1 is optional.

NOTE 3: The N9 interface may be intra-PLMN or inter PLMN (in the case of Home Routed deployment).

If there is an UL CL (Uplink Classifier) or a Branching Point (both defined in clause 5.6.4) in the data path of a PDU Session, the UL CL or Branching Point acts as the non PDU Session Anchor UPF of Figure 8.3.1-1. In that case there are multiple N9 interfaces branching out of the UL CL / Branching Point each leading to different PDU Session anchors.

NOTE 4: Co-location of the UL CL or Branching Point with a PDU Session Anchor is a deployment option.

8.3.2 User Plane for untrusted non-3GPP Access

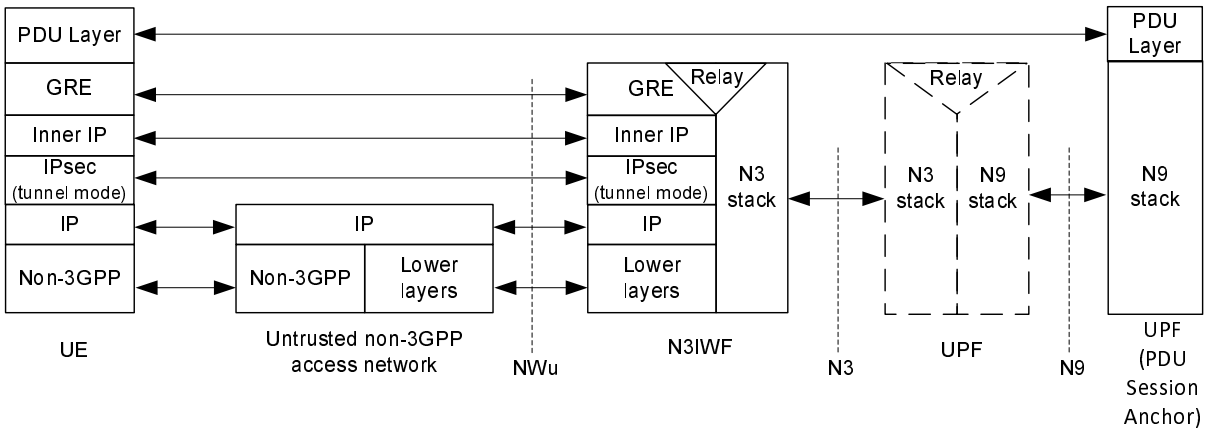


Figure 8.3.2-1: User Plane via N3IWF

Large GRE packets may be fragmented by the "inner IP" layer.

Details about the PDU Layer, the N3 stack and the N9 stack are included in clause 8.3.1. The UDP protocol may be used below the IPsec layer to enable NAT traversal.

8.3.3 User Plane for trusted non-3GPP Access

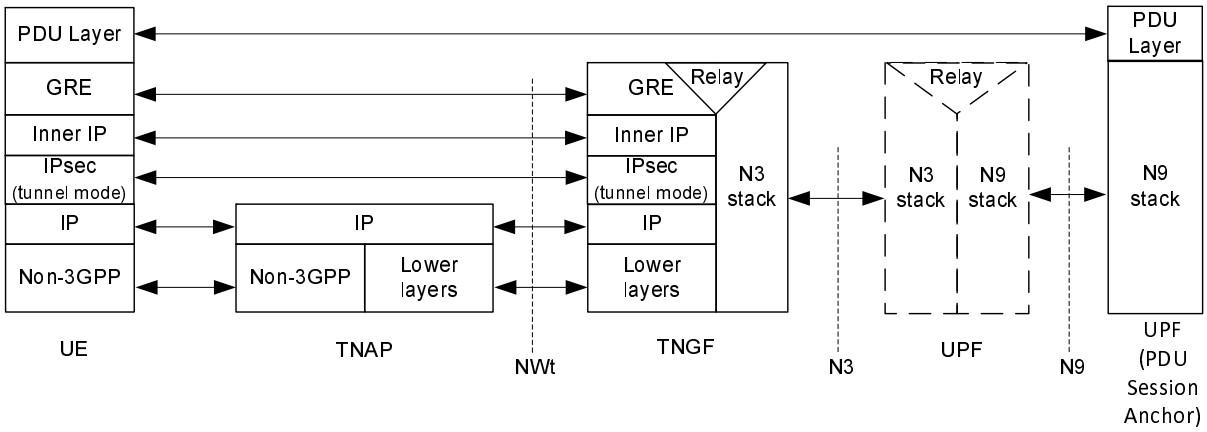


Figure 8.3.2-1: User Plane via TNGF

Large GRE packets may be fragmented by the "inner IP" layer.

Details about the PDU Layer, the N3 stack and the N9 stack are included in clause 8.3.1. The UDP protocol may be used below the IPsec layer to enable NAT traversal.

8.3.4 User Plane for W-5GAN Access

The user plane for W-5GAN is defined in clause 6 ofTS 23.316 [84].

8.3.5 User Plane for N19-based forwarding of a 5G VN group

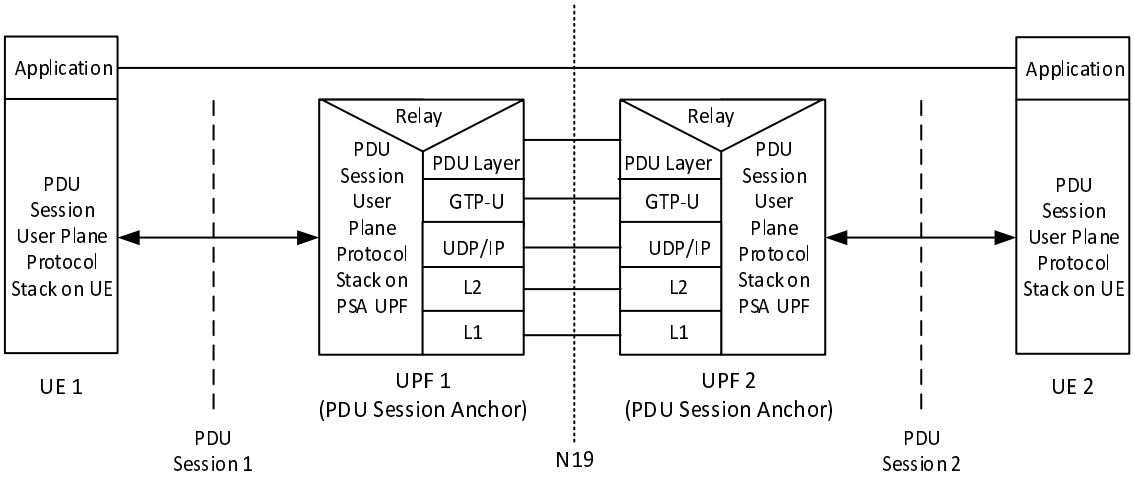


Figure 8.3.5-1: User Plane for N19-based forwarding

Details about the PDU Layer, PDU Session User Plane Protocol Stack are included in clause 8.3.1 and clause 8.3.2. The N19 is based on a shared User Plane tunnel connecting two PSA UPFs of a single 5G VN group.

Annex A (informative): Relationship between Service-Based Interfaces and Reference Points

Service-Based Interfaces and Reference Points are two different ways to model interactions between architectural entities. A Reference Point is a conceptual point at the conjunction of two non-overlapping functional groups (see TR 21.905 [1]). In figure A-1 the functional groups are equivalent to Network Functions.

A reference point can be replaced by one or more service-based interfaces which provide equivalent functionality.

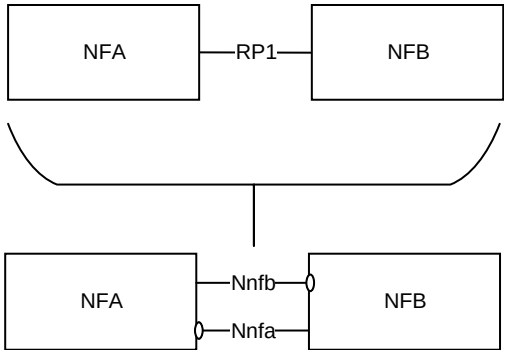


Figure A-1: Example show a Reference Point replaced by two Service based Interfaces

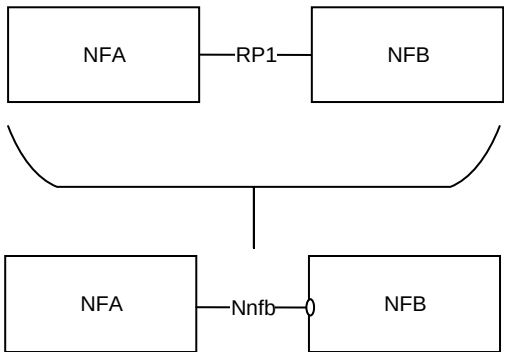


Figure A-2: Example showing a Reference Point replaced by a single Service based Interface

Reference points exist between two specific Network Functions. Even if the functionality is equal on two reference points between different Network Functions there has to be a different reference point name. Using the service-based interface representation it is immediately visible that it is the same service-based interface and that the functionality is equal on each interface.

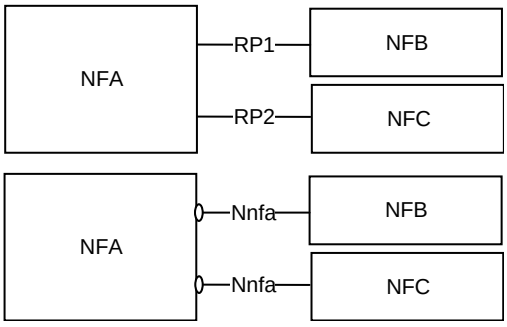


Figure A-3: Reference Points vs. Service-based Interfaces representation of equal functionality on the interfaces

A NF may expose one or more services through Service based interfaces.

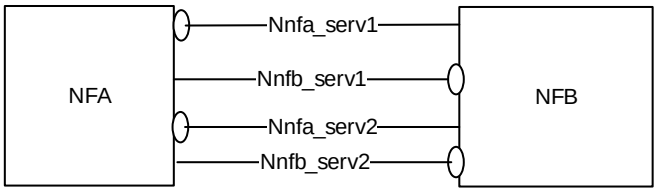


Figure A-4: One or more Services exposed by one Network Function

Annex B (normative): Mapping between temporary identities

When interworking procedures with N26 are used and the UE performs idle mode mobility from 5GC to EPC the following mapping from 5G GUTI to EPS GUTI applies:

- 5G <MCC> maps to EPS <MCC>
- 5G <MNC> maps to EPS <MNC>
- 5G <AMF Region ID> and 5G <AMF Set ID> maps to EPS <MMEGI> and part of EPS <MMEC>
- 5G <AMF Pointer> map to part of EPS <MMEC>
- 5G <5G-TMSI> maps to EPS <M-TMSI>

NOTE 1: The mapping described above does not necessarily imply the same size for the 5G GUTI and EPS GUTI fields that are mapped. The size of 5G GUTI fields and other mapping details will be defined in TS 23.003 [19].

NOTE 2: To support interworking with the legacy EPC core network entity (i.e. when MME is not updated to support interworking with 5GS), it is assumed that the 5G <AMF Region ID> and EPS <MMEGI> is partitioned to avoid overlapping values in order to enable discovery of source node (i.e. MME or AMF) without ambiguity. Once the EPS in the PLMN has been updated to support interworking with 5GS, the full address space of the AMF Region ID can be used for 5GS.

Annex C (informative): Guidelines and Principles for Compute-Storage Separation

5G System Architecture allows any NF/NF Service to store and retrieve its unstructured data (e.g. UE contexts) into/from a Storage entity (e.g. UDSF) as stated in clause 4.2.5 in this release of the specification. This clause highlights some assumptions, principles regarding NF/NF services that use this Storage entity for storing unstructured data:

1. It is up to the Network Function implementation to determine whether the Storage entity is used as a Primary Storage (in which case the corresponding context stored within the NF/NF Service is deleted after storage in the Storage entity) or the Storage entity is used as a Secondary Storage (in which case the corresponding context within the NF/NF Service is stored).

2. It is up to the NF/NF Service implementation to determine the trigger (e.g. at the end of Registration procedure, Service Request procedure etc) for storing unstructured data (e.g. UE contexts) in the Storage entity but it is a good practice for NF/NF service to store stable state in the Storage entity.

3. Multiple NF/NF service instances may require to access the same stored data in the Storage entity (e.g. UE context), around the same time, then the resolution the race condition is implementation specific.

4. In the case of AMF, all AMFs within the same AMF Set are assumed to have access to the same unstructured data stored within the Storage entity.

5. AMF planned removal with UDSF (clause 5.21.2.2.1) and AMF auto-recovery (with UDSF option in clause 5.21.2.3) assume that a storage entity/UDSF is used either as a primary storage or secondary storage by the AMF for storing UE contexts.

Annex D (informative): 5GS support for Non-Public Network deployment options

D.1 Introduction

This annex provides guidance on how 5GS features and capabilities can be used to support various Non-Public Network deployment options.

D.2 Support of Non-Public Network as a network slice of a PLMN

The PLMN operator can provide access to an NPN by using network slicing mechanisms. The following are some considerations in such a PNI-NPN case:

1. The UE has subscription and credentials for the PLMN;
2. The PLMN and NPN service provider have an agreement of where the NPN Network Slice is to be deployed (i.e. in which TAs of the PLMN and optionally including support for roaming PLMNs);
3. The PLMN subscription includes support for Subscribed S-NSSAI to be used for the NPN (see clause 5.15.3);
4. The PLMN operator can offer possibilities for the NPN service provider to manage the NPN Network Slice according to TS 28.533 [79].
5. When the UE registers the first time to the PLMN, the PLMN can configure the UE with URSP including NSSP associating Applications to the NPN S-NSSAI (if the UE also is able to access other PLMN services);
6. The PLMN can configure the UE with Configured NSSAI for the Serving PLMN (see clause 5.15.4);
7. The PLMN and NPN can perform a Network Slice specific authentication and authorization using additional NPN credentials;
8. The UE follows the logic as defined for Network Slicing, see clause 5.15;
9. The network selection logic, access control etc are following the principles for PLMN selection; and
10. The PLMN may indicate to the UE that the NPN S-NSSAI is rejected for the RA when the UE moves out of the coverage of the NPN Network Slice. However, limiting the availability of the NPN S-NSSAI would imply that the NPN is not available outside of the area agreed for the NPN S-NSSAI, e.g. resulting in the NPN PDU Sessions being terminated when the UE moves out of the coverage of the NPN Network Slice. Similarly access to NPN DNNs would not be available via non-NPN cells.
11. In order to prevent access to NPNs for authorized UE(s) in the case of network congestion/overload and if a dedicated S-NSSAI has been allocated for an NPN, the Unified Access Control can be used using the operator-defined access categories with access category criteria type (as defined in TS 24.501 [47]) set to the S-NSSAI used for an NPN.
12. If NPN isolation is desired, it is assumed that a dedicated S-NSSAI is configured for the NPN and that the UE is configured to operate in Access Stratum Connection Establishment NSSAI Inclusion Mode a, b or c, see clause 5.15.9, such that NG-RAN receives Requested NSSAI from the UE and it can use the S-NSSAI for AMF selection.

D.3 Support for access to PLMN services via Stand-alone Non-Public Network and access to Stand-alone Non Public Network services via PLMN

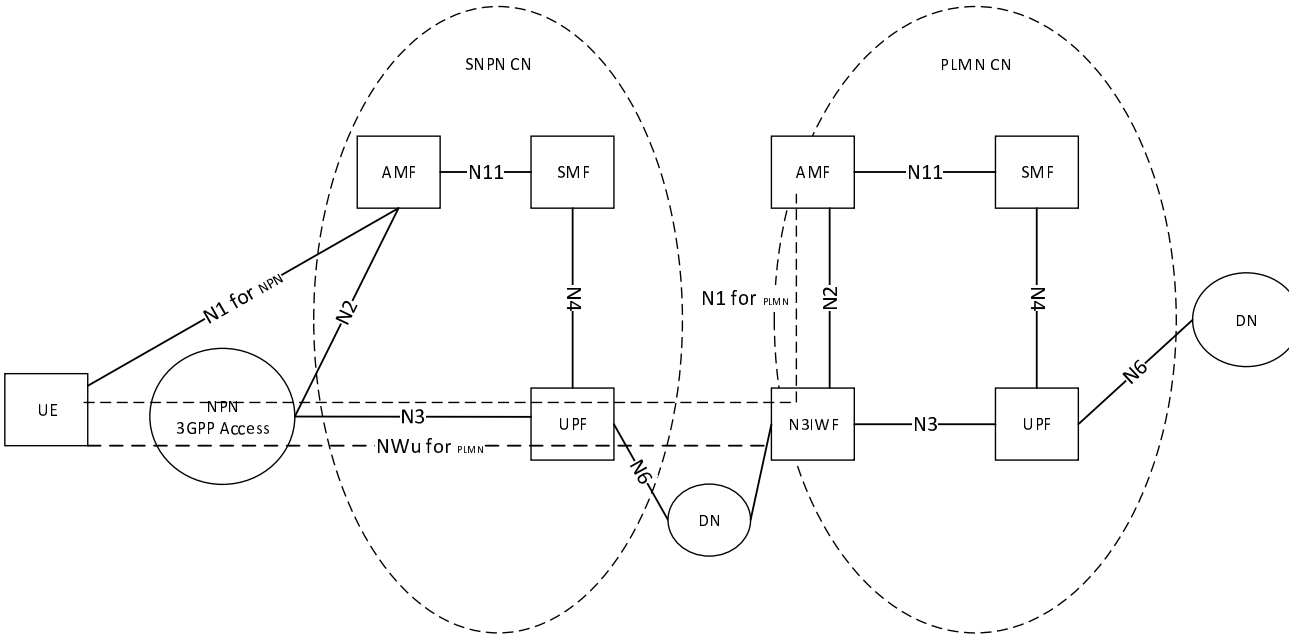


Figure D.3-1: Access to PLMN services via Stand-alone Non-Public Network

NOTE 1: The reference architecture in Figure D.3-1 and Figure D.3-2 only shows the network functions directly connected to the UPF or N3IWF and other parts of the architecture are same as defined in clause 4.2.

In order to obtain access to PLMN services when the UE is camping in NG-RAN of Stand-alone Non-Public Network, the UE obtains IP connectivity, discovers and establishes connectivity to an N3IWF in the PLMN.

In the Figure D.3-1, the N1 (for NPN) represents the reference point between UE and the AMF in Stand-alone Non-Public Network. The Nwu (for PLMN) represents the reference point between the UE and the N3IWF in the PLMN for establishing secure tunnel between UE and the N3IWF over the Stand-alone Non-Public Network. N1 (for PLMN) represents the reference point between UE and the AMF in PLMN.

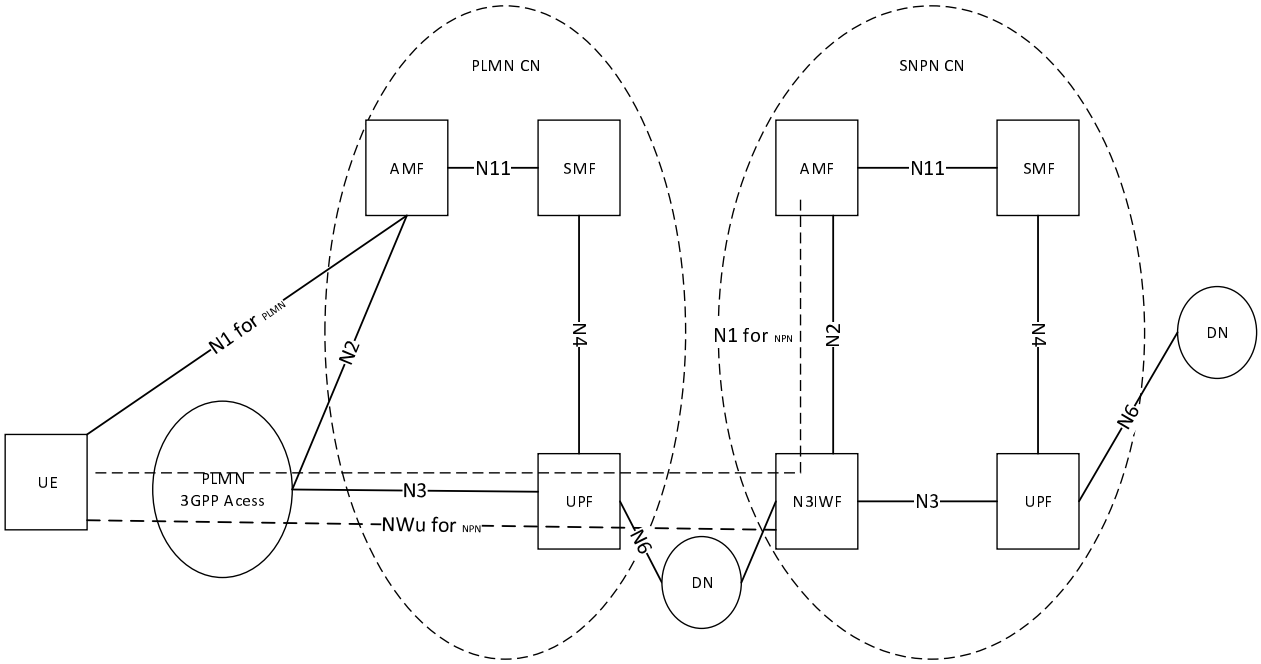


Figure D.3-2: Access to Stand-alone Non-Public Network services via PLMN

In order to obtain access to Non-Public Network services when the UE is camping in NG-RAN of a PLMN, the UE obtains IP connectivity, discovers and establishes connectivity to an N3IWF in the Stand-alone Non-Public Network.

In Figure D.3-2, the N1 (for NPN) represents the reference point between UE and the AMF in the Stand-alone Non-Public Network. The NWu (for NPN) represents the reference point between the UE and the N3IWF in the stand-alone Non-Public Network for establishing a secure tunnel between UE and the N3IWF over the PLMN. The N1 (for PLMN) represents the reference point between UE and the AMF in PLMN.

D.4 Support for UE capable of simultaneously connecting to an SNPN and a PLMN

When a UE capable of simultaneously connecting to an SNPN and a PLMN is not set to operate in SNPN access mode, the UE only performs PLMN selection procedures as defined in clause 4.4 of TS 23.122 [17] using the Uu interface for connection to the PLMN.

A UE supporting simultaneous connectivity to an SNPN and a PLMN applies the network selection as applicable for the access and network for SNPN and PLMN respectively. Whether the UE uses SNPN or PLMN for its services is implementation dependent.

A UE supporting simultaneous connectivity to an SNPN and a PLMN applies the cell (re-)selection as applicable for the access and network for SNPN and PLMN respectively. Whether the UE uses SNPN or PLMN for its services is implementation dependent.

Annex E (informative): Communication models for NF/NF services interaction

E.1 General

This annex provides a high level description of the different communication models that NF and NF services can use to interact which each other. Table E.1-1 summarizes the communication models, their usage and how they relate to the usage of an SCP.

Table E.1-1: Communication models for NF/NF services interaction summary

Communication between consumer and producer	Service discovery and request routing	Communication model
Direct communication	No NRF or SCP; direct routing	A
	Discovery using NRF services; no SCP; direct routing	B
Indirect communication	Discovery using NRF services; selection for specific instance from the Set can be delegated to SCP. Routing via SCP	C
	Discovery and associated selection delegated to an SCP using discovery and selection parameters in service request; routing via SCP	D

Model A - Direct communication without NRF interaction: Neither NRF nor SCP are used. Consumers are configured with producers' "NF profiles" and directly communicate with a producer of their choice.

Model B - Direct communication with NRF interaction: Consumers do discovery by querying the NRF. Based on the discovery result, the consumer does the selection. The consumer sends the request to the selected producer.

Model C - Indirect communication without delegated discovery: Consumers do discovery by querying the NRF. Based on discovery result, the consumer does the selection of an NF Set or a specific NF instance of NF instance set. The consumer sends the request to the SCP containing the address of the selected service producer pointing to a NF service instance or a set of NF service instances. In the latter case, the SCP selects an NF Service instance. If possible, the SCP interacts with NRF to get selection parameters such as location, capacity, etc. The SCP routes the request to the selected NF service producer instance.

Model D - Indirect communication with delegated discovery: Consumers do not do any discovery or selection. The consumer adds any necessary discovery and selection parameters required to find a suitable producer to the service request. The SCP uses the request address and the discovery and selection parameters in the request message to route the request to a suitable producer instance. The SCP can perform discovery with an NRF and obtain a discovery result.

Figure E.1-1 depicts the different communication models.

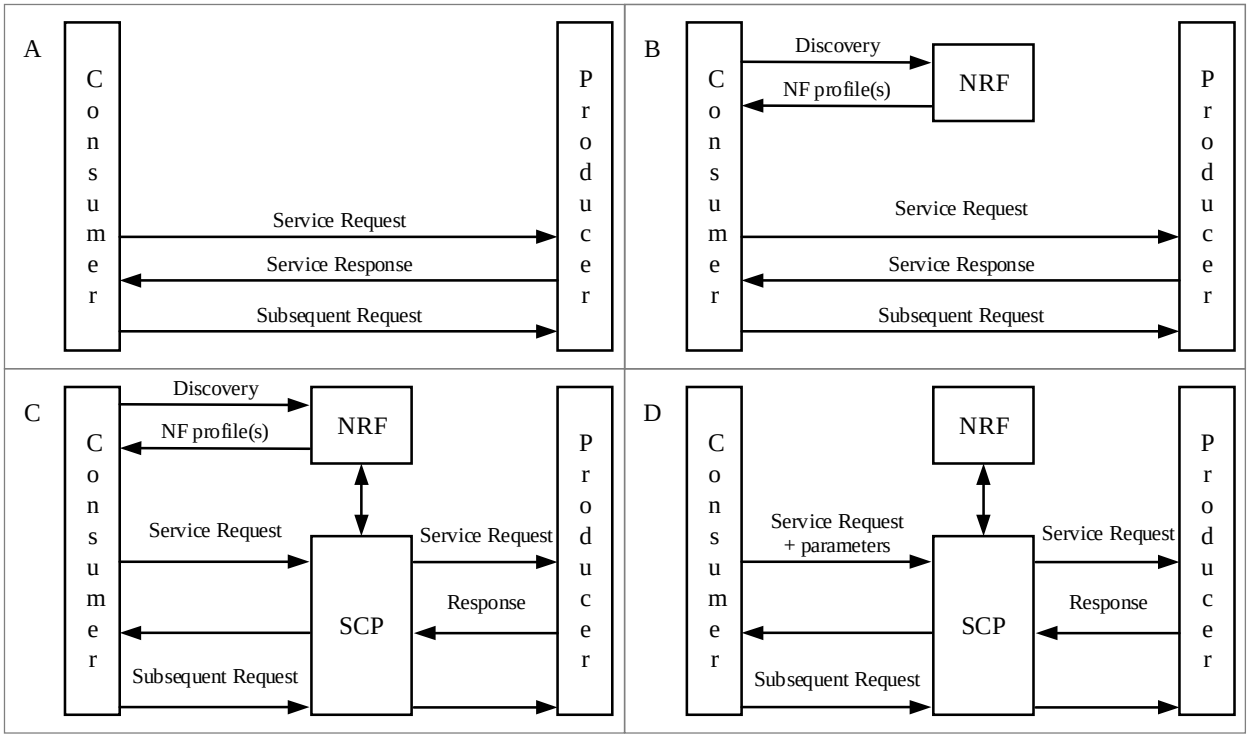


Figure E.1-1: Communication models for NF/NF services interaction

Annex F (informative): Redundant user plane paths based on multiple UEs per device

This clause describes an approach to realize multiple user plane paths in the system based on a device having multiple UEs and specific network deployments.

