ETSI TS 123 503 V16.14.0 (2023-04)

5G;
Policy and charging control framework
for the 5G System (5GS);
Stage 2
(3GPP TS 23.503 version 16.14.0 Release 16)

Reference
RTS/TSGS-0223503vge0

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 https://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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 6
Introduction 6
1 Scope 7
2 References 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 11
4 High level architectural requirements 11
4.1 General requirements 11
4.2 Non-session management related policy control requirements 12
4.2.1 Access and mobility related policy control requirements 12
4.2.2 UE policy control requirements 12
4.2.3 Network analytics information requirements 12
4.2.4 Management of packet flow descriptions 12
4.2.5 SMF selection management related policy control requirements 12
4.2.6 Support for non-session management related network capability exposure 13
4.3 Session management related policy control requirements 13
4.3.1 General requirements 13
4.3.2 Charging related requirements 14
4.3.2.1 General 14
4.3.2.2 Charging models 14
4.3.2.3 Charging requirements 14
4.3.2.4 Examples of Service Data Flow Charging 15
4.3.3 Policy control requirements 15
4.3.3.1 Gating control requirements 15
4.3.3.2 QoS control requirements 15
4.3.3.2.1 QoS control at service data flow level 15
4.3.3.2.2 QoS control at QoS Flow level 15
4.3.3.2.3 QoS control at PDU Session level 16
4.3.3.3 Subscriber spending limits requirements 16
4.3.4 Usage monitoring control requirements 16
4.3.5 Application detection and control requirements 17
4.3.6 Support for session management related network capability exposure 17
4.3.7 Traffic steering control 17
5 Architecture model and reference points 17
5.1 General 17
5.2 Reference architecture 18
5.2.1 Non-roaming architecture 18
5.2.2 Roaming architecture 19
5.2.3 Void 21
5.3 Service-based interfaces and reference points 21
5.3.1 Interactions between PCF and AF 21
5.3.2 Interactions between PCF and SMF 21
5.3.3 Interactions between PCF and AMF 21
5.3.4 Interactions between V-PCF and H-PCF 22
5.3.5 Interactions between PCF and UDR 22
5.3.6 Interactions between SMF and CHF 22
5.3.7 Void 23
5.3.8 Interactions between PCF and CHF 23

5.3.9 Interactions between SMF and NEF 23
5.3.10 Interactions between NEF and PCF 23
5.3.11 Interactions between NWDAF and PCF 24

6 Functional description 24
6.1 Overall description 24
6.1.1 General 24
6.1.1.1 PCF Discovery and Selection 24
6.1.1.2 Binding an AF request targeting an UE address to the relevant PCF 24
6.1.1.2.1 General 24
6.1.1.2.2 The Binding Support Function (BSF) 25
6.1.1.3 Policy decisions based on network analytics 26
6.1.2 Non-session management related policy control 27
6.1.2.1 Access and