The approach assumes a RAN deployment where redundant coverage by multiple gNBs (in the case of NR) is generally available. Upper layer protocols, such as the IEEE TSN (Time Sensitive Networking), can make use of the multiple user plane paths.

The UEs belonging to the same terminal device request the establishment of PDU Sessions that use independent RAN and CN network resources using the mechanisms outlined below.

This deployment option has a number of preconditions:

- The redundancy framework uses separate gNBs to achieve user plane redundancy over the 3GPP system. It is however up to operator deployment and configuration whether separate gNBs are available and used. If separate gNBs are not available for a device, the redundancy framework may still be applied to provide user plane redundancy in the rest of the network as well as between the device and the gNB using multiple UEs.
- Terminal devices integrate multiple UEs which can connect to different gNBs independently.
- RAN coverage is redundant in the target area: it is possible to connect to multiple gNBs from the same location. To ensure that the two UEs connect to different gNBs, the gNBs need to operate such that the selection of gNBs can be distinct from each other (e.g. gNB frequency allocation allows the UE to connect to multiple gNBs).
- The core network UPF deployment is aligned with RAN deployment and supports redundant user plane paths.
- The underlying transport topology is aligned with the RAN and UPF deployment and supports redundant user plane paths.
- The physical network topology and geographical distribution of functions also supports the redundant user plane paths to the extent deemed necessary by the operator.
- The operation of the redundant user plane paths is made sufficiently independent, to the extent deemed necessary by the operator, e.g., independent power supplies.

Figure F-1 illustrates the architecture view. UE1 and UE2 are connected to gNB1 and gNB2, respectively and UE1 sets up a PDU Session via gNB1 to UPF1, while UE2 sets up a PDU Session via gNB2 to UPF2. UPF1 and UPF2 connect to the same Data Network (DN), but the traffic via UPF1 and UPF2 might be routed via different user plane nodes within the DN. UPF1 and UPF2 are controlled by SMF1 and SMF2, respectively.

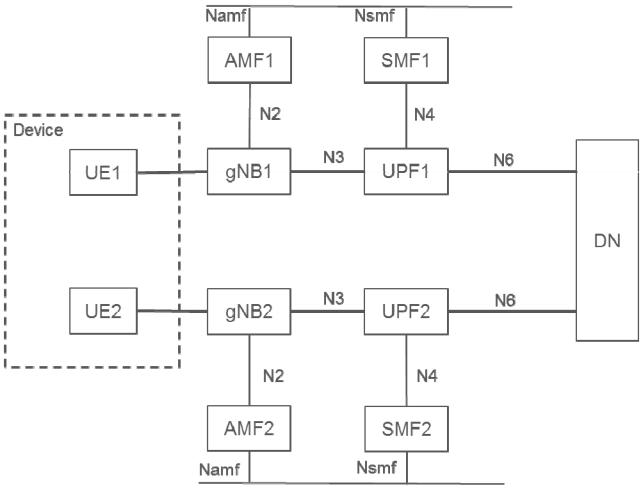


Figure F-1: Architecture with redundancy based on multiple UEs in the device

The approach comprises the following main components shown as example using NR in figure F-2.

- **gNB selection:** The selection of different gNBs for the UEs in the same device is realized by the concept of UE Reliability Groups for the UEs and also for the cells of gNBs. By grouping the UEs in the device and cells of gNBs in the network into more than one reliability group and preferably selecting cells in the same reliability group as the UE, it is ensured that UEs in the same device can be assigned different gNBs for redundancy as illustrated in Figure F-2, where UE1 and the cells of gNB1 belong to reliability group A, and UE2 and the cells of gNB2 belong to reliability group B.

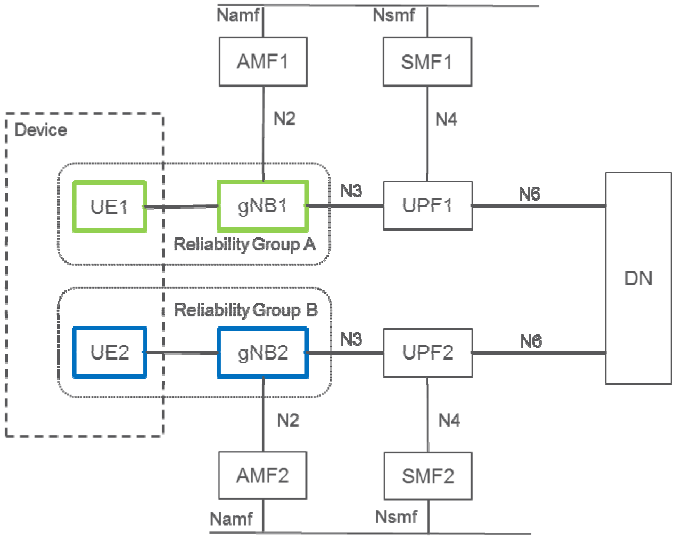


Figure F-2: Reliability group-based redundancy concept in RAN

For determining the reliability grouping of a UE, one of the following methods or a combination of them can be used:

- It could be configured explicitly to the UE and sent in a Registration Request message to the network using an existing parameter (such as an S-NSSAI in the Requested NSSAI where the SST is URLLC; the Reliability Group can be decided by the SD part).

- It could also be derived from existing system parameters (e.g., SUPI, PEI, S-NSSAI, RFSP) based on operator configuration.

The Reliability Group of each UE is represented via existing parameters and sent from the AMF to the RAN when the RAN context is established, so each gNB has knowledge about the reliability group of the connected UEs.

NOTE: An example realisation can be as follows: the UE's Allowed NSSAI can be used as input to select the RFSP index value for the UE. The RAN node uses the RFSP for RRM purposes and can based on local configuration determine the UE's Reliability Group based on the S-NSSAI in Allowed NSSAI and/or S-NSSAI for the PDU Session(s).

The reliability group of the RAN (cells of gNBs) entities are pre-configured by the O&M system in RAN. It is possible for gNBs to learn the reliability group neighbouring cells as the Xn connectivity is set up, or the reliability group of neighbouring cells are also configured into the gNBs.

In the case of connected mode mobility, the serving gNB prioritizes candidate target cells that belong to different reliability group than the UE. It follows that normally the UE is handed over only to cells in the same reliability group. If cells in the same reliability group are not available (UE is out of the coverage of cells of its own reliability group or link quality is below a given threshold) the UE may be handed over to a cell in another reliability group as well.

If the UE connects to a cell whose reliability group is different from the UE's reliability group, the gNB initiates a handover to a cell in the appropriate reliability group whenever such a suitable cell is available.

In the case of an Idle UE, it is possible to use the existing cell (re-)selection priority mechanism, with a priori UE config using dedicated signalling (in the RRCConnectionRelease message during transition from connected to idle mode) to configure the UE to reselect the cells of the appropriate reliability group for camping in deployments where the cell reliability groups use different sets of frequencies.

- **UPF selection.** UPF selection mechanisms as described in clause 6.3.3 can be used to select different UPFs for the UEs within the device. The selection may be based either on UE configuration or network configuration of different DNNs leading to the same DN, or different slices for the two UEs. It is possible to use the UE's Reliability Group, described above for gNB selection, as an input to the UPF selection. The proper operator configuration of the UPF selection can ensure that the path of the PDU Sessions of UE1 and UE2 are independent.

- **Control plane.** The approach can optionally apply different control plane entities for the individual UEs within the device. This may be achieved by using:

  - different DNNs for the individual UEs within the device to select different SMFs,

  - or applying different slices for the individual UEs within the device either based on UE configuration or network subscription, to select different AMFs and/or SMFs.

Annex G (informative): SCP Deployment Examples

G.1 General

This Annex provides deployment examples for the SCP but is not meant to be an exhaustive list of deployment options for the SCP. The first example G.1 is based on an SCP implement using (network wide) service mesh technology, while the second example builds on SCP and 5GC functions as independent deployment units.

G.2 An SCP based on service mesh

G.2.1 Introduction

This clause describes an SCP deployment based on a distributed model in which SCP endpoints are co-located with 5GC functionality (e.g. an NF, an NF Service, a subset thereof such as a microservice implementing part of an NF/NF service or a superset thereof such as a group of NFs, NF Services or microservices). This example makes no assumptions as to the internal composition of each 5GC functionality (e.g. whether they are internally composed of multiple elements or whether such internal elements communicate with means other than the service mesh depicted in this example).

In this deployment example, Service Agent(s) implementing necessary peripheral tasks (e.g. an SCP endpoint) are co-located with 5GC functionality, as depicted in Figure G.2.1-1. In this example, Service Agents and 5GC functionality, although co-located, are separate components.

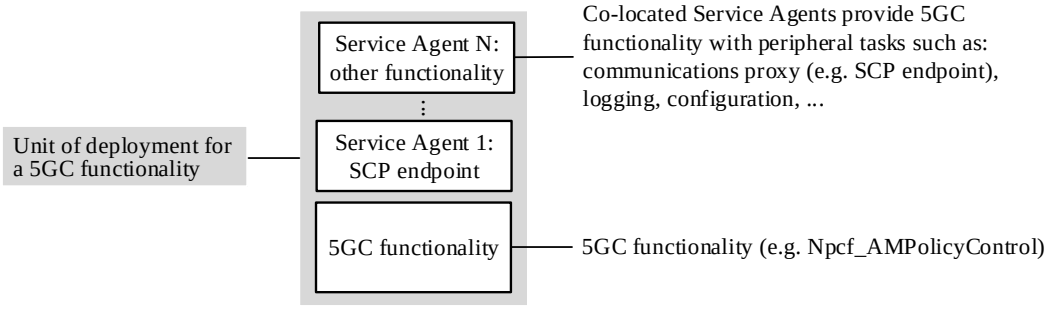


Figure G.2.1-1: Deployment unit: 5GC functionality and co-located Service Agent(s) implementing peripheral tasks

In this deployment example, an SCP Service Agent, i.e. a service communication proxy, is co-located in the same deployment unit with 5GC functionality and provides each deployed unit (e.g. a container-based VNFC) with indirect communication and delegated discovery.

Figure G.2.1-2 shows an overview of this deployment scenario. For SBI-based interactions with other 5GC functionalities, a consumer (5GC functionality A) communicates through its Service Agent via SBI. Its Service Agent selects a target producer based on the request and routes the request to the producer's (5GC functionality B) Service Agent. What routing and selection policies a Service Agent applies for a given request is determined by routing and selection policies pushed by the service mesh controller. Information required by the service mesh controller is pushed by the Service Agents to the service mesh controller.

In this deployment, the SCP manages registration and discovery for communication within the service mesh and it interacts with an external NRF for service exposure and communication across service mesh boundaries. Operator-defined policies are additionally employed to generate the routing and selection policies to be used by the Service Agents.

This example depicts only SBI-based communication via a service mesh, but it does not preclude the simultaneous use of the service mesh for protocols other than SBI supported by the service mesh or that the depicted 5GC functionality additionally communicates via other means.

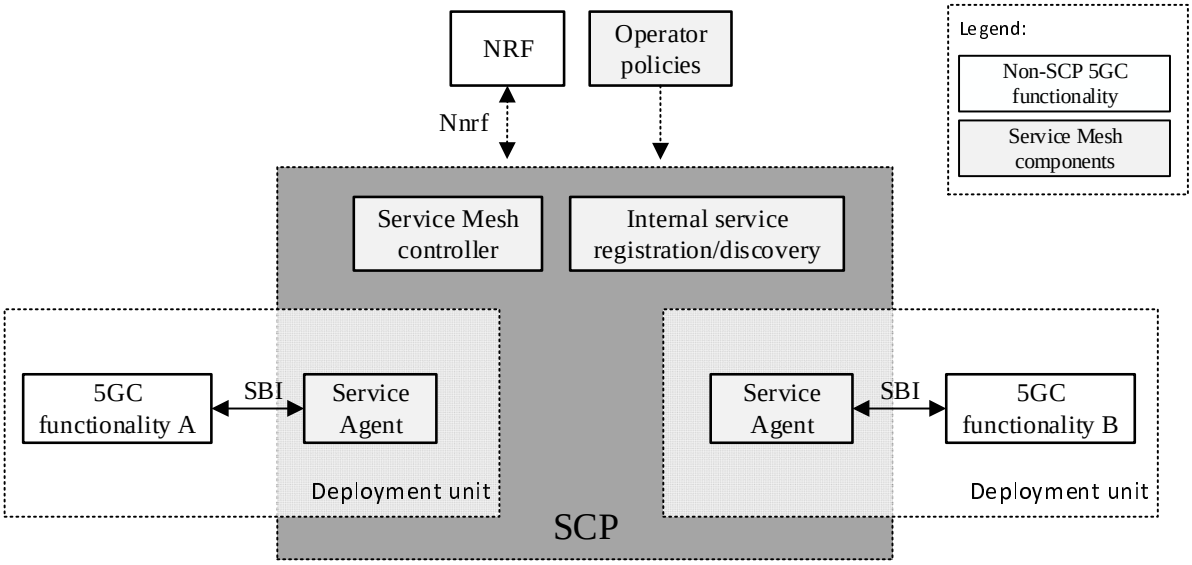


Figure G.2.1-2: SCP Service mesh co-location with 5GC functionality

From a 3GPP perspective, in this deployment example a deployment unit thus contains NF functionality and SCP functionality. Figure G.2.1-3 depicts the boundary between both 3GPP entities. In the depicted example, two NF Services part of the same NF and each exposing an SBI interface are deployed each in a container-based VNFC. A co-located Service Agent provides each NF Service with indirect communication and delegated discovery.

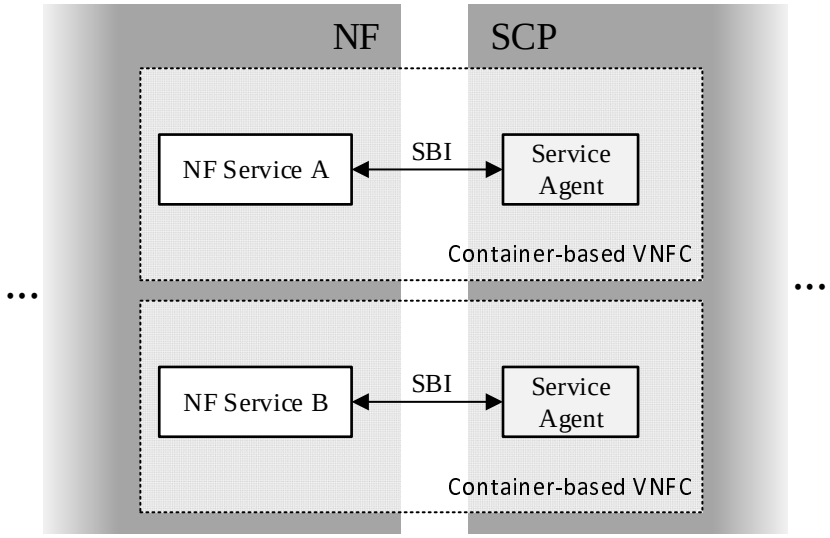


Figure G.2.1-3: Detail of the NF-SCP boundary

G.2.2 Communication across service mesh boundaries

It is a deployment where a single service mesh covers all functionality within a given deployment or not. In cases of communication across the boundaries of a service mesh, the service mesh routing the outbound message knows neither whether the selected producer is in a service mesh nor the internal topology of the potential service mesh where the producer resides.

In such a deployment, as shown in Figure G.2.2.-1, after producer selection is performed, routing policies on the outgoing service mesh are only aware of the next hop.

Given a request sent by A, A's Service Agent will perform producer selection based on the received request. If the selected producer endpoint (e.g. D) is determined to be outside of Service Mesh 1, A's Service Agent routes the request to the Egress Proxy. For a successful routing, the Egress Proxy needs to be able to determine the next hop of the request. In this case, this is the Ingress Proxy of Service Mesh 2. The Ingress Proxy of Service Mesh 2 is, based on the information in the received request and its routing policies, able to determine the route for the request. Subsequently, D receives the request. No topology information needs to be exchanged between Service Mesh 1 and Service Mesh 2 besides a general routing rule towards Service Mesh 2 (e.g. a FQDN prefix) and an Ingress Proxy destination for requests targeting endpoints in Service Mesh 2.

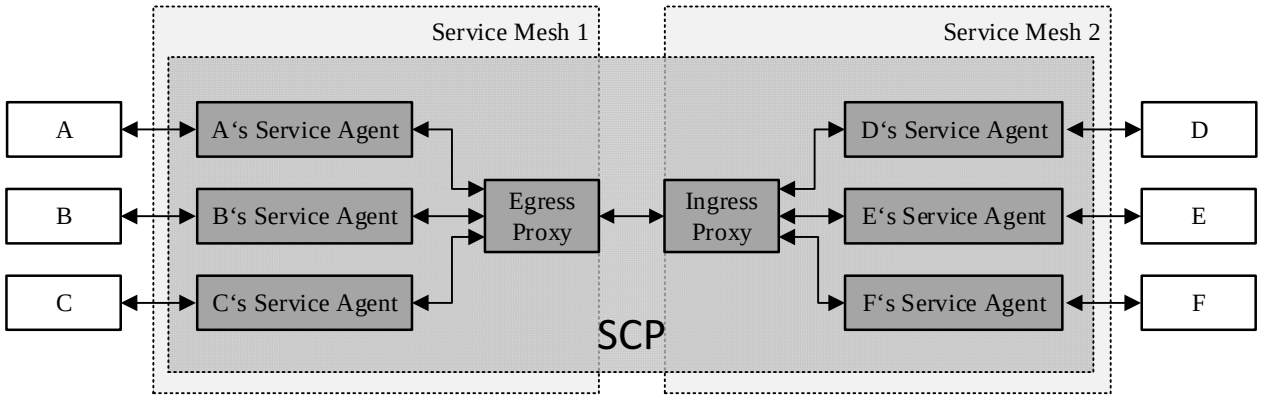


Figure G.2.2-1: Message routing across service mesh boundaries

G.3 An SCP based on independent deployment units

This clause shows an overview of SCP deployment based on the 5GC functionality and SCP being deployed in independent deployment units.

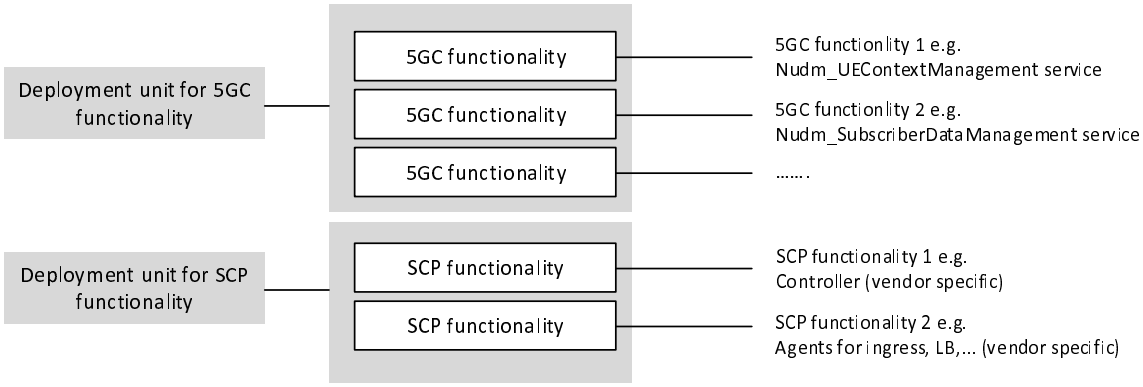


Figure G.3-1: Independent deployment units for SCP and 5GC functionality

The SCP deployment unit can internally make use of microservices, however these microservices are up to vendors implementation and can be for example SCP agents and SCP controller as used in this example. The SCP agents implement the http intermediaries between service consumers and service producers. The SCP agents are controlled by the SCP controller. Communication between SCP controller and SCP agents is via SCP internal interface (4) and up to vendors implementation.

In this model it is a deployment choice to co-locate SCP and other 5GC functions or not. The SCP interfaces (1), (2) and (3) are service based interfaces. SCP itself is not a service producer itself, however acting as http proxy it registers services on behave of the producers in NRF. Interface (2) represents same services as (1) however using SCP proxy addresses. Interface (3) is interfacing NRF e.g. for service registration on behalf of the 5GC functions or service discovery.

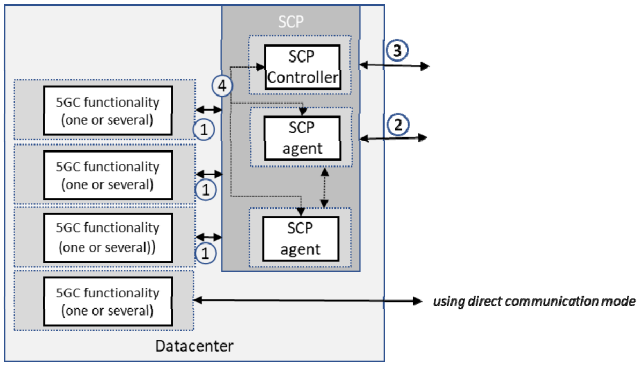


Figure G.3-2: 5GC functionality and SCP co-location choices

For SBI-based interactions with other 5GC functions, a consumer communicates through a SCP agent via SBI (1). SCP agent selects a target based on the request and routes the request to the target SCP agent (2). What routing and selection policies each SCP agent applies for a given request is determined by routing and selection policies determined by the SCP controller using for example information provided via NRF (3) or locally configured in the SCP controller. The routing and selection information is provided by the SCP controller to the SCP agents via SCP internal interface (4). Direct communication can coexist in the same deployment based on 3GPP specified mechanisms.

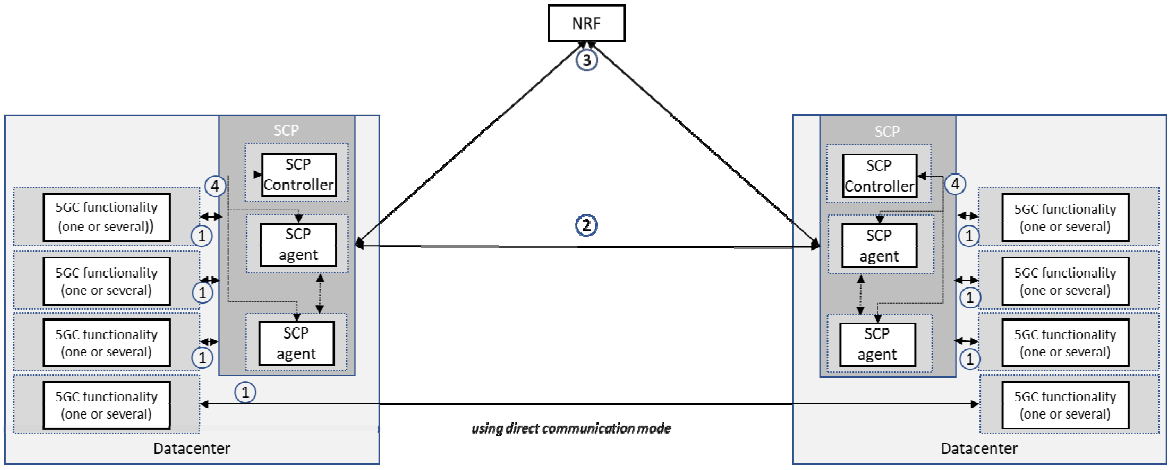


Figure G.3-3: Overview of SCP deployment

G.4 An SCP deployment example based on name-based routing

G.4.0 General Information

This clause provides a deployment example for the SCP which is based on a name-based routing mechanism that provides IP over ICN capabilities such as those described in Xylomenos, George, et al. [G1].

The scenario describes an SCP offering based on an SBA-platform to interconnect 5GC Services (or a subset of the respective services). The Name-based Routing mechanism, described in this deployment example, is realized through a Path Computation Element which is the core part of the SCP. The 5GC Services are running as microservices on cloud/deployment units (clusters). A Service Router is the communication node (access node/gateway) between the SCP and the 5GC Services and resides as a single unit within a Service Deployment Cluster. The Service Router acts as communication proxy and it is responsible for mapping IP based messages onto ICN publication and subscriptions. The Service Router serves multiple 5GC Service Endpoints within that cluster. For direct communication the Service Router is not used.

5GC Functionalities communicate with the Service Router using standardized 3GPP SBIs.

The Functionalities within the Service Deployment Cluster are containerized Service Functions.

Depicted in Figure G.4-1, the Service Router act as SCP termination point and offer the SBI to the respective 5GC Service Functionalities. In this example, Service Routers and 5GC functionality, although co-located, are separate components within the Service Deployment Cluster. Multiple Functionalities can exist within the Service Deployment Cluster, all served by the respective Service Router when needed to communicate to other Service Functionalities within different clusters.

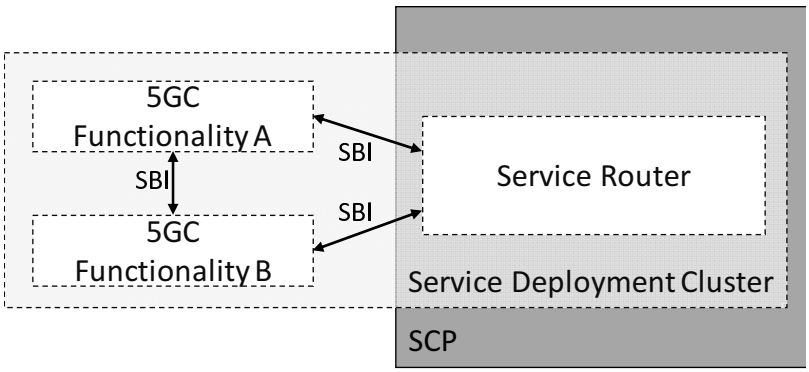


Figure G.4-1: Deployment unit: 5GC functionality and co-located Service Agent(s) implementing peripheral tasks

In Figure G.4-1, the two depicted 5GC Service Functionalities (realized as Network Function Service Instances) may communicate in two ways. However, before the communication can be established between two 5GC Functionalities, Service Registration and Service Discovery need to take place, as described in Figure G.4.1-1. Service Registration and Service Discovery are provided in a standardized manner using 3GPP Service Based Interfaces.

G.4.1 Service Registration and Service Discovery

Service registration can be done in several ways. One option is that ready 5GC Service Functions may register themselves with their service profile via the Nnrf interface. The registration request is forwarded to the internal Registry as well as forwarded to the operator's NRF. The internal registration is used to store the address to identifier relationship and the Service Deployment Cluster location. The external registration (NRF) is used to expose the Service Functionality to Services outside the depicted SCP.

Service discovery entails Function A requesting a resolvable identifier for Functionality B. This resolve request is received by the Service Router which performs the task with the help of the SCP. After the resolve is done, the 5GC Functionalities may communicate either directly without any further interaction through the SCP, when the targeted address is resolved within the same Service Deployment Cluster; or via the Service Router when the Functionality resides outside of the originator's Service Deployment Cluster. The Service Router then acts as gateway towards the underlying SCP platform.

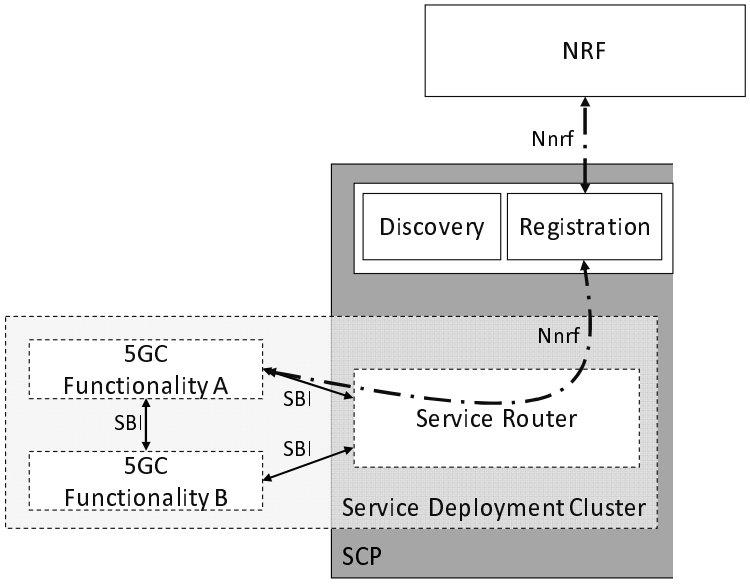


Figure G.4.1-1: Registering 5GC Functionalities in the SCP

G.4.2 Overview of Deployment Scenario

Figure G.4.2-1 shows an overview of this deployment scenario. For SBI-based interactions with other 5GC functionalities, a consumer entity (e.g. 5GC functionality B in the cluster on the left side) communicates through the cluster's Service Router with other entities in other clusters (e.g. 5GC Functionality D in the cluster on the right side). The target selection is performed through the platform's Discovery Service. From the client's perspective, the Service Router is the first and only contact point to the SCP. The platform resolves the requested Service identifier and aligns the results with the platform's policies. The Path Computation Element calculates a path between the consumer and the producer (e.g. the shortest path between the nodes).

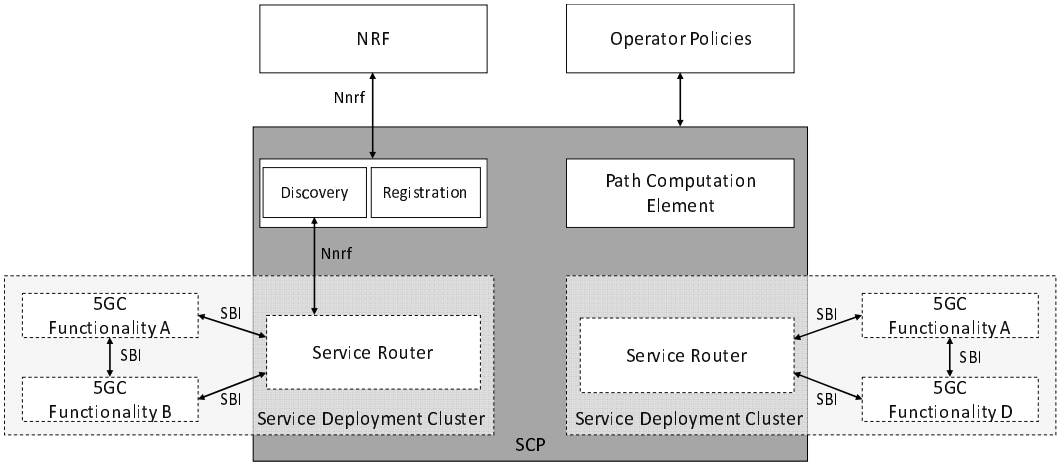


Figure G.4.2-1: (NbR-) SCP interconnects multiple deployment clusters with external NRF

G.4.3 References

[G1] Xylomenos, George, et al.: "IP over ICN goes live", 2018 European Conference on Networks and Communications (EuCNC). IEEE, 2018.

Annex H (normative): TSN usage guidelines

H.1 General

This Annex provides guidelines on the use of certain specific IEEE parameters and protocol messages in the case of TSN as described in clause 5.27.

H.2 Signalling of ingress time for time synchronization

The ingress time is provided from the NW-TT/UPF to the DS-TT/UE as part of a gPTP Sync or Follow_up message using the Suffix field defined in clause 13.4 of IEEE 1588-2008 [107]. The structure of the Suffix field follows the recommendation of clause 14.3 of IEEE 1588-2008 [107], with an organizationId specific to 3GPP, an organizationSubType referring to an ingress timestamp, and data field that carries the ingress timestamp encoded as specified in clause 5.3.3 of IEEE 1588-2008 [107]. TS 24.535 [117] specifies the fields in the gPTP Sync message.

Annex I (normative): TSN usage guidelines

I.1 Determination of traffic pattern information

As described in clause 5.27.2, the calculation of the TSCAI relies upon mapping of information for the TSN stream(s) based upon certain IEEE standard information.

Additional traffic pattern parameters such as maximum burst size and maximum flow bitrate can be mapped to MDBV and GFBR.

The traffic pattern parameter determination based on PSFP (IEEE P802.1Q [98]) is as follows:

- Periodicity of a TSN stream is set equal to PSFPAdminCycleTime if there is only one PSFPGateControlEntry with a PSFPgateStatesValue set to Open in the PSFPAdminControlList. If there is more than one PSFPGateControlEntry with a PSFPgateStatesValue set to Open in the PSFPAdminControlList, then the Periodicity of the TSN Stream is set equal to sum of the timeIntervalValues from the first gate open instance to a next gate open instance in the PSFPAdminControlList. For aggregated TSN streams with same periodicity and compatible Burst Arrival Times, the periodicity of the aggregated flow of these TSN Streams is set equal to PSFPAdminCycleTime received from CNC for one of the TSN streams that are aggregated.

NOTE: Given that only TSN streams that have the same periodicity and compatible Burst Arrival Time can be aggregated, the PSFPAdminCycleTime for those TSN streams is assumed to be the same.

- Burst Arrival time of a TSN stream at the ingress port is determined based on the following conditions:
  - The Burst Arrival Time of a TSN Stream should be set to PSFPAdminBaseTime plus the sum of the timeIntervalValues for which the PSFPgateStatesValue is Closed in the PSFP AdminControlList until the first gate open time (i.e. until PSFPgateStatesValue set to Open is found). If the PSFPgateStatesValue is Open for the first timeIntervalValue, then the Burst Arrival time is set to PSFPAdminBaseTime. For aggregated TSN streams, the arrival time is calculated similarly, but using the time interval to the first PSFPgateStatesValue that is Open from the aggregated TSN streams.
- Flow direction of a TSN stream is determined based on the following conditions:
  - If the ingress port PSFP information is targeted for a DS-TT port, the Flow direction is UL. If the ingress port PSFP information is targeted for a NW-TT port, the Flow direction is DL.
- Burst Size of a TSN stream at the ingress port (which is useful to map to MDBV) is determined based on the following conditions:
  - The Burst Size may be determined from TSN Stream gate control operations in the PSFPAdminControlList. If in the PSFPAdminControlList, IntervalOctetMax is provided for a PSFPGateControlEntry with an "open" PSFPgateStatesValue, the Burst Size is set to the IntervalOctetMax for that control list entry. If IntervalOctetMax is not provided, the Burst Size is set to the timeIntervalValue (converted from ns to s) of the PSFPGateControlEntry with an "open" PSFPgateStatesValue multiplied by the port bitrate.
  - When multiple compatible TSN Streams are aggregated, the Burst Size is set to the sum of the Burst Sizes for each TSN stream as determined above.
- Maximum Flow Bitrate of a TSN stream (which is useful to map to GFBR) is determined as follows:
  - The Maximum Flow Bitrate of a TSN Stream is equal to the summation of all timeIntervalValue (converted from ns to s) with PSFPgateStatesValue = Open, multiplied by the bitrate of the corresponding port, and divided by PSFPAdminCycleTime. For aggregated TSN streams, the same calculation is performed over the burst of aggregated streams (calculated using superposition, i.e., timeIntervalValue with PSFPgateStatesValue = Open of every stream is summed up, as they are assumed to have same periodicity, compatible Burst arrival time, and same traffic class if they are to be aggregated.

Annex J (informative): Link MTU considerations

According to clause 5.6.10.4 networks can provide link MTU size for UEs. A purpose of the link MTU size provisioning is to limit the size of the packets sent by the UE to avoid packet fragmentation in the backbone network between the UE and the UPF acting as PSA (and/or across the N6 reference point). Fragmentation within the backbone network creates a significant overhead. Therefore operators might desire to avoid it. This Annex presents an overhead calculation that can be used by operators to set the link MTU size provided by the network. A UE might not employ the provided link MTU size, e.g. when the MT and TE are separated, as discussed in clause 5.6.10.4. Therefore, providing an MTU size does not guarantee that there will be no packets larger than the provided value. However, if UEs follow the provided link MTU value operators will benefit from reduced transmission overhead within backbone networks.

One of the worst-case scenarios is when GTP packets, e.g., between a NG-RAN node and the 5GC, are transferred over IPSec tunnel in an IPv6 deployment. In that case the user packet first encapsulated in a GTP tunnel which results in the following overhead:

- IPv6 header, which is 40 octets;
- UDP overhead, which is 8 octets;
- Extended GTP-U header, which is 16 octets.

NOTE 1: The sending of a Reflective QoS Indicator within a GTP-U header extension, or the use of Long PDCP PDU numbers at handover will further increase the GTP-U header size (see TS 29.281 [75] and TS 38.415 [116]).

In this scenario the GTP packet then further encapsulated into an IPSec tunnel. The actual IPSec tunnel overhead depends on the used encryption and integrity protection algorithms. TS 33.210 [115] mandates the support of AES-GMAC with a key length of 128 bits and the use of HMAC_SHA-1 for integrity protection. Therefore, the overhead with those algorithms is calculated as:

- IPv6 header, which is 40 octets;
- IPSec Security Parameter Index and Sequence Number overhead, which is 4+4 octets;
- Initialization Vector for the encryption algorithm, which is 16 octets;
- Padding to make the size of the encrypted payload a multiple of 16;
- Padding Length and Next Header octets (2 octets);
- Integrity Check Value, which is 12 octets.

In order to make the user packet size as large as possible a padding of 0 octet is assumed. With this zero padding assumption the total overhead is 142 octets, which results a maximum user packet size of transport MTU minus 142 octets. Note that in the case of transport MTU=1500, this user packet size will result in a 1424 octets payload length to be ciphered, which is a multiple of 16, thus the assumption that no padding is needed is correct (see Figure J.1). Similar calculations can be done for networks with transport that supports larger MTU sizes.

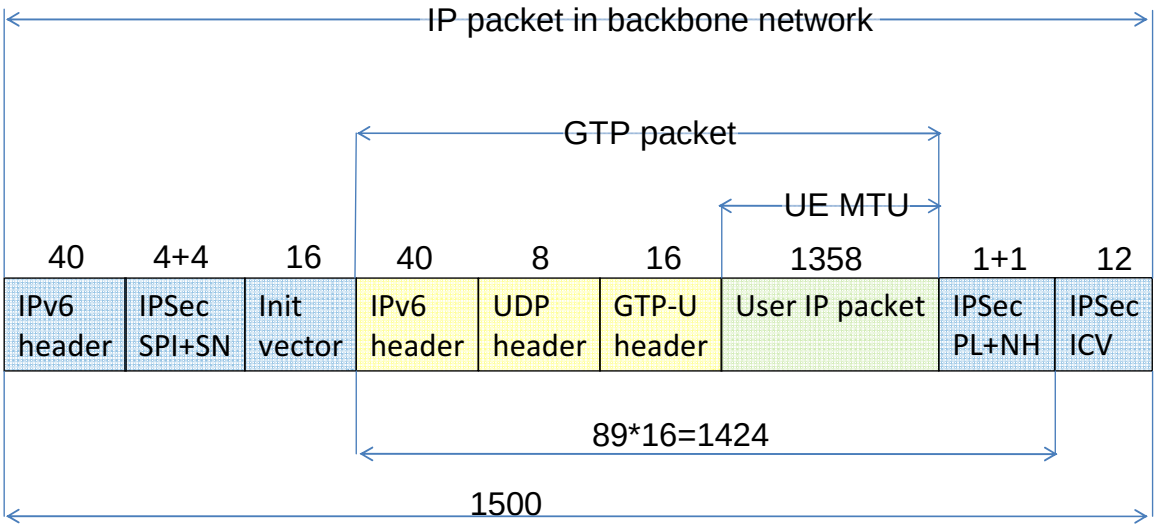


Figure J-1: Overhead calculation for transport MTU=1500 octet

The link MTU value that can prevent fragmentation in the backbone network between the UE and the UPF acting as PSA depends on the actual deployment. Based on the above calculation a link MTU value of 1358 is small enough in most of the network deployments. However for network deployments where the transport uniformly supports for example ethernet jumbo frames, transport MTU<=9216 octets can provide a much larger UE MTU and hence more efficient transfer of user data. One example of when it can be ensured that all links support larger packet sizes, is when the UE uses a specific Network Slice with a limited coverage area.

Note that using a link MTU value smaller than necessary would decrease the efficiency in the network. Moreover, a UE might also apply some tunnelling (e.g., VPN). It is desirable to use a link MTU size that assures at least MTU minus 220 octets within the UE tunnel to avoid the fragmentation of the user packets within the tunnel applied in the UE. In the case transport MTU is 1500 octets, this results a link MTU of 1280 octets (for the transport), which is the minimum MTU size in the case of IPv6.

The above methodology can be modified for calculation of the UE's link MTU when a UPF has MTU limits on the N6 reference point and is offering a PDU Session with Ethernet or Unstructured PDU Session type between the UPF and the UE.

Annex K (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
06-2017	SP#76	SP-170384	-	-	-	MCC Editorial Update for presentation to TSG SA#76 for Information	1.0.0
12-2017	SP#78	-	-	-	-	MCC Editorial Update	2.0.0
12-2017	SP#78	SP-170931	-	-	-	Correction of Annex A figure numbers for presentation to TSG SA#78 for Approval	2.0.1
12-2017	SP#78	-	-	-	-	MCC Editorial Update after TSG SA#78 Approval	15.0.0
03-2018	SP#79	SP-180090	0002	2	F	Using NRF for UPF discovery	15.1.0
03-2018	SP#79	SP-180097	0003	2	F	Configuration information the UE may exchange with the SMF during the lifetime of a PDU Session	15.1.0
03-2018	SP#79	SP-180097	0004	-	F	Handling of MM back-off timer for N3GPP Access	15.1.0
03-2018	SP#79	SP-180097	0005	-	F	Correction of the definitions of Allowed NSSAI and Configured NSSAI	15.1.0
03-2018	SP#79	SP-180097	0006	4	F	Allowed NSSAI and Access Type	15.1.0
03-2018	SP#79	SP-180097	0007	1	F	Correction to rejected S-NSSAI	15.1.0
03-2018	SP#79	SP-180097	0008	2	F	Corrections to Emergency Services	15.1.0
03-2018	SP#79	SP-180096	0009	-	D	Clarification of SUCI	15.1.0
03-2018	SP#79	SP-180096	0010	-	D	Miscellaneous editorial corrections (capitalization, messages, procedures etc.)	15.1.0
03-2018	SP#79	SP-180097	0011	-	F	Corrections to RQoS logic when receiving DL packet with RQI	15.1.0
03-2018	SP#79	SP-180097	0013	-	F	Paging Policy Differentiation correction	15.1.0
03-2018	SP#79	SP-180097	0014	-	F	Clarification on UE specific DRX parameter from old AMF to new AMF	15.1.0
03-2018	SP#79	SP-180097	0015	-	F	Clarification on PCF selection	15.1.0
03-2018	SP#79	SP-180093	0016	-	F	Adding the new clause about SMSF selection	15.1.0
03-2018	SP#79	SP-180090	0017	-	F	Use of identifiers for mobility between GERAN/UTRAN and 5GS	15.1.0
03-2018	SP#79	SP-180090	0018	1	F	Remaining IP address/prefix lifetime with SSC mode 3	15.1.0
03-2018	SP#79	SP-180097	0020	1	F	Correction to handling of S-NSSAI mapping information	15.1.0
03-2018	SP#79	SP-180090	0021	3	F	Wildcard DNN subscription	15.1.0
03-2018	SP#79	SP-180097	0022	4	F	Clarification in LADN clause 5.6.5 - TS 23.501	15.1.0
03-2018	SP#79	SP-180097	0023	-	F	Clean up on the interworking without 26 indication	15.1.0
03-2018	SP#79	SP-180097	0024	-	F	TS 23.501 mobility from EPC to 5GC	15.1.0
03-2018	SP#79	SP-18009	0025	2	F	AMF Load Re-Balancing For CONNECTED mode UE	15.1.0
03-2018	SP#79	SP-180097	0026	-	F	Update on Traffic Detection Information	15.1.0
03-2018	SP#79	SP-180097	0027	-	F	Proposal of Specifying Packet Detection Rule	15.1.0
03-2018	SP#79	SP-180097	0028	1	F	Relation between the SSC mode 3 and the PDU type	15.1.0
03-2018	SP#79	SP-180091	0031	-	F	UE-specific DRX parameter negotiation between UE and AMF	15.1.0
03-2018	SP#79	SP-180091	0033	-	F	Control of the Messages triggering Paging at AMF	15.1.0
03-2018	SP#79	SP-180091	0034	2	F	Alignment with TS 23.502 on Service Request procedure	15.1.0
03-2018	SP#79	SP-180097	0035	-	F	Corrections and clarifications for the usage of Packet Filter Set	15.1.0
03-2018	SP#79	SP-180091	0036	-	F	Update Paging Policy Differentiation	15.1.0
03-2018	SP#79	SP-180097	0037	1	F	Correction to AF influence on traffic routing	15.1.0
03-2018	SP#79	SP-180097	0038	-	F	Clarifications to AF influence on traffic routing	15.1.0
03-2018	SP#79	SP-180097	0039	-	F	Clarify NSSF discovery	15.1.0
03-2018	SP#79	SP-180090	0040	1	F	Change subscribed S-NSSAI in UE to configured NSSAI of HPLMN	15.1.0
03-2018	SP#79	SP-180097	0041	1	F	UDM discovery clarifications	15.1.0
03-2018	SP#79	SP-180097	0044	-	F	Corrections to UPF selection and resolution of related Editor's Note	15.1.0
03-2018	SP#79	SP-180097	0045	1	F	Updates to the Security Edge Protection Proxy description	15.1.0
03-2018	SP#79	SP-180098	0046	-	F	Homogeneous support for IMS voice over PS Session supported indication	15.1.0
03-2018	SP#79	SP-180098	0047	1	F	Slice selection cleanup	15.1.0
03-2018	SP#79	SP-180091	0048	-	F	Resource reservation for services sharing priority	15.1.0
03-2018	SP#79	SP-180098	0049	-	F	Replace PUI with GPSI	15.1.0
03-2018	SP#79	SP-180091	0050	-	F	Idle and connected state terminology cleanup	15.1.0
03-2018	SP#79	SP-180098	0051	-	F	NAS congestion control update	15.1.0
03-2018	SP#79	SP-180098	0052	-	F	Complete of IMS Emergency support in 5G including slice and local numbers	15.1.0
03-2018	SP#79	SP-180098	0053	1	F	Traffic mapping information that disallows UL packets	15.1.0
03-2018	SP#79	SP-180098	0054	1	F	Clean-up of Characteristics signalling	15.1.0
03-2018	SP#79	SP-180093	0055	-	F	EPS Fallback for voice	15.1.0
03-2018	SP#79	SP-180098	0056	1	F	Network sharing prioritised PLMN handling	15.1.0
03-2018	SP#79	SP-180098	0057	2	F	Corrections to Combined N3IWF/ePDG Selection	15.1.0
03-2018	SP#79	SP-180091	0058	1	F	Moving Network Analytics functionality into 23.501	15.1.0
03-2018	SP#79	SP-180098	0061	1	F	Clarification on UDR	15.1.0
03-2018	SP#79	SP-180098	0062	-	F	QFI in N9	15.1.0
03-2018	SP#79	SP-180098	0063	1	F	NF Service Discovery Corrections	15.1.0
03-2018	SP#79	SP-180098	0064	3	F	UE mobility event notification	15.1.0

03-2018	SP#79	SP-180092	0066	4	C	Architectural solution for User Plane (UP) Security policy and User Plane Integrity Protection	15.1.0
03-2018	SP#79	SP-180098	0068	-	F	CN assistance information enhancement	15.1.0
03-2018	SP#79	SP-180098	0070	-	F	Inter-PLMN mobility when N26 is not used	15.1.0
03-2018	SP#79	SP-180093	0071	3	F	Interworking without N26 corrections	15.1.0
03-2018	SP#79	SP-180098	0072	1	F	Clarification for S-NSSAI based congestion Control	15.1.0
03-2018	SP#79	SP-180098	0073	-	F	Non-roaming Architecture for Network Exposure Function in reference point representation	15.1.0
03-2018	SP#79	SP-180098	0074	1	F	NSSF service update	15.1.0
03-2018	SP#79	SP-180092	0075	1	F	Correcting the support of charging Characteristics	15.1.0
03-2018	SP#79	SP-180098	0076	-	F	Non-Allowed Area as criterion for Cell Reselection or trigger for PLMN Selection	15.1.0
03-2018	SP#79	SP-180098	0077	1	F	Correction to the use of Redirection in EPS fallback for emergency services	15.1.0
03-2018	SP#79	SP-180098	0078	2	F	Network Provided Location for non-3GPP access	15.1.0
03-2018	SP#79	SP-180098	0082	1	F	Updates to TS 23.501 Scope	15.1.0
03-2018	SP#79	SP-180098	0083	1	F	Fixes for CP protocol stack	15.1.0
03-2018	SP#79	SP-180098	0084	1	F	EPC to 5GC Migration fixes for Option 7	15.1.0
03-2018	SP#79	SP-180098	0085	1	F	EPS Interworking: 5G-S-TMSI derivation and context retrieval	15.1.0
03-2018	SP#79	SP-180099	0086	1	F	Fixes for Emergency Services and Emergency Services using Fallback	15.1.0
03-2018	SP#79	SP-180099	0087	2	F	5G QoS fixes for URLLC services related attributes - PDB, PER, MDB, 5QI	15.1.0
03-2018	SP#79	SP-180099	0088	4	F	QoS Notification control and Release	15.1.0
03-2018	SP#79	SP-180095	0089	4	C	GUTI unique across AMFs in an AMF SET	15.1.0
03-2018	SP#79	SP-180099	0090	1	F	Partitioning of Identifier space to ensure success of Context retrieval for EPS Interworking	15.1.0
03-2018	SP#79	SP-180099	0091	1	F	UDM Discovery with SUPI as input	15.1.0
03-2018	SP#79	SP-180099	0095	5	F	Clarifications of Subscribed and Configured S-NSSAI update	15.1.0
03-2018	SP#79	SP-180099	0102	4	F	Sending of congested S-NSSAI during AN signalling connection Establishment	15.1.0
03-2018	SP#79	SP-180099	0104	3	F	Clarification on modification of the set of network slices for a UE	15.1.0
03-2018	SP#79	SP-180092	0105	1	F	UE support for Multi-homed IPv6 PDU Session	15.1.0
03-2018	SP#79	SP-180099	0106	1	F	5GS support for network slicing	15.1.0
03-2018	SP#79	SP-180093	0107	2	F	UE Core Network Capability handling	15.1.0
03-2018	SP#79	SP-180099	0108	-	F	eCall over IMS supported over E-UTRA only	15.1.0
03-2018	SP#79	SP-180090	0109	2	F	Domain selection for UE in Dual Registration mode	15.1.0
03-2018	SP#79	SP-180099	0110	2	F	MICO and interworking with EPC	15.1.0
03-2018	SP#79	SP-180099	0115	2	F	Correction of NSSAI handling	15.1.0
03-2018	SP#79	SP-180099	0116	1	F	Slice Availability update	15.1.0
03-2018	SP#79	SP-180099	0122	2	F	User Plane management to support interworking with EPS	15.1.0
03-2018	SP#79	SP-180099	0124	3	F	Supporting Common API framework for NEF	15.1.0
03-2018	SP#79	SP-180099	0126	1	F	Clarification on NAS recovery procedure in RRC Inactive	15.1.0
03-2018	SP#79	SP-180099	0129	2	F	Correction for congestion control	15.1.0
03-2018	SP#79	SP-180096	0133	-	D	Correction for the usage of RQI bit	15.1.0
03-2018	SP#79	SP-180099	0134	5	F	Clarifications for QoS Framework	15.1.0
03-2018	SP#79	SP-180099	0135	2	F	DL signalling handling for non-3GPP PDU Session	15.1.0
03-2018	SP#79	SP-180099	0136	1	F	Clarification on location reporting for LADN in RRC Inactive clause 5.3.3.2.5 - TS 23.501	15.1.0
03-2018	SP#79	SP-180099	0137	2	F	Network Sharing and Interworking with EPS- TS 23.501	15.1.0
03-2018	SP#79	SP-180099	0138	-	F	Edge Computing Clarification	15.1.0
03-2018	SP#79	SP-180095	0141	1	B	Supporting 3GPP PS Data Off in 5GS	15.1.0
03-2018	SP#79	SP-180099	0144	2	F	Management of service area restriction information	15.1.0
03-2018	SP#79	SP-180099	0145	2	F	Clarification on TAI list assignment for different 5G RATs	15.1.0
03-2018	SP#79	SP-180099	0146	-	F	Network sharing for supporting RRC redirection procedure	15.1.0
03-2018	SP#79	SP-180095	0147	2	C	Selection of NAS procedures for E-UTRA connected to both EPC and 5GC	15.1.0
03-2018	SP#79	SP-180100	0149	1	F	Clarification of SM congestion control	15.1.0
03-2018	SP#79	SP-180100	0150	1	F	Updates to AF influence on traffic routing	15.1.0
03-2018	SP#79	SP-180100	0151	2	F	Updates to description of CN Tunnel Info	15.1.0
03-2018	SP#79	SP-180100	0152	-	F	Clarification on RRM desciption	15.1.0
03-2018	SP#79	SP-180100	0153	1	F	Editorial corrections in clause 5.3.2.4 Support of a UE registered over both 3GPP and Non-3GPP access	15.1.0
03-2018	SP#79	SP-180100	0154	2	F	Clarification on the association of an S-NSSAI to a given application	15.1.0
03-2018	SP#79	SP-180100	0155	2	F	Update of UE Network slicing configuration	15.1.0
03-2018	SP#79	SP-180100	0157	2	F	SBA Scope Clarification	15.1.0
03-2018	SP#79	SP-180092	0158	2	F	Clean up for BSF	15.1.0
03-2018	SP#79	SP-180092	0160	3	F	Clarification on Area of Interest for Presence Area Reporting	15.1.0
03-2018	SP#79	SP-180100	0161	3	F	Correction to Providing AF request to multiple PCFs	15.1.0
03-2018	SP#79	SP-180100	0165	1	F	Usage of Unified access control in priority mechanisms	15.1.0
03-2018	SP#79	SP-180100	0166	-	F	Update Roaming reference architectures	15.1.0

03-2018	SP#79	SP-180100	0168	5	F	Clarification of UE Requested NSSAI	15.1.0
03-2018	SP#79	SP-180100	0170	1	F	Emergency Services Support indication per RAT	15.1.0
03-2018	SP#79	SP-180100	0171	2	F	N4 User Plane Path	15.1.0
03-2018	SP#79	SP-180100	0173	1	F	SSC Mode Selection	15.1.0
03-2018	SP#79	SP-180100	0174	2	F	Proposal of QER, URR and FAR	15.1.0
03-2018	SP#79	SP-180100	0177	1	F	UE specific DRX parameters for CM-CONNECTED with Inactive state	15.1.0
03-2018	SP#79	SP-180100	0179	6	F	Slicing configuration update	15.1.0
03-2018	SP#79	SP-180100	0180	1	F	Update of Mobility Restrictions	15.1.0
03-2018	SP#79	SP-180125	0181	1	B	Addition of PDU Session type IPv4v6	15.1.0
03-2018	SP#79	SP-180100	0183	1	F	Mapping of Requested NSSAI clarification	15.1.0
03-2018	SP#79	SP-180100	0184	2	F	Clarification of the interworking between 5G and GERAN/UTRAN/E-UTRAN when UE is in RRC-inactive state	15.1.0
03-2018	SP#79	SP-180100	0187	5	F	Select the same SMF+UPF for PDU sessions of the same DNN within one slice	15.1.0
03-2018	SP#79	SP-180100	0189	2	F	Subscription Permanent Identifier	15.1.0
03-2018	SP#79	SP-180100	0192	1	F	Clarification of interworking procedures without N26 interface	15.1.0
03-2018	SP#79	SP-180100	0194	1	F	Clarification on the use of the indicator for the support of interworking without N26	15.1.0
06-2018	SP#80	SP-180482	0067	6	F	Controlled support of (AF) session binding for Ethernet PDU Session Type	15.2.0
06-2018	SP#80	SP-180491	0117	7	F	Use of Priority parameters for scheduling	15.2.0
06-2018	SP#80	SP-180489	0169	8	F	Temporary restriction of Reflective QoS	15.2.0
06-2018	SP#80	SP-180478	0196	1	F	5_16_6_Mission Critical Services - Reference Update	15.2.0
06-2018	SP#80	SP-180478	0197	1	F	5_16_6_Mission Critical Services - Editorial Changes	15.2.0
06-2018	SP#80	SP-180477	0198	-	D	Fixing Incorrect References to the Service Request Procedures	15.2.0
06-2018	SP#80	SP-180489	0199	2	F	SUPI based paging	15.2.0
06-2018	SP#80	SP-180486	0201	2	F	Mobile Terminated SMS over NAS: 5GS Access Selection	15.2.0
06-2018	SP#80	SP-180483	0203	1	F	Discovery and Topology Hiding	15.2.0
06-2018	SP#80	SP-180479	0206	3	F	Changed length and mapping of 5GS Temporary Identifiers	15.2.0
06-2018	SP#80	SP-180488	0207	5	F	Slice configuration change	15.2.0
06-2018	SP#80	SP-180483	0209	1	F	Defining NWDAF in 23.501	15.2.0
06-2018	SP#80	SP-180484	0210	3	F	Corrections to PFD management	15.2.0
06-2018	SP#80	SP-180491	0212	2	F	Update on UE mobility event notification	15.2.0
06-2018	SP#80	SP-180485	0214	1	F	Identification and update of UE derived QoS rule	15.2.0
06-2018	SP#80	SP-180479	0216	2	F	Clarification of traffic steering control in the case of interworking	15.2.0
06-2018	SP#80	SP-180491	0217	2	F	Updates to System Enablers for Priority Mechanism	15.2.0
06-2018	SP#80	SP-180478	0219	2	F	AMF Selection aspects	15.2.0
06-2018	SP#80	SP-180478	0220	1	F	AMF functionality clarification - to add SUCI	15.2.0
06-2018	SP#80	SP-180484	0222	1	F	EPS Interworking Principles - SR mode with N26	15.2.0
06-2018	SP#80	SP-180490	0224	1	F	UDM services - addition to Nudm_UEAuthentication	15.2.0
06-2018	SP#80	SP-180490	0225	0	F	UDM functionality support for SUCI	15.2.0
06-2018	SP#80	SP-180486	0226	3	F	MFBR Enforcement for GBR QoS flows	15.2.0
06-2018	SP#80	SP-180486	0227	1	F	NF Registration via the NRF	15.2.0
06-2018	SP#80	SP-180478	0229	-	F	Abbreviations supplement	15.2.0
06-2018	SP#80	SP-180478	0231	1	F	3GPP PS Data Off Clarification	15.2.0
06-2018	SP#80	SP-180477	0232	-	D	Network Sharing and Interworking Clarification	15.2.0
06-2018	SP#80	SP-180480	0237	3	F	Clarification on MT SMS domain selection by SMSF	15.2.0
06-2018	SP#80	SP-180489	0239	1	F	TS 23.501: Clean-up for the RRC Inactive related procedure	15.2.0
06-2018	SP#80	SP-180489	0240	-	F	Correction on Control Plane protocol stacks	15.2.0
06-2018	SP#80	SP-180480	0241	2	F	Clarification on NSSAI related functionality in 5G RAN	15.2.0
06-2018	SP#80	SP-180489	0242	2	F	Clarification on Application data	15.2.0
06-2018	SP#80	SP-180479	0244	3	F	AMF UE area of interest reporting in RRC inactive state	15.2.0
06-2018	SP#80	SP-180480	0245	-	F	Clarification on RAT fallback	15.2.0
06-2018	SP#80	SP-180480	0248	1	F	Clarification on notification message	15.2.0
06-2018	SP#80	SP-180477	0250	-	D	Editorial correction in clause 5.9.2 Subscription Permanent Identifier	15.2.0
06-2018	SP#80	SP-180481	0251	8	F	Correction to DNN subscription	15.2.0
06-2018	SP#80	SP-180481	0254	4	F	Clarification on the support of Delay Critical resource type	15.2.0
06-2018	SP#80	SP-180486	0255	7	F	Network slicing clause cleanup	15.2.0
06-2018	SP#80	SP-180490	0261	1	F	UE and network shall override the Core Network type restriction for regulatory prioritized services	15.2.0
06-2018	SP#80	SP-180481	0262	1	F	Clarification to the usage of Internal-Group Identifier	15.2.0
06-2018	SP#80	SP-180484	0264	5	F	Different types of Ethernet services and N4	15.2.0
06-2018	SP#80	SP-180487	0265	3	F	Providing AF with information on the N6 User Plane tunnelling information	15.2.0
06-2018	SP#80	SP-180488	0266	4	F	SMF getting UE location from the AMF for NPLI when no QoS flow to create/Update/modify	15.2.0
06-2018	SP#80	SP-180487	0267	-	F	Removal of network restriction for eight concurrent S-NSSAIs when serving a UE	15.2.0
06-2018	SP#80	SP-180487	0268	-	F	Removal of duplicated requirements for Allowed/Configured NSSAI	15.2.0

06-2018	SP#80	SP-180482	0269	2	F	Correction to AMF and S-NSSAI overload control	15.2.0
06-2018	SP#80	SP-180478	0270	-	F	AMF Name and AMF N2AP UE ID	15.2.0
06-2018	SP#80	SP-180482	0271	2	F	Correction for support of the Ethernet Type PDU Session	15.2.0
06-2018	SP#80	SP-180484	0272	1	F	Correction on aspects for LADN	15.2.0
06-2018	SP#80	SP-180489	0273	1	F	Subscription status notification for Event Exposure service	15.2.0
06-2018	SP#80	SP-180480	0275	1	F	Clarification on SMF selection	15.2.0
06-2018	SP#80	SP-180480	0276	2	F	Clarification on SMSF selection	15.2.0
06-2018	SP#80	SP-180490	0280	1	F	Update for providing policy requirements to multiple UEs	15.2.0
06-2018	SP#80	SP-180481	0282	2	F	Clarifying handling of reachability state	15.2.0
06-2018	SP#80	SP-180484	0283	6	F	Dual Registration mode of operation from E-UTRA cell connecting to both EPC and 5GC	15.2.0
06-2018	SP#80	SP-180482	0284	2	F	Consolidation of UE Network Capabilities	15.2.0
06-2018	SP#80	SP-180486	0285	1	F	NAS level congestion control for emergency and high priority access	15.2.0
06-2018	SP#80	SP-180476	0286	1	C	Coexistence of RRC Inactive and Dual Connectivity	15.2.0
06-2018	SP#80	SP-180486	0287	3	F	Mapped parameters in case of No N26	15.2.0
06-2018	SP#80	SP-180481	0289	2	F	Clarification on the use of shared AMF Pointer value	15.2.0
06-2018	SP#80	SP-180488	0290	1	F	ReAuthentication by an external DN-AAA server	15.2.0
06-2018	SP#80	SP-180484	0292	6	F	LADN configuration of UE	15.2.0
06-2018	SP#80	SP-180479	0295	1	F	Clarification of S-NSSAI based congestion control	15.2.0
06-2018	SP#80	SP-180478	0296	4	F	Add indication of Notification Control to QoS rules sent to UE	15.2.0
06-2018	SP#80	SP-180485	0297	1	F	Local deactivate MICO for emergency service	15.2.0
06-2018	SP#80	SP-180484	0298	4	F	How the SMF validates UE location when requested for LADN PDU Session establishment	15.2.0
06-2018	SP#80	SP-180479	0302	1	F	AUSF clarification and alignment	15.2.0
06-2018	SP#80	SP-180477	0303	-	D	Correction to references	15.2.0
06-2018	SP#80	SP-180480	0304	3	F	Clarification on N3GPP TAI	15.2.0
06-2018	SP#80	SP-180482	0305	6	F	Correction on capability negotiation on "SMS over NAS"	15.2.0
06-2018	SP#80	SP-180478	0306	1	F	Alignment of the name of the network function	15.2.0
06-2018	SP#80	SP-180482	0308	3	F	Correction on NAS level congestion control	15.2.0
06-2018	SP#80	SP-180479	0310	2	F	Clarification on AMF management	15.2.0
06-2018	SP#80	SP-180488	0311	4	F	S-NSSAI check for activation of UP connection of PDU Session	15.2.0
06-2018	SP#80	SP-180481	0313	3	F	Clarifications required resulting from 6-bit QFI limit	15.2.0
06-2018	SP#80	SP-180486	0314	1	F	Missing "redirection" to E-UTRA connected to 5GC	15.2.0
06-2018	SP#80	SP-180479	0319	1	F	Clarification of high priority access	15.2.0
06-2018	SP#80	SP-180476	0323	3	F	Dual connectivity support for network slices	15.2.0
06-2018	SP#80	SP-180481	0325	-	F	Clarification to the NRF Roaming architecture	15.2.0
06-2018	SP#80	SP-180488	0326	2	F	Slicing information and RFSP	15.2.0
06-2018	SP#80	SP-180490	0327	-	F	TS 23.501: UE DL Signalling handling in RRC Inactive State	15.2.0
06-2018	SP#80	SP-180489	0331	1	F	Some TADs fix's	15.2.0
06-2018	SP#80	SP-180485	0334	1	F	Handling of maximum supported data rate per UE for integrity protection	15.2.0
06-2018	SP#80	SP-180486	0335	-	F	NF/NF service registration and status subscribe/notify description updates	15.2.0
06-2018	SP#80	SP-180491	0336	1	F	Use of results of NF/NF service discovery for NF/NF service selection	15.2.0
06-2018	SP#80	SP-180489	0338	4	F	Subscribed SMSF address	15.2.0
06-2018	SP#80	SP-180488	0339	-	F	SEPP fully redundant and next-hop IPX proxy	15.2.0
06-2018	SP#80	SP-180488	0342	1	F	SMF selection factor	15.2.0
06-2018	SP#80	SP-180485	0344	-	F	IPsec SAs in tunnel mode	15.2.0
06-2018	SP#80	SP-180484	0345	1	F	Determining interworking support for PDU sessions in case of interworking without N26	15.2.0
06-2018	SP#80	SP-180485	0346	1	F	Fixing the definition of signalled QoS rule	15.2.0
06-2018	SP#80	SP-180481	0349	2	F	Clarify GUTI aspects for single-registration mode UEs for interworking without N26	15.2.0
06-2018	SP#80	SP-180486	0351	-	F	N9 missing in some figures	15.2.0
06-2018	SP#80	SP-180486	0352	2	F	NF instance and NF service instance definitions	15.2.0
06-2018	SP#80	SP-180483	0353	2	F	Correction to UE Radio Capability handling	15.2.0
06-2018	SP#80	SP-180485	0355	1	F	Further QoS clean-up	15.2.0
06-2018	SP#80	SP-180482	0356	1	F	Coordination of reference point allocation	15.2.0
06-2018	SP#80	SP-180485	0359	2	F	Handling of Configured NSSAIs in Roaming Scenarios - 23.501	15.2.0
06-2018	SP#80	SP-180490	0363	1	F	Update and correction of table for AMF, UDM, UDR, NSSF, UDSF and BSF services	15.2.0
06-2018	SP#80	SP-180490	0365	1	F	Update of FAR	15.2.0
06-2018	SP#80	SP-180486	0367	1	F	NEF Services	15.2.0
06-2018	SP#80	SP-180477	0368	2	D	Editor's note clean-up	15.2.0
06-2018	SP#80	SP-180482	0370	3	F	Compute - Storage split principles	15.2.0
06-2018	SP#80	SP-180484	0371	-	F	Emergency Services Fallback Support indicator validity in the Registration Area	15.2.0
06-2018	SP#80	SP-180485	0372	-	F	LMF Services	15.2.0
06-2018	SP#80	SP-180490	0375	2	F	UDM-AUSF Discovery	15.2.0

06-2018	SP#80	SP-180481	0383	2	F	Clarification on usage of PLMN ID received via PCO during PDN connection establishment	15.2.0
06-2018	SP#80	SP-180483	0385	-	F	Correction to the mapping to the Subscribed S-NSSAI(s)	15.2.0
06-2018	SP#80	SP-180487	0386	2	F	Provisioning NSSP	15.2.0
06-2018	SP#80	SP-180489	0389	1	F	Tracking Area in 5GS	15.2.0
06-2018	SP#80	SP-180483	0390	1	F	Correction to S-NSSAI congestion	15.2.0
06-2018	SP#80	SP-180481	0391	1	F	Clarification to PDU Session Types: MTU	15.2.0
06-2018	SP#80	SP-180478	0394	3	F	Alignment of radio capabilities procedure	15.2.0
06-2018	SP#80	SP-180482	0396	2	F	CN type indicator in AS signalling	15.2.0
06-2018	SP#80	SP-180483	0397	1	F	Correction to eCall Support by NR	15.2.0
06-2018	SP#80	SP-180479	0398	1	F	Bit rate enforcement	15.2.0
06-2018	SP#80	SP-180480	0399	-	F	Clarification on TAC format at inter-system handover	15.2.0
06-2018	SP#80	SP-180478	0401	1	F	Add table of CHF Spending Limit Control service in 7.2.x	15.2.0
06-2018	SP#80	SP-180488	0402	2	F	S-NSSAI of VPLMN when HO from 4G to 5G	15.2.0
06-2018	SP#80	SP-180489	0403	-	F	SSC Mode Selection clarification	15.2.0
06-2018	SP#80	SP-180485	0404	1	F	How Peer CP NF sends notification to target/new AMF after AMF planned removal	15.2.0
06-2018	SP#80	SP-180478	0405	1	F	AF influence on traffic routing for Ethernet type PDU Session	15.2.0
06-2018	SP#80	SP-180479	0406	2	F	Avoid the case the one UE MAC shared by multiple Ethernet PDU Sessions	15.2.0
06-2018	SP#80	SP-180485	0407	1	F	How AMF provides LADN Information to UE	15.2.0
06-2018	SP#80	SP-180477	0410	-	D	Non-3GPP access node selection information	15.2.0
06-2018	SP#80	SP-180496	0411	-	F	Clarify RAT restrictions are not provided to the UE	15.2.0
06-2018	SP#80	SP-180485	0414	1	F	Including GUAMI in RRC message of related procedures	15.2.0
06-2018	SP#80	SP-180479	0415	1	F	Clarification on CN assistance information	15.2.0
06-2018	SP#80	SP-180481	0416	2	F	Clarify the relationship between GFBR and MDBV	15.2.0
06-2018	SP#80	SP-180480	0417	2	F	Clarification on support of MFBR greater than GFBR	15.2.0
06-2018	SP#80	SP-180480	0418	1	F	Clarification on requested NSSAI usage by RAN	15.2.0
06-2018	SP#80	SP-180480	0422	-	F	Clarification on SMSF checking subscription data	15.2.0
06-2018	SP#80	SP-180488	0423	-	F	S-NSSAI back off timer for UE requested PDU session release	15.2.0
06-2018	SP#80	SP-180479	0424	2	F	Clarification on AF influence on traffic routing	15.2.0
06-2018	SP#80	SP-180482	0425	2	F	Combined SMF+PGW-C Selection	15.2.0
06-2018	SP#80	SP-180488	0430	-	F	Resume procedure in the equivalent PLMN	15.2.0
06-2018	SP#80	SP-180478	0433	-	F	Alignment of selective activation of UP connection of existing PDU Session	15.2.0
06-2018	SP#80	SP-180478	0435	1	F	Alignment of PCF selection description	15.2.0
06-2018	SP#80	SP-180487	0436	4	F	QNC during Handover	15.2.0
06-2018	SP#80	SP-180487	0437	3	F	Reflective QoS in interworking	15.2.0
06-2018	SP#80	SP-180491	0438	2	F	Use of Network Instance	15.2.0
06-2018	SP#80	SP-180490	0439	3	F	Update of N4 Parameter Descriptions and Tables	15.2.0
06-2018	SP#80	SP-180480	0441	3	F	Clarification on LADN 5.6.5	15.2.0
06-2018	SP#80	SP-180486	0444	3	F	Network slicing subsription change and update of UE configuration	15.2.0
06-2018	SP#80	SP-180479	0446	2	F	Clarification note on Network Slice limitation	15.2.0
06-2018	SP#80	SP-180478	0447	1	F	Adding default value for Averaging Window	15.2.0
06-2018	SP#80	SP-180486	0448	1	F	Mobility restrictions	15.2.0
06-2018	SP#80	SP-180479	0451	2	F	Capturing subsequent mobility to and from GERAN/UTRAN	15.2.0
06-2018	SP#80	SP-180485	0453	-	F	GFBR is applicable only for GBR QoS flows	15.2.0
06-2018	SP#80	SP-180556	0454	2	F	NSSAI handling in PDU Session Establishment procedures in roaming	15.2.0
06-2018	SP#80	SP-180483	0456	1	F	Correction to identifiers in Registration procedure	15.2.0
06-2018	SP#80	SP-180487	0459	1	F	Radio capabilities after 5GS registration	15.2.0
09-2018	SP#81	SP-180713	0455	3	F	Storage of structured proprietory data in UDSF	15.3.0
09-2018	SP#81	SP-180713	0460	3	F	Missing TADs behaviour	15.3.0
09-2018	SP#81	SP-180713	0463	-	F	Correcting handling of RAT restriction and Forbidden Areas	15.3.0
09-2018	SP#81	SP-180713	0464	3	F	Clarification on LADN	15.3.0
09-2018	SP#81	SP-180713	0465	3	F	Clarification on a wildcard DNN	15.3.0
09-2018	SP#81	SP-180713	0466	3	F	Correcting use of identifiers during registration in equivalent PLMNs	15.3.0
09-2018	SP#81	SP-180713	0470	1	F	Clarification on UE context exchanged on N26 interface	15.3.0
09-2018	SP#81	SP-180713	0471	1	F	Correction to AF influence on traffic routing	15.3.0
09-2018	SP#81	SP-180713	0472	2	F	Clarification on UE Registration type with only PDU Session for Emergency Services	15.3.0
09-2018	SP#81	SP-180713	0473	7	F	The resource type of QoS Flow associated with the default QoS rule	15.3.0
09-2018	SP#81	SP-180724	0474	5	B	Support of tracing in 5GS signalling: overview	15.3.0
09-2018	SP#81	SP-180713	0475	-	F	MCC implementation correction of 23.501 CR0255R7	15.3.0
09-2018	SP#81	SP-180713	0480	3	F	5QI-QCI alignment	15.3.0
09-2018	SP#81	SP-180713	0481	2	F	Number of packet filters supported by UE	15.3.0
09-2018	SP#81	SP-180713	0482	2	F	Paging policy differentiation for RRC inactive	15.3.0
09-2018	SP#81	SP-180713	0485	4	F	Application detection report when the PFDs are removed	15.3.0
09-2018	SP#81	SP-180713	0487	5	F	Correction to Configured NSSAI for the HPLMN	15.3.0
09-2018	SP#81	SP-180713	0488	1	F	Correction to TAI list generation	15.3.0

09-2018	SP#81	SP-180713	0493	1	F	Network Exposure in Roaming Situations	15.3.0
09-2018	SP#81	SP-180713	0494	1	F	Handling of UP Security Policy when IWK with EPS	15.3.0
09-2018	SP#81	SP-180713	0497	2	F	Clarification on handling of Ethernet frames at UPF	15.3.0
09-2018	SP#81	SP-180713	0498	4	F	Completion of description on Configured NSSAIs	15.3.0
09-2018	SP#81	SP-180713	0499	-	F	LADN Clarification	15.3.0
09-2018	SP#81	SP-180713	0500	1	F	DNN Usage Clarification	15.3.0
09-2018	SP#81	SP-180713	0501	4	F	Clarification for pre-configured QoS rule	15.3.0
09-2018	SP#81	SP-180714	0502	1	F	Clarification for QoS handling at UPF	15.3.0
09-2018	SP#81	SP-180714	0504	3	F	DL signalling handling for non-3GPP PDU Session	15.3.0
09-2018	SP#81	SP-180714	0508	2	F	Emergency call and eCall support when the ng-eNode is connected to EPC and 5GC	15.3.0
09-2018	SP#81	SP-180714	0509	1	F	Mobility Restriction List clean up	15.3.0
09-2018	SP#81	SP-180714	0515	1	F	Subscription of selecting the same SMF and UPF	15.3.0
09-2018	SP#81	SP-180714	0516	3	F	GUAMI Definition Correction	15.3.0
09-2018	SP#81	SP-180714	0518	1	F	Merging Network Slice with regular EPS Interworking	15.3.0
09-2018	SP#81	SP-180714	0520	2	F	Notification Control applicability	15.3.0
09-2018	SP#81	SP-180714	0521	1	F	23.501: 5G AN Parameters sent during Service Request	15.3.0
09-2018	SP#81	SP-180714	0524	-	F	Null interworking with GERAN/UTRAN CS domain	15.3.0
09-2018	SP#81	SP-180714	0525	-	F	Correction on mobility management back-off timer	15.3.0
09-2018	SP#81	SP-180714	0527	-	F	5G-TMSI should map to M-TMSI	15.3.0
09-2018	SP#81	SP-180714	0529	1	F	Clarification on Homogeneous Support of IMS Voice over PS Sessions indication	15.3.0
09-2018	SP#81	SP-180714	0530	3	F	Clarification on the non-IP PDU session type for EPS to 5GS interworking	15.3.0
09-2018	SP#81	SP-180714	0531	2	F	Clarification on the PDU session handling in EPS to 5GS handover with N26	15.3.0
09-2018	SP#81	SP-180714	0532	1	F	Incorrect text implying slicing is optional	15.3.0
09-2018	SP#81	SP-180714	0533	-	F	Update of SMSF selection function	15.3.0
09-2018	SP#81	SP-180714	0534	1	F	Corrections to NF profile description	15.3.0
09-2018	SP#81	SP-180714	0535	1	F	Corrections to NF services names and references	15.3.0
09-2018	SP#81	SP-180714	0536	-	F	Update on AUSF service operation to support Steering of Roaming	15.3.0
09-2018	SP#81	SP-180714	0538	3	F	Correction to interworking with EPC with N3GPP PDU Sessions	15.3.0
09-2018	SP#81	SP-180714	0539	3	F	Emergency Services Support indicator for non-3GPP access	15.3.0
09-2018	SP#81	SP-180714	0540	1	F	Clarification of the AMF Set definition	15.3.0
09-2018	SP#81	SP-180714	0542	1	F	Clarification on priority service	15.3.0
09-2018	SP#81	SP-180715	0543	1	F	Unified Access Control for UE configured for EAB	15.3.0
09-2018	SP#81	SP-180715	0544	2	F	UE configuration of NSSAI and associated mapping	15.3.0
09-2018	SP#81	SP-180715	0545	-	F	Corrections to NEF functionalities description	15.3.0
09-2018	SP#81	SP-180715	0546	2	F	Update of N4 Parameter Descriptions and Tables/ Ethernet PDU Session Type	15.3.0
09-2018	SP#81	SP-180715	0547	1	F	Miscellaneous Corrections to SM specifications (SSC mode, PCFP reference, etc.)	15.3.0
09-2018	SP#81	SP-180715	0548	2	F	Specify AUSF selection by UDM	15.3.0
09-2018	SP#81	SP-180715	0551	-	F	Obsolete reference to Lawful Interception specifications	15.3.0
09-2018	SP#81	SP-180715	0555	2	F	Clearification on UE's configuraiton update	15.3.0
09-2018	SP#81	SP-180715	0558	2	F	Corrections to AF influence (5.6.7) based on CT WG3 LS on AF influence on traffic routing	15.3.0
09-2018	SP#81	SP-180715	0559	2	F	Alignment with CT WG1 on the QoS Flow Description	15.3.0
09-2018	SP#81	SP-180715	0562	-	F	UDM procedures in EPS-5GS interworking without N26	15.3.0
09-2018	SP#81	SP-180715	0563	-	F	Update of NEF service table (7.2.8) for Chargeable party and AFsessionWithQoS	15.3.0
09-2018	SP#81	SP-180715	0564	1	F	Radio Capabilities for DRM in emergency services	15.3.0
09-2018	SP#81	SP-180715	0565	3	F	Selection of S-NSSAIs used in the Requested NSSAI	15.3.0
09-2018	SP#81	SP-180715	0566	3	F	Temporary identifier usage at interworking	15.3.0
09-2018	SP#81	SP-180715	0567	1	F	Temporary identifier coordination	15.3.0
09-2018	SP#81	SP-180715	0569	1	F	Updating radio capabilities from RRC_Inactive	15.3.0
09-2018	SP#81	SP-180715	0573	1	F	SMS support used in different meanings	15.3.0
09-2018	SP#81	SP-180715	0575	-	F	Exposure function reference correction	15.3.0
09-2018	SP#81	SP-180715	0583	3	F	Consistent Description of 5QI	15.3.0
09-2018	SP#81	SP-180715	0584	-	F	Corrections to N4 and UP tunnel protocol descriptions	15.3.0
09-2018	SP#81	SP-180715	0585	1	F	Handling of pending DL NAS signalling (related to LS In S2-187632)	15.3.0
09-2018	SP#81	SP-180715	0586	-	F	Alignment of Slice Selection logic in the AMF and NSSF	15.3.0
09-2018	SP#81	SP-180715	0587	3	F	Missing requirements to trigger Notification Control	15.3.0
09-2018	SP#81	SP-180716	0588	2	F	OAuth2 Authorization Service	15.3.0
09-2018	SP#81	SP-180716	0589	2	F	Clarification of the service area restriction and NSSAIs to EPLMNs	15.3.0
09-2018	SP#81	SP-180716	0591	1	F	23.501: Reference Point and Services correction	15.3.0
09-2018	SP#81	SP-180716	0592	1	F	23.501: UDM Services	15.3.0
09-2018	SP#81	SP-180716	0593	2	F	23.501: Subscription for EPS IWK	15.3.0
09-2018	SP#81	SP-180716	0594	-	F	23.501: AUSF, UDM, UDR Discovery	15.3.0
09-2018	SP#81	SP-180716	0595	2	F	Voice centric UE behaviour in non-allowed area	15.3.0

09-2018	SP#81	SP-180716	0597	5	F	Update to PCF discovery and selection	15.3.0
09-2018	SP#81	SP-180716	0598	3	F	Clarification to IMS emergency procedure	15.3.0
09-2018	SP#81	SP-180716	0604	1	F	Clarification on reporting of PS Data Off status change	15.3.0
09-2018	SP#81	SP-180716	0605	4	F	TAI List provision to RAN by AMF for RRC Inactive UE	15.3.0
09-2018	SP#81	SP-180716	0606	2	F	Clarifications for signalled QoS characteristics	15.3.0
09-2018	SP#81	SP-180716	0608	1	F	IPv6 multi-homed routing rule	15.3.0
09-2018	SP#81	SP-180716	0609	1	F	Clarification on priority of URSP and configuration of association between application and LADN DNN	15.3.0
09-2018	SP#81	SP-180716	0616	2	F	Update N4 principles and parameters	15.3.0
09-2018	SP#81	SP-180716	0617	-	F	Clarification on NF profile parameters	15.3.0
09-2018	SP#81	SP-180716	0618	-	F	Update to service area restriction	15.3.0
09-2018	SP#81	SP-180791	0611	3	F	Clarification on the AMF store the DNN and PGW-C+SMF to UDM/HSS without N26.	15.3.0
2018-12	SP#82	SP-181084	0576	6	F	CHF discovery and selection	15.4.0
2018-12	SP#82	SP-181085	0590	2	F	Clarification to the slice based congestion control handling at NG-RAN	15.4.0
2018-12	SP#82	SP-181085	0607	11	F	Clarifications for 5QI priority level	15.4.0
2018-12	SP#82	SP-181090	0621	2	F	Using preconfigured 5QI for QoS Flow associated with the default QoS rule	15.4.0
2018-12	SP#82	SP-181090	0622	3	F	Update of Default Configured NSSAI	15.4.0
2018-12	SP#82	SP-181086	0625	2	F	Clarifying the boundaries of an NF instance	15.4.0
2018-12	SP#82	SP-181086	0626	-	F	Correcting discovery and selection	15.4.0
2018-12	SP#82	SP-181089	0628	3	F	Reporting PS Data Off status change when SM back off timer is running	15.4.0
2018-12	SP#82	SP-181086	0629	1	F	Correction of the indication of UE 5GSM capabilities after intersystem change	15.4.0
2018-12	SP#82	SP-181090	0630	1	F	UE unable to use N3IWF identifier configuration in stand-alone N3IWF selection	15.4.0
2018-12	SP#82	SP-181089	0633	2	F	Removal of Editor's Note re mandatoriness of RRC_Inactive	15.4.0
2018-12	SP#82	SP-181084	0634	3	F	Avoiding mandatory MME impacts from 3-byte TAC	15.4.0
2018-12	SP#82	SP-181084	0637	1	F	Alignment of NF Profile with adding priority parameter	15.4.0
2018-12	SP#82	SP-181084	0638	2	F	Clarification on RQ Timer	15.4.0
2018-12	SP#82	SP-181088	0639	2	F	Interactions with PCF - Updates to reference architecure for interworking	15.4.0
2018-12	SP#82	SP-181089	0641	1	F	Registration Area and Service Restriction Area in relation to multiple PLMNs	15.4.0
2018-12	SP#82	SP-181086	0645	1	F	Correcting the interaction needed for the NSSF service	15.4.0
2018-12	SP#82	SP-181086	0648	-	F	Connections on Default Configured NSSAI	15.4.0
2018-12	SP#82	SP-181086	0651	1	F	Correction and clarification for CM-CONNECTED with RRC Inactive state	15.4.0
2018-12	SP#82	SP-181089	0653	2	F	SUPI definition and NAI format	15.4.0
2018-12	SP#82	SP-181084	0655	1	F	Addition of abbreviations	15.4.0
2018-12	SP#82	SP-181088	0656	8	F	Network controlled NSSAI for SR-related Access Stratum connection establishment	15.4.0
2018-12	SP#82	SP-181195	0660	8	F	Unified Access Control clarification and triggers	15.4.0
2018-12	SP#82	SP-181087	0661	3	B	Data Volume Reporting for Option 4/7	15.4.0
2018-12	SP#82	SP-181086	0662	4	F	Configuration Transfer Procedure	15.4.0
2018-12	SP#82	SP-181084	0666	3	F	Avoiding overloading the target of AMF Load Re-Balancing	15.4.0
2018-12	SP#82	SP-181090	0667	1	F	UE storage of NSSAI and associated mapping	15.4.0
2018-12	SP#82	SP-181085	0668	1	F	Clarification of PS Voice Support for 3GPP and non-3GPP	15.4.0
2018-12	SP#82	SP-181089	0669	1	F	Secondary authentication update	15.4.0
2018-12	SP#82	SP-181087	0671	1	F	Emergency registration in a normally camped cell	15.4.0
2018-12	SP#82	SP-181088	0672	1	F	Priority indication over SBA interfaces via Message Priority header	15.4.0
2018-12	SP#82	SP-181088	0675	3	F	MME/AMF registration in HSS+UDM	15.4.0
2018-12	SP#82	SP-181086	0676	1	F	Completion of 5QI characteristics table	15.4.0
2018-12	SP#82	SP-181086	0677	-	F	Consistent usage of terminology in QoS notification control description	15.4.0
2018-12	SP#82	SP-181084	0679	3	F	Alignment for always-on PDU sessions	15.4.0
2018-12	SP#82	SP-181089	0680	1	C	PS Data Off supporting non-IP data packet	15.4.0
2018-12	SP#82	SP-181089	0682	3	F	Clarification on the PDU Session handover procedure with the User Plane Security Enforcement	15.4.0
2018-12	SP#82	SP-181089	0683	1	F	Clean up congestion control	15.4.0
2018-12	SP#82	SP-181089	0685	3	F	Correction on SSCMSP	15.4.0
2018-12	SP#82	SP-181089	0686	4	F	Clarification on the AMF store the DNN and PGW-C+SMF to UDM+HSS	15.4.0
2018-12	SP#82	SP-181085	0687	1	F	Clarification on NPLI for EPS Fallback	15.4.0
2018-12	SP#82	SP-181087	0688	1	F	Correction on UE inclusion of UE's usage setting	15.4.0
2018-12	SP#82	SP-181090	0690	3	F	UE radio capability for paging information with NR and eLTE connected to the CN	15.4.0
2018-12	SP#82	SP-181087	0691	2	F	Correction to traffic steering control	15.4.0
2018-12	SP#82	SP-181090	0692	-	F	Using TCP for reliable NAS transport between UE and N3IWF	15.4.0
2018-12	SP#82	SP-181084	0693	1	C	5GS Support for MCS Subscription	15.4.0

2018-12	SP#82	SP-181091	0695	1	F	UE sending UE Integrity Protection Data Rate capability over any access	15.4.0
2018-12	SP#82	SP-181087	0696	1	F	Correction on Subscribed 5QI	15.4.0
2018-12	SP#82	SP-181089	0699	-	F	Selective deactivation for always-on PDU sessions	15.4.0
2018-12	SP#82	SP-181091	0701	1	F	Use of emergency DNN when Emergency Registered	15.4.0
2018-12	SP#82	SP-181090	0703	3	F	Requirements on 5G-TMSI randomness	15.4.0
2018-12	SP#82	SP-181087	0707	1	F	Emergency registration over two accesses	15.4.0
2018-12	SP#82	SP-181090	0708	1	F	Registration procedure with different Registration types	15.4.0
2018-12	SP#82	SP-181088	0709	2	F	EPS to 5GS with network slices	15.4.0
2018-12	SP#82	SP-181084	0710	2	F	AUSF and UDM selection	15.4.0
2018-12	SP#82	SP-181089	0712	2	F	Providing a threshold to UPF while waiting for quota	15.4.0
2018-12	SP#82	SP-181088	0713	1	F	Corrections to usage of IP index	15.4.0
2018-12	SP#82	SP-181085	0716	2	F	Clarification on OVERLOAD behaviour for the EUTRA connected to 5GC	15.4.0
2018-12	SP#82	SP-181085	0719	2	F	Clarification on Registration with AMF re-allocation	15.4.0
2018-12	SP#82	SP-181089	0720	1	F	PDN Disconnection handling	15.4.0
2018-12	SP#82	SP-181084	0721	3	F	Always on Setting for the EBI allocated PDU Session	15.4.0
2018-12	SP#82	SP-181085	0722	2	F	Clarification on packet filter handling	15.4.0
2018-12	SP#82	SP-181086	0723	4	F	Clarify for PDB of dynamically assigned 5QI	15.4.0
2018-12	SP#82	SP-181091	0724	2	F	Update the UCU procedure with operator-defined access category definitions	15.4.0
2018-12	SP#82	SP-181087	0725	-	F	Correction of VLAN ID	15.4.0
2018-12	SP#82	SP-181085	0726	1	F	Clarification on DN authorization data between PCF and SMF	15.4.0
2018-12	SP#82	SP-181084	0730	2	F	Addition of URRP-AMF definition	15.4.0
2019-03	SP#83	SP-190154	0700	3	F	Use of S-NSSAI at interworking from EPS to 5GS	15.5.0
2019-03	SP#83	SP-190154	0733	2	F	Slice interworking HR mode update	15.5.0
2019-03	SP#83	SP-190154	0741	1	F	UDR selection	15.5.0
2019-03	SP#83	SP-190154	0742	2	F	Fixing text related to discovery and selection	15.5.0
2019-03	SP#83	SP-190154	0743	1	F	Change of the term confidence level	15.5.0
2019-03	SP#83	SP-190154	0756	2	F	Correction to NSSAI logic	15.5.0
2019-03	SP#83	SP-190154	0758	2	F	UL Session-AMBR enforcement in UPF	15.5.0
2019-03	SP#83	SP-190154	0759	1	F	Alignment with stage 3 for EPS interworking indications	15.5.0
2019-03	SP#83	SP-190154	0762	2	F	Clarification of user plane security enforcement between NG-RAN and SMF in Dual Connectivity scenario	15.5.0
2019-03	SP#83	SP-190154	0767	2	F	QoS Notification Control during handover	15.5.0
2019-03	SP#83	SP-190154	0773	1	F	Correction to traffic steering control	15.5.0
2019-03	SP#83	SP-190154	0774	3	F	Configurable time for subsequent notification that the GFBR cannot be fulfilled	15.5.0
2019-03	SP#83	SP-190154	0775	1	F	Clarification for default values	15.5.0
2019-03	SP#83	SP-190154	0784	4	F	5GC emergency calls over non-3GPP	15.5.0
2019-03	SP#83	SP-190154	0786	1	F	Adding UE Local Configuration as an additional option to the URSP	15.5.0
2019-03	SP#83	SP-190154	0789	-	F	Update of network slicing text on NSSAI inclusion in RRC	15.5.0
2019-03	SP#83	SP-190154	0791	3	C	Supporting early trace in AUSF	15.5.0
2019-03	SP#83	SP-190154	0792	1	F	IMS voice over PS Session Supported Indication in roaming cases.	15.5.0
2019-03	SP#83	SP-190154	0793	2	F	Introduce Charging Function in overall architecture	15.5.0
2019-03	SP#83	SP-190155	0797	2	F	Update of configured NSSAI handling	15.5.0
2019-03	SP#83	SP-190155	0806	3	F	Corrections to AMF overlad control procedure	15.5.0
2019-03	SP#83	SP-190155	0808	-	F	TS 23.501 Update to Network Slice availability	15.5.0
2019-03	SP#83	SP-190155	0818	-	F	No services defined for Ngmlc	15.5.0
2019-03	SP#83	SP-190155	0824	6	F	Clarification on DN authorization data	15.5.0
2019-03	SP#83	SP-190155	0833	-	F	Clarification on Establishing a PDU Session in a Network Slice	15.5.0
2019-03	SP#83	SP-190155	0834	8	F	Clarification on NAS level congestion control	15.5.0
2019-03	SP#83	SP-190155	0853	6	F	PS Data Off status update when congestion control is applied in AMF	15.5.0
2019-03	SP#83	SP-190155	0857	1	F	Correction to Mobility Restrictions (for non-3GPP access)	15.5.0
2019-03	SP#83	SP-190155	0860	3	F	Clarification on the UE behaviours under NAS level congestion control	15.5.0
2019-03	SP#83	SP-190155	0875	-	F	Permanent identifier with IMEISV format	15.5.0
2019-03	SP#83	SP-190155	0876	2	F	Removing a superfluous NOTE about the need for ultra-low latency QCI/5Qis	15.5.0
2019-03	SP#83	SP-190155	0877	7	F	Allowed Area and Non-Allowed Area encoding	15.5.0
2019-03	SP#83	SP-190155	0901	2	F	Alignment of Emergency Registered definition with Stage 3	15.5.0
2019-03	SP#83	SP-190155	0904	-	F	Addition of PCF services Npcf_UEPolicyControl and Npcf_EventExposure	15.5.0
2019-03	SP#83	SP-190155	0910	3	F	Clarification on ARP Proxy	15.5.0
2019-03	SP#83	SP-190155	0913	2	F	PS Data Off status update when UE in non-allowed area or out of LADN area	15.5.0
2019-03	SP#83	SP-190155	0915	2	F	Non-roaming reference architecture correction	15.5.0
2019-03	SP#83	SP-190155	0922	2	F	TS 23.501: correction for enforcement of user plane integrity protection	15.5.0

2019-03	SP#83	SP-190156	0932	2	F	Clarification on the PDU Session parameter	15.5.0
2019-03	SP#83	SP-190156	0942	2	F	Transport Level Packet Marking	15.5.0
2019-03	SP#83	SP-190156	0943	2	F	Support of baseline Frame Routing feature	15.5.0
2019-03	SP#83	SP-190156	0945	1	F	Disabling E-UTRA connected to EPC radio capability	15.5.0
2019-03	SP#83	SP-190156	0949	2	F	Correction of slicing terminology	15.5.0
2019-03	SP#83	SP-190156	0958	1	F	Adding a new 5G-GUTI allocation condition	15.5.0
2019-03	SP#83	SP-190156	0968	2	F	Clarify on Network Slice availability change	15.5.0
2019-03	SP#83	SP-190156	0969	2	F	Correction the terms on Secondary authentication/authorization of the PDU Session Establishment	15.5.0
2019-03	SP#83	SP-190156	0975	1	F	Clarificaiton on Core Network type Restriction	15.5.0
2019-03	SP#83	SP-190156	0976	3	F	Clarification on AMF planned removal	15.5.0
2019-03	SP#83	SP-190156	0979	1	F	Correction of UE 5GSM Core Network Capability	15.5.0
2019-03	SP#83	SP-190156	0982	2	F	Clarification on QoS Notification control	15.5.0
2019-03	SP#83	SP-190156	0988	0	F	Correction on reference	15.5.0
2019-03	SP#83	SP-190156	0992	3	F	Slice interworking HR mode update	15.5.0
2019-03	SP#83	SP-190156	0996	2	F	Clarification on PCF selection	15.5.0
2019-03	SP#83	SP-190156	1006	-	F	Corrections on routing rule	15.5.0
2019-03	SP#83	SP-190156	1012	2	F	Clarification on GTP-u protocol	15.5.0
2019-03	SP#83	SP-190175	0704	4	C	New 5QIs for Enhanced Framework for Uplink Streaming	**16.0.0**
2019-03	SP#83	SP-190169	0734	8	B	TS 23.501: Introducing Non-public network	**16.0.0**
2019-03	SP#83	SP-190169	0747	12	B	Support for 5G LAN	**16.0.0**
2019-03	SP#83	SP-190194	0757	8	B	Introducing support for Non-Public Networks	**16.0.0**
2019-03	SP#83	SP-190169	0903	2	B	Introduction of 5G LAN-type service	**16.0.0**
2019-03	SP#83	SP-190169	1007	2	B	Introducing support TSC Deterministic QoS	**16.0.0**
2019-03	SP#83	SP-190169	1008	2	B	Introducing support Hold and Forward Buffers for TSC Deterministic QoS	**16.0.0**
2019-03	SP#83	SP-190169	1002	3	B	5GS Logical TSN bridge management	**16.0.0**
2019-03	SP#83	SP-190165	0748	3	B	CIoT High Level Description in 23.501	**16.0.0**
2019-03	SP#83	SP-190165	0751	3	B	High Latency Overall Description	**16.0.0**
2019-03	SP#83	SP-190165	0752	4	B	Introducing Rate Control for 5G CIoT	**16.0.0**
2019-03	SP#83	SP-190165	0768	6	B	Introduction of eDRX in 5GS	**16.0.0**
2019-03	SP#83	SP-190165	0819	1	B	CIoT Monitoring Events	**16.0.0**
2019-03	SP#83	SP-190165	0820	4	B	Restriction of use of Enhanced Coverage in 5GC	**16.0.0**
2019-03	SP#83	SP-190165	0825	2	B	Introduction to Reliable Data Service	**16.0.0**
2019-03	SP#83	SP-190165	0889	7	B	Introduction of data transfer in Control Plane CIoT 5GS Optimisation	**16.0.0**
2019-03	SP#83	SP-190165	0890	6	B	Introduction of NEF based infrequent small data transfer via NAS	**16.0.0**
2019-03	SP#83	SP-190165	0893	7	B	Introduction of Power Saving Functions for CIoT	**16.0.0**
2019-03	SP#83	SP-190165	0894	5	B	CIoT Introduction of Overload Control	**16.0.0**
2019-03	SP#83	SP-190165	0895	2	B	Introduction of Inter-RAT mobility support to and from NB-IoT	**16.0.0**
2019-03	SP#83	SP-190165	0896	2	B	CIoT Introduction of CN Selection and Steering	**16.0.0**
2019-03	SP#83	SP-190165	1014	2	B	Introduction of Service Gap Control	**16.0.0**
2019-03	SP#83	SP-190173	0735	11	B	Introduction of ATSSS Support	**16.0.0**
2019-03	SP#83	SP-190173	0740	7	B	Support of Steering Functions for ATSSS	**16.0.0**
2019-03	SP#83	SP-190173	0770	4	B	QoS for Multi-Access PDU Session	**16.0.0**
2019-03	SP#83	SP-190173	0921	3	B	Access Network Performance Measurements	**16.0.0**
2019-03	SP#83	SP-190171	0810	2	B	New clause for URLLC supporting	**16.0.0**
2019-03	SP#83	SP-190171	0753	8	B	General description of solution 1 in 23.725 for user plane redundancy	**16.0.0**
2019-03	SP#83	SP-190171	0811	6	B	Add description of solution 4 in 23.725 to 23.501	**16.0.0**
2019-03	SP#83	SP-190171	0872	3	B	Description of solution 7 in 23.725 as replication framework	**16.0.0**
2019-03	SP#83	SP-190164	0732	2	B	ETSUN - Architecture conclusion	**16.0.0**
2019-03	SP#83	SP-190164	0848	5	B	UL CL/BP controlled by I-SMF	**16.0.0**
2019-03	SP#83	SP-190175	0704	4	C	New 5QIs for Enhanced Framework for Uplink Streaming	**16.0.0**
2019-03	SP#83	SP-190171	0755	2	B	Description of solution 11 in 23.725 for Ethernet anchor relocation	**16.0.0**
2019-03	SP#83	SP-190169	0734	8	B	Introducing Non-public network	**16.0.0**
2019-03	SP#83	SP-190215	0736	10	B	Introduction of indirect communication between NF services, and implicit discovery	**16.0.0**
2019-03	SP#83	SP-190167	0744	4	B	SUPI and SUCI for wireline access	**16.0.0**
2019-03	SP#83	SP-190167	0745	6	B	Mobility restrictions for wireline access	**16.0.0**
2019-03	SP#83	SP-190167	0746	2	B	IP addressing enhancements	**16.0.0**
2019-03	SP#83	SP-190169	0747	12	B	Support for 5G LAN	**16.0.0**
2019-03	SP#83	SP-190171	0754	2	B	Description of solution 2 in 23.725 for redundancy as an informational annex	**16.0.0**
2019-03	SP#83	SP-190173	0761	1	B	ATSSS-SMF and UPF selection	**16.0.0**
2019-03	SP#83	SP-190165	0776	3	B	CIoT Introduction of extended DRX in CM-CONNECTED with RRC Inactive state	**16.0.0**
2019-03	SP#83	SP-190167	0781	2	B	Support of Trusted non-3GPP access	**16.0.0**
2019-03	SP#83	SP-190167	0783	2	B	Trusted non-3GPP Access Network Selection	**16.0.0**
2019-03	SP#83	SP-190173	0785	5	B	Updating 5.8.2.11 for N4 Rules to support ATSSS	**16.0.0**
2019-03	SP#83	SP-190174	0799	10	B	eSBA communication schemas related to general discovery and selection	**16.0.0**

2019-03	SP#83	SP-190174	0800	3	B	eSBA communication schemas related to UDM and UDR discovery and selection	**16.0.0**
2019-03	SP#83	SP-190172	0940	3	B	Use of analytics for SMF selection	**16.0.0**
2019-03	SP#83	SP-190174	0801	7	B	eSBA communication schemas related to SMF discovery and selection	**16.0.0**
2019-03	SP#83	SP-190174	0802	3	B	eSBA communication schemas related to PCF discovery and selection	**16.0.0**
2019-03	SP#83	SP-190174	0803	5	B	eSBA communication schemas related to AUSF discovery and selection	**16.0.0**
2019-03	SP#83	SP-190174	0804	4	B	eSBA communication schemas related to AMF discovery and selection	**16.0.0**
2019-03	SP#83	SP-190165	0826	2	B	Introduction of the MSISDN-less MO SMS Service	**16.0.0**
2019-03	SP#83	SP-190165	0828	1	B	Introduction of the SCEF+NEF	**16.0.0**
2019-03	SP#83	SP-190172	0831	6	B	CR for TS 23.501 based on conclusion of eNA TR 23.791	**16.0.0**
2019-03	SP#83	SP-190172	0837	3	B	Use of NWDAF analytics for decision of MICO mode parameters	**16.0.0**
2019-03	SP#83	SP-190169	0841	2	B	FQDN format of N3IWF in a standalone non-public network	**16.0.0**
2019-03	SP#83	SP-190168	0843	2	F	Update to LCS related definitions	**16.0.0**
2019-03	SP#83	SP-190238	0844	8	B	Network reliability support with Sets	**16.0.0**
2019-03	SP#83	SP-190199	0850	1	B	Enhancement on slice interworking--501	**16.0.0**
2019-03	SP#83	SP-190162	0859	2	B	Adding 5G SRVCC description to 23.501	**16.0.0**
2019-03	SP#83	SP-190167	0862	7	B	UPF Selection influenced by the indication of the identity/identities of 5G AN N3 User Plane capability	**16.0.0**
2019-03	SP#83	SP-190167	0863	8	B	Architecture and reference points for Wireline AN	**16.0.0**
2019-03	SP#83	SP-190167	0866	8	B	Clarification of RM and CM for 5G-RG	**16.0.0**
2019-03	SP#83	SP-190169	0870	3	B	TSC definitions	**16.0.0**
2019-03	SP#83	SP-190169	0871	4	B	TSC Architecture	**16.0.0**
2019-03	SP#83	SP-190174	0873	8	B	eSBA communication schema co-existence	**16.0.0**
2019-03	SP#83	SP-190170	0878	2	B	NEF service for service specific parameter provisioning	**16.0.0**
2019-03	SP#83	SP-190165	0886	5	B	Introduction for solution 14 to key issue 9	**16.0.0**
2019-03	SP#83	SP-190171	0897	7	B	Sol#6 specific updates to 5.6.4.2	**16.0.0**
2019-03	SP#83	SP-190165	0898	6	B	External parameters provisioning to the 5GS	**16.0.0**
2019-03	SP#83	SP-190172	0899	1	B	Use of analytics for user plane function selection	**16.0.0**
2019-03	SP#83	SP-190172	0900	1	B	Use of analytics for UE mobility procedures	**16.0.0**
2019-03	SP#83	SP-190169	0909	3	B	Control of traffic forwarding in 5G-LAN	**16.0.0**
2019-03	SP#83	SP-190165	0916	1	B	User Plane Forwarding with Control Plane CIoT 5GS Optimisation	**16.0.0**
2019-03	SP#83	SP-190174	0926	2	B	Update the support of virtualized deployment with SCP distribution and the NF/NF service instance Set	**16.0.0**
2019-03	SP#83	SP-190174	0927	1	C	Update of NRF functionalities	**16.0.0**
2019-03	SP#83	SP-190164	0931	2	B	UE IP address Allocation by UPF: N4 impacts	**16.0.0**
2019-03	SP#83	SP-190164	0933	1	B	ETSUN - Conclusion alignment	**16.0.0**
2019-03	SP#83	SP-190167	0934	2	B	Support of full Frame Routing feature	**16.0.0**
2019-03	SP#83	SP-190174	0941	4	B	Location information	**16.0.0**
2019-03	SP#83	SP-190164	0954	2	B	Addition of UE IP address Allocation by UPF	**16.0.0**
2019-03	SP#83	SP-190167	0961	1	B	Protocol stack for W-5GAN support	**16.0.0**
2019-03	SP#83	SP-190167	0962	3	C	Session Management of 5G-RG/FN-RG connection to 5GC in the Wireline ANs	**16.0.0**
2019-03	SP#83	SP-190172	0964	2	B	NEF service for NWDAF analytics	**16.0.0**
2019-03	SP#83	SP-190171	0972	3	B	Add description of solution 13 in 23.725 to TS 23.501	**16.0.0**
2019-03	SP#83	SP-190167	0981	2	B	Extension of the QoS model for wireline access	**16.0.0**
2019-03	SP#83	SP-190172	0983	2	B	Update of TS 23.501 for Rel.16 BDT Notification	**16.0.0**
2019-03	SP#83	SP-190168	0984	2	F	Update the description and the reference of LMF service	**16.0.0**
2019-03	SP#83	SP-190172	0987	3	B	CR for TS 23.501 Clarifications NWDAF Discovery and Selection	**16.0.0**
2019-03	SP#83	SP-190171	0989	2	B	Introduction of E2E PDB Division	**16.0.0**
2019-03	SP#83	SP-190169	1003	2	B	QoS parameters mapping between TSN characters and 5G QoS	**16.0.0**
2019-03	SP#83	SP-190174	1010	3	B	Introducing NF Set and NF Service Set	**16.0.0**
2019-03	SP#83	SP-190175	1022	2	B	Introduction of Dedicated Bearer for Ethernet support in EPC	**16.0.0**
2019-04	-	-	-	-	-	MCC correction of clause 5.29.3 (to 5.30.3) and position of clause 5.31.7.2. Editorial style and formatting corrections	**16.0.1**
2019-04	-	-	-	-	-	MCC correction swapping clause 5.28 to 5.29 and clause 5.29 to 5.28 for readability purposes	**16.0.2**
2019-06	SP#84	SP-190407	0892	4	B	Introduction of inter-UE QoS differentiation for NB-IoT using NB-IoT UE Priority	16.1.0
2019-06	SP#84	SP-190407	1019	3	B	Support of EPC interworking for CIoT Monitoring Events	16.1.0
2019-06	SP#84	SP-190428	1028	1	D	Proper naming of the reference point between two UPFs for direct routing	16.1.0
2019-06	SP#84	SP-190416	1033	2	B	Clarification on MA PDU session	16.1.0
2019-06	SP#84	SP-190416	1034	5	B	Determination of access availability	16.1.0
2019-06	SP#84	SP-190419	1035	4	B	NRF based P-CSCF discovery	16.1.0
2019-06	SP#84	SP-190425	1037	3	B	Introduction of RACS: UCMF services	16.1.0
2019-06	SP#84	SP-190514	1042	6	A	Correcting factors to consider for PCF selection	16.1.0
2019-06	SP#84	SP-190399	1044	2	A	QoS Notification Control	16.1.0
2019-06	SP#84	SP-190407	1047	3	F	MICO mode and Periodic Registration Timer Control	16.1.0

2019-06	SP#84	SP-190422	1050	4	B	Transfer of N4 information for local traffic switching from SMF to I-SMF	16.1.0
2019-06	SP#84	SP-190428	1015	2	B	Proposed update to 5G LAN terminology	16.1.0
2019-06	SP#84	SP-190428	1052	8	B	Further detailing of 5G LAN group management	16.1.0
2019-06	SP#84	SP-190413	1055	2	F	Correction of SMF selecting UPF for a particular PDU Session supporting EPS IWK	16.1.0
2019-06	SP#84	SP-190410	1056	2	F	Network Slicing and delegated discovery	16.1.0
2019-06	SP#84	SP-190407	1059	1	F	UE specific DRX parameter use for NB-IOT	16.1.0
2019-06	SP#84	SP-190399	1062	1	A	Congestion control exception for reporting 5GSM Core Network Capability and Always-on PDU Session Requested indication	16.1.0
2019-06	SP#84	SP-190399	1064	1	A	Data volume reporting granularity	16.1.0
2019-06	SP#84	SP-190399	1066	-	A	Removal of restriction of using UE requested PDU modification request for Emergency PDU	16.1.0
2019-06	SP#84	SP-190427	1067	6	F	Return to NR from EPS/RAT fallback	16.1.0
2019-06	SP#84	SP-190427	1068	2	F	Clarification on PRA	16.1.0
2019-06	SP#84	SP-190412	1070	3	F	Clarification to support associating URLLC traffic to redundant PDU sessions	16.1.0
2019-06	SP#84	SP-190425	1071	5	B	Introduction of Radio Capabilities Signalling Optimisation feature	16.1.0
2019-06	SP#84	SP-190428	1073	4	B	Support of emergency services in public network integrated NPNs	16.1.0
2019-06	SP#84	SP-190407	1075	3	F	Clarification on MICO and eDRX during CN node changes	16.1.0
2019-06	SP#84	SP-190416	1078	1	F	Correction and clarifications for QoS Flow in MA PDU Session	16.1.0
2019-06	SP#84	SP-190416	1079	2	F	Correction related to ATSSS Rule	16.1.0
2019-06	SP#84	SP-190416	1080	2	F	Clear ENs about Measurement Assistance Information for ATSSS	16.1.0
2019-06	SP#84	SP-190428	1083	6	B	Clarification of Inserting and Removing VLAN tags for 5GLAN	16.1.0
2019-06	SP#84	SP-190410	1091	2	F	Update of the NF/NF service discovery result	16.1.0
2019-06	SP#84	SP-190410	1092	3	C	Update of NRF function and services	16.1.0
2019-06	SP#84	SP-190410	1093	2	F	Update of network reliability support	16.1.0
2019-06	SP#84	SP-190420	1094	1	C	Back-off timers handling for scheduled communication	16.1.0
2019-06	SP#84	SP-190428	1095	5	C	Addressing Editor's notes on TSN	16.1.0
2019-06	SP#84	SP-190428	1098	1	F	Access Control for PLMN Integrated NPN	16.1.0
2019-06	SP#84	SP-190407	1101	9	B	Establishing UP connection during CP Data Transfer	16.1.0
2019-06	SP#84	SP-190416	1103	1	F	Corrections for SMF, UPF and PCF selection for an MA PDU session	16.1.0
2019-06	SP#84	SP-190416	1104	1	F	Corrections for N4 rules for ATSSS	16.1.0
2019-06	SP#84	SP-190407	1109	2	B	Service Gap corrections	16.1.0
2019-06	SP#84	SP-190399	1116	2	F	Local cache information for ARP proxy	16.1.0
2019-06	SP#84	SP-190416	1118	1	F	UE Requested PDU Session Establishment with Network Modification to MA PDU Session	16.1.0
2019-06	SP#84	SP-190428	1119	2	C	Granularity of TSN bridge	16.1.0
2019-06	SP#84	SP-190412	1120	1	C	Filtering own address for Ethernet PDU Sessions	16.1.0
2019-06	SP#84	SP-190428	1123	3	B	TSN QoS mapping and 802.1Qbv parameters	16.1.0
2019-06	SP#84	SP-190415	1128	3	B	Access to 5GC from UEs not supporting NAS over non-3GPP access	16.1.0
2019-06	SP#84	SP-190399	1130	1	A	Validity of LADN information and LADN discovery/storage in the UE per-PLMN	16.1.0
2019-06	SP#84	SP-190399	1131	3	A	Conclusions on applicability of Allowed NSSAI to E-PLMNs	16.1.0
2019-06	SP#84	SP-190399	1132	1	A	Correction to the provisioning of the UE Integrity Protection Data Rate capability	16.1.0
2019-06	SP#84	SP-190419	1134	3	B	Allowing IMS to use N5 interface to interact with PCF	16.1.0
2019-06	SP#84	SP-190428	1135	3	F	Correction regarding legacy UE and non-NPN UE	16.1.0
2019-06	SP#84	SP-190427	1139	3	F	AMF selection during inter PLMN mobility	16.1.0
2019-06	SP#84	SP-190412	1142	6	C	Update description for E2E PDB division	16.1.0
2019-06	SP#84	SP-190412	1144	2	C	Explicit indication of AF response to be expected for runtime coordination with AF	16.1.0
2019-06	SP#84	SP-190407	1149	9	B	Roaming support for service exposure	16.1.0
2019-06	SP#84	SP-190399	1152	1	A	Corrections for the activation of usage reporting in the UPF	16.1.0
2019-06	SP#84	SP-190399	1159	2	A	Clarification on NAS level congestion control	16.1.0
2019-06	SP#84	SP-190399	1161	3	A	Correction of UE 5GSM Core Network Capability	16.1.0
2019-06	SP#84	SP-190423	1162	1	B	Introduce a new standardized SST value dedicated for V2X services	16.1.0
2019-06	SP#84	SP-190412	1163	1	F	Clarification on the CN PDB configured in each NG-RAN node	16.1.0
2019-06	SP#84	SP-190416	1164	2	B	Clarification on GBR QoS Flow establishment	16.1.0
2019-06	SP#84	SP-190416	1168	5	C	RTT measurements with TCP	16.1.0
2019-06	SP#84	SP-190416	1169	2	F	MA PDU QoS Aspects On Link-Specific Multipath and MPTCP Proxy Addresses	16.1.0
2019-06	SP#84	SP-190422	1170	1	F	ETSUN Architecture Update	16.1.0
2019-06	SP#84	SP-190410	1171	4	F	SCP Function Update	16.1.0
2019-06	SP#84	SP-190412	1173	2	F	Redundant PDU session handling	16.1.0
2019-06	SP#84	SP-190421	1174	6	B	Introduction of Slice-Specific Authentication and Authorisation	16.1.0
2019-06	SP#84	SP-190399	1176	1	A	Association between the GUAMI and AMF instance	16.1.0
2019-06	SP#84	SP-190422	1177	5	B	LADN handling in ETSUN scenario	16.1.0
2019-06	SP#84	SP-190422	1179	7	B	Traffic offload by UPF controlled by the I-SMF	16.1.0

2019-06	SP#84	SP-190422	1180	1	B	UE IP address Allocation by AAA/DHCP	16.1.0
2019-06	SP#84	SP-190428	1183	3	C	SNPN deployment scenarios	16.1.0
2019-06	SP#84	SP-190407	1186	8	B	Introducing 5GS UP optimization	16.1.0
2019-06	SP#84	SP-190420	1187	1	B	Adding NF load information inside NFprofile	16.1.0
2019-06	SP#84	SP-190428	1190	2	C	Resolving editor's note on eSBA	16.1.0
2019-06	SP#84	SP-190416	1191	3	F	ATSSS support for Unstructured Data	16.1.0
2019-06	SP#84	SP-190428	1194	3	F	Removing the EN on the DNN and 5G LAN group mapping	16.1.0
2019-06	SP#84	SP-190428	1198	8	C	Resolving the EN on traffic pattern to the TT	16.1.0
2019-06	SP#84	SP-190428	1199	3	F	Clarification on the CAG ID and slicing	16.1.0
2019-06	SP#84	SP-190420	1201	2	B	CR for adding Naf_EventExposure services	16.1.0
2019-06	SP#84	SP-190428	1202	2	F	Clarification on PDU Session management for 5G-LAN multicast	16.1.0
2019-06	SP#84	SP-190409	1205	-	B	Add new Reference points	16.1.0
2019-06	SP#84	SP-190428	1207	3	F	5G-LAN Service continuity	16.1.0
2019-06	SP#84	SP-190428	1212	1	B	Update to Support TSAI for TSC Deterministic QoS	16.1.0
2019-06	SP#84	SP-190428	1214	10	B	Introducing support for UE and UPF Residence Time for TSC Deterministic QoS	16.1.0
2019-06	SP#84	SP-190412	1217	4	C	5G URLLC: Optimizing Redundancy	16.1.0
2019-06	SP#84	SP-190428	1218	2	F	Standalone NPN - NID Management	16.1.0
2019-06	SP#84	SP-190428	1219	1	F	Standalone NPN - EPS Interworking support	16.1.0
2019-06	SP#84	SP-190410	1222	12	B	NF Set and NF Service Set - Open items resolution	16.1.0
2019-06	SP#84	SP-190413	1226	-	F	AMF Failure - Other CP NF Behaviour	16.1.0
2019-06	SP#84	SP-190399	1228	1	A	Correction on home-routed roaming architecture for EPC interworking	16.1.0
2019-06	SP#84	SP-190428	1230	4	C	Dedicated SMF selection for a 5G LAN group	16.1.0
2019-06	SP#84	SP-190415	1233	4	F	Requirements on the Ta interface	16.1.0
2019-06	SP#84	SP-190399	1235	2	A	Configuration transfer between NG-RAN and eNodeB	16.1.0
2019-06	SP#84	SP-190399	1237	1	A	Cleanup of NAS Congestion Control	16.1.0
2019-06	SP#84	SP-190415	1239	4	B	Removal of roaming support from Rel-16 for W-5GAN	16.1.0
2019-06	SP#84	SP-190407	1243	-	B	Update to NEF description by adding NIDD support	16.1.0
2019-06	SP#84	SP-190399	1249	2	A	Correction of SM congestion control override	16.1.0
2019-06	SP#84	SP-190407	1250	2	B	Corrections to MICO mode with Active Time	16.1.0
2019-06	SP#84	SP-190407	1251	1	B	Subscription Information Influence on PDU Session Rate Control	16.1.0
2019-06	SP#84	SP-190407	1252	2	B	Handling of Stored Small Data Rate Control Status at Subsequent PDU Session Establishment	16.1.0
2019-06	SP#84	SP-190407	1256	4	F	Corrections to CN assisted RAN parameters tuning	16.1.0
2019-06	SP#84	SP-190413	1257	3	F	Corrections to Network Slice Registration	16.1.0
2019-06	SP#84	SP-190420	1258	2	B	CR for TS 23.501 Clarifications NWDAF Discovery and Selection	16.1.0
2019-06	SP#84	SP-190407	1262	1	F	RRC Inactive information for eDRX	16.1.0
2019-06	SP#84	SP-190427	1263	2	F	AMF utilizes NRF to discover NSSF	16.1.0
2019-06	SP#84	SP-190428	1264	3	F	QoS differentiation for access to SNPN (PLMN) services via PLMN (SNPN)	16.1.0
2019-06	SP#84	SP-190422	1265	-	D	Fixing clause number reference	16.1.0
2019-06	SP#84	SP-190427	1266	2	F	Correction of description of the IMS voice over PS Session Supported Indication	16.1.0
2019-06	SP#84	SP-190410	1271	13	D	SCP: Service-mesh-based deployment options	16.1.0
2019-06	SP#84	SP-190427	1274	2	F	Clarification on the UE operates in SR mode in case the NW does not support IWK	16.1.0
2019-06	SP#84	SP-190399	1275	-	A	Removing unnecessary PDU release during inter-system handover	16.1.0
2019-06	SP#84	SP-190399	1277	1	A	Definition of LPP	16.1.0
2019-06	SP#84	SP-190399	1278	2	A	UE's usage setting indicating UE capability of supporting voice over E-UTRA	16.1.0
2019-06	SP#84	SP-190399	1279	-	A	Clarification for interface identifier allocation in IPv6 Multi-homing	16.1.0
2019-06	SP#84	SP-190407	1283	3	F	Interaction between MICO mode with active time and eDRX	16.1.0
2019-06	SP#84	SP-190407	1287	-	F	Update reference to TS 24.250	16.1.0
2019-06	SP#84	SP-190426	1291	1	B	Introduction of UDICOM	16.1.0
2019-06	SP#84	SP-190417	1296	2	C	Adding Support for Indicating Serialization Format in RDS	16.1.0
2019-06	SP#84	SP-190428	1297	2	F	CAG and Network Slice Selection	16.1.0
2019-06	SP#84	SP-190428	1298	3	F	Unified Access Control with NPN	16.1.0
2019-06	SP#84	SP-190399	1301	1	A	Configuring Transport Level Marking values	16.1.0
2019-06	SP#84	SP-190427	1303	1	F	Alignment of Network Slice selection logic	16.1.0
2019-06	SP#84	SP-190413	1305	2	F	Enforcement of UP integrity protection	16.1.0
2019-06	SP#84	SP-190429	1306	2	F	Ethernet support clarification	16.1.0
2019-06	SP#84	SP-190412	1307	2	F	Generalized text for redundant user planes in RAN	16.1.0
2019-06	SP#84	SP-190413	1308	3	C	DNN replacement in 5GC	16.1.0
2019-06	SP#84	SP-190410	1312	1	B	Extending the significance of the locality parameter	16.1.0
2019-06	SP#84	SP-190399	1315	2	A	Correcting AMF selection	16.1.0
2019-06	SP#84	SP-190422	1316	1	C	Clarify which parameters are (not) applicable for I-SMF selection.	16.1.0
2019-06	SP#84	SP-190412	1320	3	F	Clarification on redundant N3 tunnel solution	16.1.0
2019-06	SP#84	SP-190427	1321	-	F	Clarification on IWK without N26	16.1.0
2019-06	SP#84	SP-190418	1323	1	C	S6b optional for ePDG connected to 5GS	16.1.0
2019-06	SP#84	SP-190429	1328	2	F	Data forwarding for 5G-LAN multicast	16.1.0
2019-06	SP#84	SP-190410	1331	3	B	Support of Service Context Transfer in TS23.501	16.1.0

2019-06	SP#84	SP-190413	1333	1	B	Alignment of IMS Voice Service via EPS Fallback with RAN specifications	16.1.0
2019-06	SP#84	SP-190407	1337	1	B	Update to High Latency Overall Description	16.1.0
2019-06	SP#84	SP-190429	1338	2	F	NPN: Corrections to handling of Allowed CAG list and CAG-only indication	16.1.0
2019-06	SP#84	SP-190429	1339	2	F	NPN: Correction to CAG-only indication	16.1.0
2019-06	SP#84	SP-190429	1341	2	F	NPN: Update and enforcement of new Allowed CAG list and CAG-only indication	16.1.0
2019-06	SP#84	SP-190407	1346	2	F	CIoT scope clarification	16.1.0
2019-06	SP#84	SP-190404	1350	2	A	Location Reporting of secondary cell	16.1.0
2019-06	SP#84	SP-190416	1351	2	B	Network request re-activation of user-plane resources	16.1.0
2019-06	SP#84	SP-190416	1352	2	B	Clarification on Access Network Performance Measurements	16.1.0
2019-06	SP#84	SP-190399	1358	1	A	Emergency Fallback from non-3GPP/ePDG	16.1.0
2019-06	SP#84	SP-190407	1360	1	F	NIDD related indications	16.1.0
2019-06	SP#84	SP-190420	1362	2	B	Description regarding NEF support of data retrieval from external party	16.1.0
2019-06	SP#84	SP-190427	1366	3	F	Subscription Segmentation in PCF and UDR	16.1.0
2019-06	SP#84	SP-190427	1367	2	C	Serving PLMN UE-AMBR control	16.1.0
2019-06	SP#84	SP-190415	1372	1	B	Access network selection for devices that do not support NAS over WLAN	16.1.0
2019-06	SP#84	SP-190415	1374	-	B	AMF overload control for trusted non-3GPP access	16.1.0
2019-06	SP#84	SP-190413	1375	2	B	23.501 part of PCF selection for PDU sessions with same DNN and S-NSSAI	16.1.0
2019-06	SP#84	SP-190407	1376	1	B	Support for Enhanced Coverage Restriction Control via NEF	16.1.0
2019-06	SP#84	SP-190413	1378	1	F	Support for Dynamic Port Management in RDS	16.1.0
2019-06	SP#84	SP-190429	1381	2	B	Introduction of TSN Sync soln #28A	16.1.0
2019-06	SP#84	SP-190429	1382	1	F	Update to Survival time EN	16.1.0
2019-06	SP#84	SP-190419	1384	3	B	Adding UDR NF Group ID association functionality	16.1.0
2019-06	SP#84	SP-190413	1390	2	F	Correction of use of PEI/IMEI for non-3GPP only UEs	16.1.0
2019-06	SP#84	SP-190416	1395	1	F	Clarifications on Reflective QoS for MPTCP	16.1.0
2019-06	SP#84	SP-190429	1396	1	B	NW selection considering RAN sharing for SNPNs	16.1.0
2019-06	SP#84	SP-190421	1404	1	F	Target AMF Selection during mobility from EPS to 5GS	16.1.0
2019-06	SP#84	SP-190420	1405	-	F	Corrections to analytics used by AMF for MICO mode and SMF for UPF selection	16.1.0
2019-06	SP#84	SP-190420	1406	1	B	Update NRF descriptions to support AF Available Data Registration as described in TS23.288	16.1.0
2019-06	SP#84	SP-190427	1408	2	F	Corrections and alignments for the 5QI characteristics table	16.1.0
2019-06	SP#84	SP-190410	1413	2	B	NF Set concept for SMF	16.1.0
2019-06	SP#84	SP-190407	1417	2	B	Stateless IPv6 Address Autoconfiguration for Control Plane CIoT 5GS Optimisation	16.1.0
2019-06	SP#84	SP-190407	1418	2	B	Introduction of Small Data Rate Control Interworking with APN Rate Control	16.1.0
2019-06	SP#84	SP-190415	1420	2	B	Location information for trusted N3GPP	16.1.0
2019-06	SP#84	SP-190429	1423	2	B	TSC Burst Arrival Time usage and Clock Reference	16.1.0
2019-06	SP#84	SP-190413	1424	2	F	Correction on Location reporting procedure	16.1.0
2019-06	SP#84	SP-190429	1425	3	C	Address editor's notes for 5GS Bridge management and QoS mapping	16.1.0
2019-06	SP#84	SP-190429	1426	4	C	clarifications on SNPN	16.1.0
2019-06	SP#84	SP-190429	1427	2	C	Support for unicast traffic forwarding within a 5G VN group	16.1.0
2019-06	SP#84	SP-190429	1430	2	C	implementation of 5GLAN related interfaces	16.1.0
2019-06	SP#84	SP-190407	1431	1	B	Support of User Plane Optimisations in Preferred and Supported Network Behaviour	16.1.0
2019-06	SP#84	SP-190429	1432	1	B	Ingress timestamp signalling	16.1.0
2019-06	SP#84	SP-190413	1436	-	F	Align CHF service for offline only charging	16.1.0
2019-06	SP#84	SP-190419	1438	2	B	HSS discovery via NRF	16.1.0
2019-06	SP#84	SP-190429	1443	1	B	AF influence for traffic forwarding in 5GLAN	16.1.0
2019-06	SP#84	SP-190431	1445	2	B	Update of TS23.501 to finalize xBDT feature	16.1.0
2019-06	SP#84	SP-190429	1448	-	D	Vertical_LAN - Editorial clean up	16.1.0
2019-06	SP#84	SP-190399	1449	1	A	Applicability of Allowed NSSAI to PLMNs whose TAIs are in the RA TAI list	16.1.0
2019-06	SP#84	SP-190399	1451	-	A	Clarification on S-NSSAI for PDU session in Requested NSSAI	16.1.0
2019-09	SP#85	SP-190608	0990	6	B	Introduction of QoS Monitoring to assist URLLC Service	16.2.0
2019-09	SP#85	SP-190618	1097	3	F	Support of Standalone Non-Public Networks	16.2.0
2019-09	SP#85	SP-190618	1240	5	F	Clarification of support of dual radio UE	16.2.0
2019-09	SP#85	SP-190610	1329	3	F	IP Address Accessibility for MA PDU Session	16.2.0
2019-09	SP#85	SP-190610	1330	2	F	N3/N9 Tunnels for the MA-PDU Session	16.2.0
2019-09	SP#85	SP-190605	1347	6	F	Introducing of UP CIoT 5GS Optimisation capability	16.2.0
2019-09	SP#85	SP-190605	1364	1	F	NIDD Description Update for Maximum Packet Size	16.2.0
2019-09	SP#85	SP-190618	1371	3	F	Clarification for the related CAG identifier	16.2.0
2019-09	SP#85	SP-190618	1379	2	F	Support for access to PLMN services via SNPN and SNPN services via PLMN	16.2.0
2019-09	SP#85	SP-190608	1414	3	B	QoS monitoring based on GTP-U paths	16.2.0

2019-09	SP#85	SP-190615	1440	8	B	Enhancements to QoS Handling for V2X Communication Over Uu Reference Point	16.2.0
2019-09	SP#85	SP-190607	1453	4	F	Completion of the PCF Group	16.2.0
2019-09	SP#85	SP-190622	1454	2	F	Inter Core Network Roaming	16.2.0
2019-09	SP#85	SP-190609	1455	3	F	Align PLMN selection with service requirements	16.2.0
2019-09	SP#85	SP-190605	1457	2	F	NAS RAI corrections	16.2.0
2019-09	SP#85	SP-190605	1461	2	F	Clarifications to QoS support for NB-IoT	16.2.0
2019-09	SP#85	SP-190617	1463	3	F	Correction on support of RACS	16.2.0
2019-09	SP#85	SP-190618	1464	3	C	Completing Ethernet port management	16.2.0
2019-09	SP#85	SP-190605	1465	2	F	Adding N4 Notification about buffered packets being dropped	16.2.0
2019-09	SP#85	SP-190609	1466	-	F	PEI for 5G-RG and FN-RG	16.2.0
2019-09	SP#85	SP-190618	1467	1	F	Corrections to general 5G LAN description	16.2.0
2019-09	SP#85	SP-190618	1468	3	F	5G LAN user plane corrections	16.2.0
2019-09	SP#85	SP-190610	1469	4	F	Awareness of UE PMF port number and MAC address in UPF	16.2.0
2019-09	SP#85	SP-190607	1470	4	F	Clarification of the Locality of a NF Instance	16.2.0
2019-09	SP#85	SP-190621	1476	2	F	Replacement of VPLMN by serving PLMN where appropriate	16.2.0
2019-09	SP#85	SP-190621	1477	1	F	Clarification on the misalignment of service area restriction between UE and Network	16.2.0
2019-09	SP#85	SP-190611	1478	1	F	Correction of P-CSCF selection to consider proximity to UPF	16.2.0
2019-09	SP#85	SP-190605	1479	1	F	Aligning Terminology referring to the CIoT 5GS Optimisations	16.2.0
2019-09	SP#85	SP-190617	1480	1	F	Corrections of PLMN assigned Capability signaling	16.2.0
2019-09	SP#85	SP-190621	1483	1	F	Correction of Network Slice selection with NSSF	16.2.0
2019-09	SP#85	SP-190621	1487	3	C	DNN replacement in 5GC	16.2.0
2019-09	SP#85	SP-190608	1489	1	F	Failure handling for redundancy based on dual connectivity	16.2.0
2019-09	SP#85	SP-190608	1490	1	F	Clarification on reordering requirement with GTP-U redundancy	16.2.0
2019-09	SP#85	SP-190601	1494	1	A	Discrepancy with TS 33.501 with respect to Secondary Authentication	16.2.0
2019-09	SP#85	SP-190610	1500	2	F	Clarification of traffic switching for GBR QoS flow in MA PDU session	16.2.0
2019-09	SP#85	SP-190618	1501	3	F	N19 Tunnel management	16.2.0
2019-09	SP#85	SP-190618	1504	3	C	TSN Time Synchronization Traffic Handling	16.2.0
2019-09	SP#85	SP-190618	1507	3	F	TSC Assistance Information update	16.2.0
2019-09	SP#85	SP-190605	1509	1	F	Handling of CIoT optimisations not supported over NR	16.2.0
2019-09	SP#85	SP-190617	1517	2	C	Handling of NB-IOT radio capabilities and RACS in 5GS	16.2.0
2019-09	SP#85	SP-190601	1519	2	A	Allowed NSSAI and TAI list from (previous) UE Configuration Update	16.2.0
2019-09	SP#85	SP-190622	1521	1	F	Use of the URSP rules when UE attaches to EPS	16.2.0
2019-09	SP#85	SP-190624	1522	1	B	Introduction of the IAB support in 5GS	16.2.0
2019-09	SP#85	SP-190621	1540	2	F	Clarification on the meaning of Emergency Services Support indicator	16.2.0
2019-09	SP#85	SP-190605	1541	2	F	Addition of missing CIoT services	16.2.0
2019-09	SP#85	SP-190606	1543	1	F	Addition of missing GMLC and its service	16.2.0
2019-09	SP#85	SP-190614	1544	3	F	Mobility event management	16.2.0
2019-09	SP#85	SP-190608	1547	-	F	Improvement for support of redundant transmission on N3/N9 interfaces	16.2.0
2019-09	SP#85	SP-190621	1548	1	F	Clarification on S-NSSAI(s) for PDU session	16.2.0
2019-09	SP#85	SP-190622	1556	2	D	Adding Policy Charging and Control related reference points	16.2.0
2019-09	SP#85	SP-190621	1557	2	F	Update to NEF related reference points	16.2.0
2019-09	SP#85	SP-190611	1563	1	F	NF Group resolution by SCP	16.2.0
2019-09	SP#85	SP-190610	1570	1	F	Corrections about default QoS rule	16.2.0
2019-09	SP#85	SP-190610	1571	3	B	Interworking for MA PDU Session	16.2.0
2019-09	SP#85	SP-190605	1573	2	F	Conditions to use CP or UP CIoT	16.2.0
2019-09	SP#85	SP-190621	1578	1	F	Correction of NAS transport for LCS	16.2.0
2019-09	SP#85	SP-190605	1580	2	F	Corrections to Control Plane CIoT 5GS Optimisation description	16.2.0
2019-09	SP#85	SP-190605	1581	-	F	Alignment of the term Early Data Transmission	16.2.0
2019-09	SP#85	SP-190610	1586	3	B	Network request re-activation of user-plane resources	16.2.0
2019-09	SP#85	SP-190610	1587	1	F	PMF message delivery	16.2.0
2019-09	SP#85	SP-190613	1588	3	F	AMF capability of Network Slice-Specific Authentication and Authorization	16.2.0
2019-09	SP#85	SP-190622	1589	3	F	Priority of CHF selection	16.2.0
2019-09	SP#85	SP-190605	1596	1	B	Clarify short DRX cycle length CM-CONNECTED with RRC inactive for eMTC	16.2.0
2019-09	SP#85	SP-190605	1598	3	F	Clarification on NEF discovery by an AF	16.2.0
2019-09	SP#85	SP-190618	1604	-	F	Exclusive Gating Mechanism	16.2.0
2019-09	SP#85	SP-190611	1607	1	F	Update P-CSCF Discovery using NRF	16.2.0
2019-09	SP#85	SP-190618	1608	1	F	GUAMI allocation for standalone non-public network	16.2.0
2019-09	SP#85	SP-190607	1622	-	F	Relation between Group and Set	16.2.0
2019-09	SP#85	SP-190607	1624	3	F	Network Function/NF Service Context	16.2.0
2019-09	SP#85	SP-190605	1632	3	F	Clarification on strictly periodic timer in relation to MICO mode.	16.2.0
2019-09	SP#85	SP-190610	1636	2	F	Mandatory support of ATSSS-LL for PDU Sessions of type Ethernet	16.2.0
2019-09	SP#85	SP-190618	1637	3	F	Update of 5G LAN-type service feature description	16.2.0

2019-09	SP#85	SP-190608	1643	2	C	Clarifications on URLLC support	16.2.0
2019-09	SP#85	SP-190608	1644	1	F	Clarification and correction to AF response	16.2.0
2019-09	SP#85	SP-190610	1646	1	F	MA PDU IP Address/Prefix Handling in UPF	16.2.0
2019-09	SP#85	SP-190618	1647	1	F	Use of NW instance for N19 interface	16.2.0
2019-09	SP#85	SP-190609	1650	1	F	Corrections for devices that do not support 5GC NAS over WLAN access	16.2.0
2019-09	SP#85	SP-190610	1652	-	F	Correction to protocol stacks for RTT measurements	16.2.0
2019-09	SP#85	SP-190610	1653	3	F	Clarification about an MA PDU Session using only MPTCP functionality	16.2.0
2019-09	SP#85	SP-190618	1659	2	C	Support of forwarding of broadcast and multicast packets	16.2.0
2019-09	SP#85	SP-190618	1660	2	C	Address editor's notes for TSN	16.2.0
2019-09	SP#85	SP-190607	1664	4	F	eSBA SMF and PCF selection-option 2	16.2.0
2019-09	SP#85	SP-190605	1665	1	F	Clarification on Preferred Network Behaviour for CIoT 5GS Optimisations	16.2.0
2019-09	SP#85	SP-190605	1669	1	F	Removal of eDRX support with RRC_INACTIVE for NB-IoT	16.2.0
2019-09	SP#85	SP-190605	1670	2	F	UPF Service Area awareness for keeping UL N3 Tunnel available	16.2.0
2019-09	SP#85	SP-190612	1671	3	F	Correction on data collection from an AF	16.2.0
2019-09	SP#85	SP-190618	1675	2	C	Modification to the QoS parameters mapping for 5GS Bridge configuration	16.2.0
2019-09	SP#85	SP-190612	1677	1	F	Updating the stored information in NRF to support BSF discovery	16.2.0
2019-09	SP#85	SP-190622	1678	5	C	On the usage of rateRatio, one-step vs two-step sync operation and dedicated QoS Flow	16.2.0
2019-12	SP#86	SP-191068	1363	3	B	Identification of LTE-M (eMTC) traffic	16.3.0
2019-12	SP#86	SP-191076	1373	2	F	Corrections to Trusted Non-3GPP Access Network selection	16.3.0
2019-12	SP#86	SP-191090	1459	3	F	Correcting AMF selection	16.3.0
2019-12	SP#86	SP-191071	1472	2	F	Correcting behavior if binding indication is not provided	16.3.0
2019-12	SP#86	SP-191071	1473	4	F	Correcting delegated discovery and selection and the use of IDs in binding	16.3.0
2019-12	SP#86	SP-191068	1485	3	F	Service Gap Control at IWK	16.3.0
2019-12	SP#86	SP-191068	1486	1	F	Serving PLMN rate control parameters in modification procedure	16.3.0
2019-12	SP#86	SP-191071	1527	3	F	SMF Set and UPF	16.3.0
2019-12	SP#86	SP-191076	1553	2	F	Completing the introduction of TNGF in 23.501	16.3.0
2019-12	SP#86	SP-191088	1564	3	F	Correction to deletion of PLMN-assigned UE Radio Capability ID	16.3.0
2019-12	SP#86	SP-191090	1576	2	F	Correction of UE Radio Capability Update IE encoding	16.3.0
2019-12	SP#86	SP-191088	1592	10	F	Resolution of Editor's Note on UCMF-AMF interaction	16.3.0
2019-12	SP#86	SP-191068	1594	3	F	I-NEF in Interworking Scenarios	16.3.0
2019-12	SP#86	SP-191071	1623	2	F	NRF use of UDR Group ID Mapping service	16.3.0
2019-12	SP#86	SP-191080	1654	2	F	UE related analytics for UPF selection	16.3.0
2019-12	SP#86	SP-191068	1666	8	F	Corrections to Small Data Rate Control and Exception Reporting	16.3.0
2019-12	SP#86	SP-191068	1667	4	B	Introduction of RRC Connection Re-Establishment for CP	16.3.0
2019-12	SP#86	SP-191071	1679	2	F	Clarification on target address in service request message	16.3.0
2019-12	SP#86	SP-191074	1687	1	A	Condition for the UE to provide a Requested NSSAI	16.3.0
2019-12	SP#86	SP-191076	1688	-	F	Network slicing impacts of Wireless and Wireline Convergence	16.3.0
2019-12	SP#86	SP-191068	1689	2	F	Support of TAs with heterogeneous support of eDRX	16.3.0
2019-12	SP#86	SP-191068	1690	2	F	Control Plane CIoT 5GS Optimisations restriction on NR	16.3.0
2019-12	SP#86	SP-191068	1692	1	F	Addition of I-NEF to Network Functions	16.3.0
2019-12	SP#86	SP-191068	1693	1	F	Service Exposure in Interworking Scenarios	16.3.0
2019-12	SP#86	SP-191090	1695	2	F	Correction to PPI setting control over N4	16.3.0
2019-12	SP#86	SP-191082	1697	-	F	Interaction between ETSUN and CIoT.	16.3.0
2019-12	SP#86	SP-191082	1698	1	F	Clarifications to ETSUN specification	16.3.0
2019-12	SP#86	SP-191077	1702	3	F	Clarification on QoS Support for ATSSS	16.3.0
2019-12	SP#86	SP-191090	1703	3	F	Clarification on DNN replacement	16.3.0
2019-12	SP#86	SP-191090	1710	4	F	Clarification on N6 traffic routing information for Ethernet type PDU Session	16.3.0
2019-12	SP#86	SP-191092	1711	1	F	clarification on N6-based traffic forwarding of 5GLAN	16.3.0
2019-12	SP#86	SP-191077	1714	2	F	MA PDU Upgrade in modification procedure	16.3.0
2019-12	SP#86	SP-191071	1715	1	F	Delegated discovery and selection in SCP for CHF and SMSF	16.3.0
2019-12	SP#86	SP-191073	1716	1	C	Update N4 rules for QoS Monitoring	16.3.0
2019-12	SP#86	SP-191088	1717	2	F	Clarification on UE capability update	16.3.0
2019-12	SP#86	SP-191068	1721	2	F	Removal of ENs for control plane congestion control	16.3.0
2019-12	SP#86	SP-191090	1722	2	F	Multicast forwarding for Ethernet type PDU Session	16.3.0
2019-12	SP#86	SP-191081	1723	2	F	Alignments to support Network Slice-Specific Authentication and Authorization	16.3.0
2019-12	SP#86	SP-191082	1726	2	F	Clarification on IPv6 Router Advertisement message in ETSUN	16.3.0
2019-12	SP#86	SP-191090	1728	1	F	SMF selection clarification	16.3.0
2019-12	SP#86	SP-191071	1729	4	F	Group ID and Set ID	16.3.0
2019-12	SP#86	SP-191081	1730	1	F	AMF redirection at handover from 4G to 5G	16.3.0
2019-12	SP#86	SP-191077	1733	1	F	Clarification of Access Availability report via N4	16.3.0
2019-12	SP#86	SP-191090	1734	1	F	Clarification of terms in secondary authentication	16.3.0
2019-12	SP#86	SP-191084	1735	1	B	Extension of standardized 5QI to QoS characteristics mapping table to accommodate enhanced V2X requirements	16.3.0
2019-12	SP#86	SP-191090	1736	2	F	Determination of Emergency Services Fallback support in the AMF	16.3.0

2019-12	SP#86	SP-191080	1737	-	F	UDM Discovery by Internal Group ID	16.3.0
2019-12	SP#86	SP-191074	1738	3	F	UE may provide NSSAI in AS for initial registration	16.3.0
2019-12	SP#86	SP-191090	1739	5	F	No impact on IMS voice session by a change of the IMS voice over PS session indicator during fallback	16.3.0
2019-12	SP#86	SP-191090	1740	1	F	Clarification of Homogeneous Support of IMS Voice over PS Sessions	16.3.0
2019-12	SP#86	SP-191073	1742	1	F	Enhancement of UP path management based on the coordination with AFs	16.3.0
2019-12	SP#86	SP-191090	1743	2	F	PCF selection for multiple PDU Sessions to the same DNN and S-NSSAI	16.3.0
2019-12	SP#86	SP-191068	1745	-	F	Extended NAS timers for CE mode B	16.3.0
2019-12	SP#86	SP-191068	1746	1	F	Correcting AMF decision to set CP only indicator	16.3.0
2019-12	SP#86	SP-191092	1747	7	F	5GS Bridge Management	16.3.0
2019-12	SP#86	SP-191092	1750	3	F	Completing QoS and TSCAI mapping	16.3.0
2019-12	SP#86	SP-191092	1751	3	F	Clarifying N3IWF access to SNPN	16.3.0
2019-12	SP#86	SP-191092	1752	3	F	Clarifying CAG handling during RRC resume procedure	16.3.0
2019-12	SP#86	SP-191090	1754	1	F	Update to Clause 4.2.7 Reference Points	16.3.0
2019-12	SP#86	SP-191090	1755	3	F	Corrections on Session-AMBR setting and enforcement	16.3.0
2019-12	SP#86	SP-191074	1757	1	A	Correction on PCF selection and discovery	16.3.0
2019-12	SP#86	SP-191078	1759	-	F	UDR service for mapping IMS Public Identity to HSS Group ID for HSS selection	16.3.0
2019-12	SP#86	SP-191071	1765	3	F	Notification receiver information in a subscription	16.3.0
2019-12	SP#86	SP-191071	1766	3	F	Correcting delegated discovery for PCF	16.3.0
2019-12	SP#86	SP-191090	1767	2	F	23.501:PCF provides PCC rule to SMF based on Local routing indication in subscription information	16.3.0
2019-12	SP#86	SP-191073	1768	2	F	Delivery of SMF waiting time to AF for session continuity	16.3.0
2019-12	SP#86	SP-191077	1769	3	F	Corrections for performance measurements	16.3.0
2019-12	SP#86	SP-191074	1770	2	F	Correction on TNLA binding	16.3.0
2019-12	SP#86	SP-191077	1771	3	F	General corrections for MA PDU sessions	16.3.0
2019-12	SP#86	SP-191077	1772	2	F	Corrections to interworking with EPS for ATSSS	16.3.0
2019-12	SP#86	SP-191077	1773	2	F	N4 impacts due to ATSSS	16.3.0
2019-12	SP#86	SP-191077	1774	3	F	Corrections to steering functionalities description	16.3.0
2019-12	SP#86	SP-191090	1775	2	F	PCF selection for DNN replacement	16.3.0
2019-12	SP#86	SP-191074	1778	2	F	Remote Interference Management support	16.3.0
2019-12	SP#86	SP-191084	1785	2	F	Corrections to handling of Alternative QoS Profiles	16.3.0
2019-12	SP#86	SP-191080	1787	7	F	Consistency on Definitions related to NWDAF	16.3.0
2019-12	SP#86	SP-191068	1792	2	F	EDT support for UP CIoT Optimisation	16.3.0
2019-12	SP#86	SP-191092	1797	3	F	Support of PLMN managed NIDs	16.3.0
2019-12	SP#86	SP-191092	1798	2	F	Support of NG-RAN sharing options for NPN	16.3.0
2019-12	SP#86	SP-191074	1801	2	F	TS 23.501: PEI format for non-3GPP devices	16.3.0
2019-12	SP#86	SP-191092	1802	2	F	TSN 5QI clarification and static TSC QoS Flow establishment	16.3.0
2019-12	SP#86	SP-191092	1804	3	F	5GS bridge model interpretation	16.3.0
2019-12	SP#86	SP-191092	1806	5	F	Revision on MDBV mapping	16.3.0
2019-12	SP#86	SP-191092	1815	2	F	clarification on the Qos parameters mapping and TSCAI creation	16.3.0
2019-12	SP#86	SP-191073	1816	-	F	Clarification on the Standardized or pre-configured 5QI parameters modification	16.3.0
2019-12	SP#86	SP-191068	1817	1	F	Expected UE behaviour data contents	16.3.0
2019-12	SP#86	SP-191068	1818	2	F	Correction of Small Data Rate Control interworking	16.3.0
2019-12	SP#86	SP-191090	1819	1	F	Network selection correction	16.3.0
2019-12	SP#86	SP-191092	1821	3	F	Clarification of SMF management of 5GLAN PDU sessions	16.3.0
2019-12	SP#86	SP-191092	1822	3	F	Clarification of UPF selection for 5GLAN communication	16.3.0
2019-12	SP#86	SP-191092	1823	1	F	Clarification of use of AF influence in 5GLAN	16.3.0
2019-12	SP#86	SP-191088	1828	3	F	Misleading RACS architecture pictures	16.3.0
2019-12	SP#86	SP-191088	1829	6	F	removing requirement that TAC+SV is used to identify UE model in manufacturer assigned ID	16.3.0
2019-12	SP#86	SP-191086	1833	3	F	changing IAB-MT to IAB-UE	16.3.0
2019-12	SP#86	SP-191074	1837	2	F	Correction on applicability of slicing to more than 3GPP access	16.3.0
2019-12	SP#86	SP-191074	1839	2	F	Incorrect reference to clause in specification	16.3.0
2019-12	SP#86	SP-191090	1840	1	F	Alignment with SA5 on Charging for 5G connection and mobility domain	16.3.0
2019-12	SP#86	SP-191082	1842	3	F	PDU Session with SSC mode 2/3	16.3.0
2019-12	SP#86	SP-191090	1845	3	C	General description and data volume reporting for NR in unlicensed bands	16.3.0
2019-12	SP#86	SP-191090	1847	2	B	Access restrictions for primary and secondary RAT	16.3.0
2019-12	SP#86	SP-191090	1849	1	B	Introduction of UE specific DRX for NB-IOT	16.3.0
2019-12	SP#86	SP-191074	1853	1	A	Correction of QFI value in QER	16.3.0
2019-12	SP#86	SP-191073	1854	5	F	Management of GBR QoS Flows at handover	16.3.0
2019-12	SP#86	SP-191092	1857	5	F	Updates to the 5G VN broadcast solution	16.3.0
2019-12	SP#86	SP-191090	1859	4	F	PDU session anchor terminology clarification	16.3.0
2019-12	SP#86	SP-191074	1860	4	F	Remove incorrect reasoning of default MDBV value setting	16.3.0
2019-12	SP#86	SP-191077	1868	5	F	ATSSS Link-Specific Multipath IP Address Configuration	16.3.0
2019-12	SP#86	SP-191077	1869	10	F	ATSSS Steering of non-MPTCP Traffic	16.3.0

2019-12	SP#86	SP-191077	1870	3	F	ATSSS PMF Protocol over UDP	16.3.0
2019-12	SP#86	SP-191077	1875	2	F	Interworking with EPS for the MA PDU Session	16.3.0
2019-12	SP#86	SP-191073	1878	2	F	5G URLLC Handling PDU Session Failure	16.3.0
2019-12	SP#86	SP-191092	1879	2	F	UPF selection for 5G URLLC PDU Sessions	16.3.0
2019-12	SP#86	SP-191092	1881	3	F	UE identifier for SNPN	16.3.0
2019-12	SP#86	SP-191092	1887	2	F	N4 Impacts - Bridge Management	16.3.0
2019-12	SP#86	SP-191092	1888	5	F	Clarification for TSC QoS Mapping clause	16.3.0
2019-12	SP#86	SP-191092	1889	2	F	TSC PDU Session Restrictions	16.3.0
2019-12	SP#86	SP-191092	1890	7	F	TSCAI granularity	16.3.0
2019-12	SP#86	SP-191092	1893	3	F	UPF functional update for TSC	16.3.0
2019-12	SP#86	SP-191071	1895	-	F	Clarification on SMF identifier in HR roaming	16.3.0
2019-12	SP#86	SP-191068	1899	2	F	Clarifications on CN assistance information sent to the RAN	16.3.0
2019-12	SP#86	SP-191086	1901	1	B	Handling of IAB-indication to 5GC	16.3.0
2019-12	SP#86	SP-191086	1902	1	B	Handling of OAM traffic for IAB-node	16.3.0
2019-12	SP#86	SP-191086	1903	1	B	Support of IAB operation in EN-DC mode	16.3.0
2019-12	SP#86	SP-191086	1905	1	F	Mobility support limitation for IAB	16.3.0
2019-12	SP#86	SP-191078	1912	-	F	Including IMS related interfaces in list of 5G interfaces	16.3.0
2019-12	SP#86	SP-191090	1918	-	F	Clarification on UE mobility event notification	16.3.0
2019-12	SP#86	SP-191076	1920	1	F	Avoid specifying SUPI / SUCI and PEI used for FN RG both in 23.501 and 23.316	16.3.0
2019-12	SP#86	SP-191077	1923	2	F	Corrections to ATSSS capabilities of a MA PDU Session	16.3.0
2019-12	SP#86	SP-191077	1924	1	F	Applicability of UP Security Policy to a MA PDU Session	16.3.0
2019-12	SP#86	SP-191082	1929	3	F	(I)SMF notifications: which SMF events need to be supported by ISMF	16.3.0
2019-12	SP#86	SP-191092	1932	2	F	Clarification on the PDU session management for VN	16.3.0
2019-12	SP#86	SP-191074	1934	1	F	Correction on SMSF change	16.3.0
2019-12	SP#86	SP-191074	1935	2	F	Correction on UE context handling during inter system mobility	16.3.0
2019-12	SP#86	SP-191088	1936	2	F	Inclusion of Version Identifier in PLMN assigned ID	16.3.0
2019-12	SP#86	SP-191077	1937	1	F	Corrections for link-specific multipath address/prefix and MPTCP proxy IP address	16.3.0
2019-12	SP#86	SP-191074	1940	3	F	Selecting SMF that support static IP address	16.3.0
2019-12	SP#86	SP-191090	1941	4	F	Number of EBIs	16.3.0
2019-12	SP#86	SP-191071	1942	2	F	Notification URI	16.3.0
2019-12	SP#86	SP-191082	1943	2	F	I-SMF handling of N4 Information	16.3.0
2019-12	SP#86	SP-191090	1945	-	F	Correction of implementation of CR #1321	16.3.0
2019-12	SP#86	SP-191074	1949	1	F	Clarification on the PCF selection	16.3.0
2019-12	SP#86	SP-191074	1956	-	A	Removal of wrongly implemented Network Slicing CR #1031 and mirror CR #1131	16.3.0
2019-12	SP#86	SP-191073	1971	-	F	Correction on support of redundant transmission on N3/N9 interfaces	16.3.0
2019-12	SP#86	SP-191068	1972	-	F	Clarification on Control Plane Only Indicator	16.3.0
2019-12	SP#86	SP-191073	1973	1	F	Correction and clarification to AF influence in URLLC	16.3.0
2019-12	SP#86	SP-191074	1976	2	F	ULCL/BP based on the local routing policy	16.3.0
2019-12	SP#86	SP-191081	1979	2	F	On NSSAA Services	16.3.0
2019-12	SP#86	SP-191092	1981	5	F	Applying Per-Stream Filtering and Policing	16.3.0
2019-12	SP#86	SP-191074	1985	1	A	S-NSSAI setting for emergency service	16.3.0
2019-12	SP#86	SP-191074	1986	2	B	Solution on support of NAT in 5GS	16.3.0
2019-12	SP#86	SP-191080	1992	1	F	Corrections to NWDAF discovery and selection	16.3.0
2019-12	SP#86	SP-191068	1993	-	F	UE support of CP optimization over NB-IoT	16.3.0
2019-12	SP#86	SP-191071	1994	1	F	Correction of CHF discovery to consider eSBA binding principles	16.3.0
2019-12	SP#86	SP-191092	1997	3	F	PNI-NPN - Reusing NSSAI for AMF selection when NPN isolation is needed	16.3.0
2019-12	SP#86	SP-191084	2001	-	F	Correction on the support of V2X in 5GS	16.3.0
2019-12	SP#86	SP-191086	2003	-	F	Remove protocol stack diagrams for IAB	16.3.0
2019-12	SP#86	SP-191086	2004	1	F	Remove Editor's Notes for IAB related clauses	16.3.0
2019-12	SP#86	SP-191081	2005	1	F	Correction on pending NSSAA indication to UE	16.3.0
2019-12	SP#86	SP-191082	2006	-	F	ETSUN: correction for I-SMF trace	16.3.0
2020-03	SP#87E	SP-200075	1482	7	F	Alignments and corrections to Non-Public Network functionality	16.4.0
2020-03	SP#87E	SP-200075	1520	4	F	PLMN+CAG information - minimum, maximum storage and survival of power cycle	16.4.0
2020-03	SP#87E	SP-200075	1595	2	F	23.501 Supporting for AF providing UE IP address(es) for 5G VN group PDU sessions	16.4.0
2020-03	SP#87E	SP-200062	1668	4	F	Clarification to MICO mode and Periodic Registration Timer Control	16.4.0
2020-03	SP#87E	SP-200062	1691	3	F	Alignment with TS 23.502 and clarification on Extended Buffering	16.4.0
2020-03	SP#87E	SP-200075	1749	7	F	Item#4: Apply StaticFilteringEntry information in 5GS	16.4.0
2020-03	SP#87E	SP-200069	1782	4	F	Applicability of PS data off to ATSSS and MA PDU sessions	16.4.0
2020-03	SP#87E	SP-200078	1783	6	F	UE IDLE over N3GPP responding to indication of DL data when access is available	16.4.0
2020-03	SP#87E	SP-200075	1799	7	F	Support of CAG ID privacy	16.4.0
2020-03	SP#87E	SP-200078	1848	14	F	Introduction of the Inter PLMN UP functionality in the architecture	16.4.0
2020-03	SP#87E	SP-200075	1882	4	F	UDM - AUSF Discovery & Selection in an SNPN	16.4.0

2020-03	SP#87E	SP-200069	1947	3	F	Corrections to general MA PDU session handling	16.4.0
2020-03	SP#87E	SP-200075	1951	4	F	Clarifying gPTP message forwarding for multiple TSN PDU sessions	16.4.0
2020-03	SP#87E	SP-200069	1957	2	F	Adding ATSSS functionality into the UPF	16.4.0
2020-03	SP#87E	SP-200075	1980	3	F	MDBV mapping and configuration for TSC QoS Flow	16.4.0
2020-03	SP#87E	SP-200075	2007	1	F	Correction on TSCAI: TSN open issue #1	16.4.0
2020-03	SP#87E	SP-200075	2009	1	F	Correct errors in Port Management information table	16.4.0
2020-03	SP#87E	SP-200071	2011	1	F	Re-allowing UE for services after the NSSAA revocation	16.4.0
2020-03	SP#87E	SP-200078	2015	2	F	CN component of the PDB is configured per UL and DL	16.4.0
2020-03	SP#87E	SP-200078	2017	1	F	Correcting AMF selection	16.4.0
2020-03	SP#87E	SP-200075	2019	2	F	Procedures for handover between SNPN and PLMN	16.4.0
2020-03	SP#87E	SP-200078	2020	3	F	MTU size considerations	16.4.0
2020-03	SP#87E	SP-200065	2021	4	F	Binding for notification reselection corrections	16.4.0
2020-03	SP#87E	SP-200065	2022	3	F	Correcting delegated discovery for PCF	16.4.0
2020-03	SP#87E	SP-200075	2026	1	F	Correction of current context and using 5GS bridge to refer to 5GS functions act as TSN bridge	16.4.0
2020-03	SP#87E	SP-200068	2027	2	F	Support of Wireline access requires both N1 signalling and N2 signalling	16.4.0
2020-03	SP#87E	SP-200075	2028	3	F	Clarification on the 5G VN usage of IP Multicast mechanisms from TS 23.316	16.4.0
2020-03	SP#87E	SP-200075	2029	4	F	Usage of Ethernet PDU Session Information to support 5G VN Group point to point Ethernet traffic	16.4.0
2020-03	SP#87E	SP-200072	2030	1	F	Criteria for I-SMF (and V-SMF) selection and change including also ATSSS cases	16.4.0
2020-03	SP#87E	SP-200078	2031	1	F	Support of TNAP identifier when the Trusted Access does not correspond to WLAN	16.4.0
2020-03	SP#87E	SP-200069	2032	3	F	ATSSS capabilities cooperation between the UE and UPF	16.4.0
2020-03	SP#87E	SP-200068	2033	4	F	Access type and RAT type per Non-3GPP accesses	16.4.0
2020-03	SP#87E	SP-200062	2035	-	F	Service Gap Control handling at UE side during IWK	16.4.0
2020-03	SP#87E	SP-200069	2036	2	F	Corrections for handling of serving networks not supporting ATSSS	16.4.0
2020-03	SP#87E	SP-200078	2038	2	F	Requested NSSAI provided at the AS layer	16.4.0
2020-03	SP#87E	SP-200071	2040	1	F	Clarification on pending NSSAI in Network Slice-Specific Authentication and Authorization	16.4.0
2020-03	SP#87E	SP-200075	2042	4	F	Item #5 Support of emergency services for Rel-16 UE not supporting CAG in CAG cells	16.4.0
2020-03	SP#87E	SP-200069	2044	1	F	Clarification the deregistration in single access	16.4.0
2020-03	SP#87E	SP-200075	2046	2	F	Clarification of N2 based handover considering CAG IDs supported by the target NG-RAN node	16.4.0
2020-03	SP#87E	SP-200068	2047	1	F	TS23.501 - Correction on User Location Information	16.4.0
2020-03	SP#87E	SP-200072	2048	-	F	Paging Policy Differentiation	16.4.0
2020-03	SP#87E	SP-200075	2050	2	F	TSN CN PDB	16.4.0
2020-03	SP#87E	SP-200069	2051	-	F	Access availability report configuration in the UPF	16.4.0
2020-03	SP#87E	SP-200062	2053	3	B	Assistance indication for WUS grouping	16.4.0
2020-03	SP#87E	SP-200078	2054	2	F	Correction on MDBV and CN PDB	16.4.0
2020-03	SP#87E	SP-200078	2056	2	F	Default ARP values for dedicated QoS Flows	16.4.0
2020-03	SP#87E	SP-200078	2057	1	F	Correction of ARP description	16.4.0
2020-03	SP#87E	SP-200078	2060	4	F	Clarification on the EBI context if target MME does not support EBI extension during 5GS to EPS mobility	16.4.0
2020-03	SP#87E	SP-200075	2064	3	F	Item#4: Clarification on the PSFP and Qbv for TSC traffic	16.4.0
2020-03	SP#87E	SP-200075	2067	1	F	Clarifying TSCAI based on TSN clock used by PSFP gate operation	16.4.0
2020-03	SP#87E	SP-200075	2069	5	F	Clarifying UL configuration issue	16.4.0
2020-03	SP#87E	SP-200075	2070	2	F	Traffic Forwarding issue at UPF side	16.4.0
2020-03	SP#87E	SP-200075	2073	2	F	#1_Clarification for supporting 5G VN group communication	16.4.0
2020-03	SP#87E	SP-200076	2074	3	F	#2_clarification on N6-based traffic forwarding of 5GLAN	16.4.0
2020-03	SP#87E	SP-200069	2079	1	F	Clarification on multiple PDU Session anchors for a MA PDU Session	16.4.0
2020-03	SP#87E	SP-200076	2084	3	F	Correction to Emergency services support by SNPN	16.4.0
2020-03	SP#87E	SP-200076	2085	4	F	Correction to TSN stream aggregation and QoS parameter mapping guidelines	16.4.0
2020-03	SP#87E	SP-200078	2087	1	F	Clarification on the use of reference points N14 and N26	16.4.0
2020-03	SP#87E	SP-200062	2088	1	F	NAS signalling of CP Relocation Indication Truncated 5G-S-TMSI Parameters	16.4.0
2020-03	SP#87E	SP-200062	2089	3	F	Correction for MO Exception Data Rate and its inclusion in charging information	16.4.0
2020-03	SP#87E	SP-200076	2097	2	F	Correction to Access SNPN via PLMN	16.4.0
2020-03	SP#87E	SP-200060	2100	1	A	Alignment with SA5 on Charging for SMS over NAS	16.4.0
2020-03	SP#87E	SP-200064	2102	1	F	NEF service to support location transfer	16.4.0
2020-03	SP#87E	SP-200074	2106	2	F	UCMF provisioning correction	16.4.0
2020-03	SP#87E	SP-200078	2108	3	F	Clarification on the CN tunnel info allocation and release	16.4.0
2020-03	SP#87E	SP-200078	2109	2	F	Clarification on internal group ID usage	16.4.0
2020-03	SP#87E	SP-200065	2111	2	F	Update of the binding related descriptions	16.4.0

2020-03	SP#87E	SP-200074	2116	1	F	On UCMF discovery	16.4.0
2020-03	SP#87E	SP-200074	2117	-	F	RACS and NB-IoT corrections	16.4.0
2020-03	SP#87E	SP-200067	2122	2	F	Correction for the wrongly implemented CR1785r8	16.4.0
2020-03	SP#87E	SP-200067	2123	5	F	Corrections of Alternative QoS Profiles - proper TS version	16.4.0
2020-03	SP#87E	SP-200062	2128	1	F	Sending EPS APN rate control information during PDU session establishment	16.4.0
2020-03	SP#87E	SP-200078	2132	-	F	Correction to Reference Points for Non-3GPP Access	16.4.0
2020-03	SP#87E	SP-200076	2133	1	F	Clarification of TSN stream and traffic class	16.4.0
2020-03	SP#87E	SP-200078	2136	1	F	Correction to UE configuration update procedure conditions for re-registration	16.4.0
2020-03	SP#87E	SP-200076	2137	1	F	Selecting network for Emergency services	16.4.0
2020-03	SP#87E	SP-200070	2140	1	F	Corrections to UE mobility event notification	16.4.0
2020-03	SP#87E	SP-200069	2141	-	F	QoS handling of MA PDU Session for interworking with N26	16.4.0
2020-03	SP#87E	SP-200076	2143	1	F	Correct the transfer and determination of the bridge delay related parameters	16.4.0
2020-03	SP#87E	SP-200062	2147	1	F	PDU Session release when Control Plane Only indication becomes not applicable	16.4.0
2020-03	SP#87E	SP-200062	2148	1	F	Correction on PTW determincation	16.4.0
2020-03	SP#87E	SP-200069	2150	-	F	Correction on MA PDU Session request indication	16.4.0
2020-03	SP#87E	SP-200067	2154	1	F	Update N4 rules to support QoS Monitoring and ATSSS	16.4.0
2020-03	SP#87E	SP-200081	2157	-	F	Subscription based access restriction for E-UTRA in unlicensed	16.4.0
2020-03	SP#87E	SP-200062	2158	1	F	Subscription based access restriction for LTE-M	16.4.0
2020-03	SP#87E	SP-200070	2159	1	F	Clarification on NWDAF information maintained in NRF	16.4.0
2020-03	SP#87E	SP-200062	2160	1	F	Missing capabilities in 5GMM Capability IE	16.4.0
2020-03	SP#87E	SP-200074	2161	-	D	Editorial updates in RACS clauses	16.4.0
2020-03	SP#87E	SP-200062	2163	-	D	Mega CR on editorial corrections for 5G_CIoT	16.4.0
2020-03	SP#87E	SP-200076	2164	1	F	Correction to network selection with multiple subscribed SNPNs	16.4.0
2020-03	SP#87E	SP-200076	2165	1	F	Clarification for Support for multiple TSN working domains	16.4.0
2020-03	SP#87E	SP-200072	2169	1	F	ETSUN related CR for non-FASMO corrections	16.4.0
2020-03	SP#87E	SP-200076	2171	-	F	Adding reference points in the Architecture to support Time Sensitive Communication	16.4.0
2020-03	SP#87E	SP-200076	2172	1	F	UPF selection based on traffic classes and VLAN	16.4.0
2020-03	SP#87E	SP-200060	2175	1	A	UE capability match request during the registration procedure	16.4.0
2020-03	SP#87E	SP-200076	2178	-	F	Replace IEEE802.1Qbv with IEEE802.1Q	16.4.0
2020-03	SP#87E	SP-200076	2183	1	F	Correction on QoS Flow Binding about TSN	16.4.0
2020-03	SP#87E	SP-200068	2186	-	F	Correction for support of N5CW devices to access 5GC via trusted WLAN access networks	16.4.0
2020-03	SP#87E	SP-200065	2190	1	F	Endpoint Address correction	16.4.0
2020-03	SP#87E	SP-200078	2191	1	F	Clarification on PS Data Off for non-3GPP access PDU Session	16.4.0
2020-03	SP#87E	SP-200071	2192	1	F	Handling of NSSAA during N2 handover procedure	16.4.0
2020-03	SP#87E	SP-200076	2194	1	F	Clear description of Access to an SNPN	16.4.0
2020-03	SP#87E	SP-200078	2195	1	F	AMF Management	16.4.0
2020-03	SP#87E	SP-200076	2197	1	F	Vertical_LAN 5GLAN related CR for non-FASMO corrections	16.4.0
2020-03	SP#87E	SP-200076	2198	1	F	Vertical_LAN TSN related CR for non-FASMO corrections	16.4.0
2020-03	SP#87E	SP-200076	2199	-	F	Vertical_LAN NPN related CR for non-FASMO corrections	16.4.0
2020-03	SP#87E	SP-200078	2201	1	F	Correction on area of interest used by SMF	16.4.0
2020-03	SP#87E	SP-200076	2202	1	F	TSN working domain and aggregation	16.4.0
2020-03	SP#87E	SP-200076	2204	1	F	Updates for Bridge Delay information reporting and QoS mapping	16.4.0
2020-03	SP#87E	SP-200076	2205	-	F	Incorrect reference to IEEE 1588 Timestamp data type in normative Annex H.2	16.4.0
2020-03	SP#87E	SP-200078	2209	1	F	Clarification on network instance determination	16.4.0
2020-03	SP#87E	SP-200076	2212	1	F	UPF selection based on TSN parameters and context correction	16.4.0
2020-03	SP#87E	SP-200068	2214	1	F	Inclusion of Requested NSSAI in AN Parameters for non-3GPP access	16.4.0
2020-03	SP#87E	SP-200068	2216	1	F	5WWC related CR for non-FASMO corrections	16.4.0
2020-03	SP#87E	SP-200293	2179	3	F	Change of the restriction of enhanced coverage	16.4.0
2020-07	SP#88E	SP-200433	2131	2	F	Support of ETSUN and ATSSS	16.5.0
2020-07	SP#88E	SP-200424	2138	2	F	Selection of direct vs indirect communication	16.5.0
2020-07	SP#88E	SP-200428	2153	1	F	Steering modes for GBR traffic	16.5.0
2020-07	SP#88E	SP-200438	2170	2	F	QoS container vs. TSCAI input container	16.5.0
2020-07	SP#88E	SP-200438	2217	1	F	Fix terminology on maximum number of CAGs per cell instead of per NG-RAN node	16.5.0
2020-07	SP#88E	SP-200425	2222	1	F	Update of QoS monitoring for URLLC based on RAN WG3 decision	16.5.0
2020-07	SP#88E	SP-200438	2223	1	F	Clarification on the supported and non-supported features and services for SNPN	16.5.0
2020-07	SP#88E	SP-200438	2224	1	F	SMF to request the UE IP address from the DN-AAA server based on subscription information	16.5.0
2020-07	SP#88E	SP-200433	2225	1	F	Support of ETSUN within and between PLMN(s)	16.5.0
2020-07	SP#88E	SP-200438	2227	1	F	TSN QoS information for DL traffic	16.5.0
2020-07	SP#88E	SP-200437	2232	-	F	Common Network Exposure	16.5.0
2020-07	SP#88E	SP-200438	2234	1	F	Alignment of traffic forwarding information	16.5.0

2020-07	SP#88E	SP-200436	2236	1	F	Missing the Radio Capability Filtering linkage to the UE Radio Capability ID	16.5.0
2020-07	SP#88E	SP-200552	2238	1	F	ARP values for additional QoS Flows	16.5.0
2020-07	SP#88E	SP-200428	2240	-	F	Handling of mobility when target does not support ATSSS	16.5.0
2020-07	SP#88E	SP-200420	2242	-	A	UE radio capability retrieval	16.5.0
2020-07	SP#88E	SP-200438	2246	1	F	QoS parameters mapping: GFBR, ARP	16.5.0
2020-07	SP#88E	SP-200438	2247	1	F	UPF selection criteria	16.5.0
2020-07	SP#88E	SP-200438	2248	-	F	Missing change in Annex I	16.5.0
2020-07	SP#88E	SP-200438	2251	1	F	Correction on the derived MDBV	16.5.0
2020-07	SP#88E	SP-200436	2254	-	F	Correction on the interface N58 b/w NEF and AF	16.5.0
2020-07	SP#88E	SP-200436	2255	1	F	Support of multiple radio capability formats	16.5.0
2020-07	SP#88E	SP-200436	2257	1	F	Clarification on Version ID	16.5.0
2020-07	SP#88E	SP-200428	2258	1	F	Corrections to steering modes	16.5.0
2020-07	SP#88E	SP-200438	2263	1	F	NF selection in SNPN 5GC	16.5.0
2020-07	SP#88E	SP-200432	2268	1	F	Handling of pending NSSAI	16.5.0
2020-07	SP#88E	SP-200424	2269	2	F	Enablers for multiple SCPs (23.501)	16.5.0
2020-07	SP#88E	SP-200432	2270	1	F	Removal of service area for UE registration with empty Allowed NSSAI due to pending NSSAA	16.5.0
2020-07	SP#88E	SP-200424	2271	1	F	Corrections to Principles for Binding, Selection and Reselection	16.5.0
2020-07	SP#88E	SP-200432	2274	1	F	Clarification for the NSSAI in NSSAA procedure of roaming scenario	16.5.0
2020-07	SP#88E	SP-200428	2276	1	F	MA-PDU Session establishment in Non-allowed Area	16.5.0
2020-07	SP#88E	SP-200422	2277	1	F	Small data rate control enforcement of normal and exception data	16.5.0
2020-07	SP#88E	SP-200438	2278	1	F	Correcting 5GS TSN bridge delays	16.5.0
2020-07	SP#88E	SP-200430	2279	1	F	Corrections to HSS Discovery	16.5.0
2020-07	SP#88E	SP-200438	2285	-	F	Annex I Clarification	16.5.0
2020-07	SP#88E	SP-200438	2287	1	F	Bridge Management Clarification	16.5.0
2020-07	SP#88E	SP-200428	2292	1	F	Correction on ATSSS rule generation	16.5.0
2020-07	SP#88E	SP-200425	2293	1	F	Correction of RAN part of packet delay for QoS monitoring	16.5.0
2020-07	SP#88E	SP-200420	2299	1	A	Incorrect NOTE 14 for 5QI 3	16.5.0
2020-07	SP#88E	SP-200422	2302	1	F	Corrections to restriction of use of Enhanced Coverage	16.5.0
2020-07	SP#88E	SP-200428	2303	1	F	Corrections related to UPF support of RTT measurements without PMF	16.5.0
2020-07	SP#88E	SP-200438	2305	1	F	Correction on RAN sharing for NPN networks	16.5.0
2020-07	SP#88E	SP-200427	2308	1	F	Correction on RAT type	16.5.0
2020-07	SP#88E	SP-200427	2309	-	F	Correction on wireline access and reference point between N5CW device and TWAP	16.5.0
2020-07	SP#88E	SP-200552	2311	1	C	Remove restriction for support of eCall over NR	16.5.0
2020-07	SP#88E	SP-200433	2315	1	F	Pause of Charging	16.5.0
2020-07	SP#88E	SP-200438	2319	1	F	Alignment on Identifying PDU session in TSN AF	16.5.0
2020-07	SP#88E	SP-200438	2321	1	F	Clarification on the bridge delay	16.5.0
2020-07	SP#88E	SP-200428	2327	-	F	Correction of reference to mptcp RFC8684	16.5.0
2020-07	SP#88E	SP-200438	2334	1	F	Clarify the 5GS Bridge ID	16.5.0
2020-07	SP#88E	SP-200432	2336	-	F	Correction on the value of S-NSSAIs for NSSAA	16.5.0
2020-07	SP#88E	SP-200551	2338	1	F	Correction on description about area of interest	16.5.0
2020-07	SP#88E	SP-200551	2339	1	F	Reordering DL data during SR procedure	16.5.0
2020-07	SP#88E	SP-200438	2340	1	F	Correction for TSCAI Calculation	16.5.0
2020-07	SP#88E	SP-200551	2341	-	F	Correction on QoS handling for priority sessions	16.5.0
2020-07	SP#88E	SP-200438	2344	1	F	Correction of the gPTP domain and the selection of UPF	16.5.0
2020-07	SP#88E	SP-200438	2346	1	F	Update on 5G VN group subscription data retrieval	16.5.0
2020-07	SP#88E	SP-200551	2347	1	F	Update on IPUPS functionality	16.5.0
2020-07	SP#88E	SP-200438	2348	1	F	Support of 5G LAN-type service under ETSUN architecture	16.5.0
2020-07	SP#88E	SP-200551	2350	-	F	Correction on AF influence on traffic routing	16.5.0
2020-07	SP#88E	SP-200551	2351	1	F	Correction on Control and User Plane Protocol Stacks	16.5.0
2020-07	SP#88E	SP-200438	2352	1	F	Support of emergency services for Rel-15 UE in CAG cells	16.5.0
2020-07	SP#88E	SP-200424	2353	1	F	Update of NF profile	16.5.0
2020-07	SP#88E	SP-200438	2363	1	F	VLAN Information configuration and information exchange	16.5.0
2020-07	SP#88E	SP-200433	2365	1	F	MA PDU Session not supported in ETSUN case	16.5.0
2020-07	SP#88E	SP-200515	2230	2	F	Spliting port management information into port- and bridge-specific information	16.5.0
2020-07	SP#88E	SP-200438	2135	5	F	Updating the UE with new CAG information	16.5.0
2020-07	SP#88E	SP-200588	2370	2	F	Alignment on Alternative QoS Profile (This CR was noted, corrected to implement CR2730R1 in v16.5.1)	16.5.0
2020-07	SP#88E	SP-200420	1732	5	A	Reflective QoS	16.5.0
2020-07	SP#88E	SP-200422	2243	3	F	Service Area Restriction clarification	16.5.0
2020-07	SP#88E	SP-200610	2361	3	F	PDU Session release when Control Plane Only indication is not available	16.5.0
2020-07	SP#88E	SP-200432	2368	1	F	PCO support for DNS over (D)TLS (avoiding attacks against DNS traffic)	16.5.0
2020-07	SP#88E	SP-200427	2369	1	F	Clarification of the Support of the Frame Routing Feature	16.5.0
2020-07	SP#88E	SP-200433	2371	1	F	URLLC - TSN interworking with ETSUN	16.5.0

2020-07	SP#88E	SP-200432	2372	-	F	Replacing AUSF by NSSAAF to support NSSAA	16.5.0
2020-07	SP#88E	SP-200422	2374	-	F	Removal of I-NEF	16.5.0
2020-07	SP#88E	SP-200422	2378	1	F	UE specific DRX for NB-IoT RAN support clarification based on LS R2-2004057	16.5.0
2020-07	SP#88E	SP-200434	2379	1	F	Capability for HPLMN to understand whether or not the NG-RAN node supports Alternative QoS Profiles	16.5.0
2020-07	SP#88E	SP-200438	2380	2	F	Handling manipulation of CAG by VPLMN -Sol 1	16.5.0
2020-07	SP#88E	SP-200435	2382	1	F	IAB support in NPN deployment	16.5.0
2020-08	SP#88E	SP-200434	2370	1	F	Alignment on Alternative QoS Profile (Correction to implemention of CR2730R2 from v16.5.0)	16.5.1

History

Document history		
V16.5.0	July 2020	Publication (withdrawn)
V16.5.1	September 2020	Publication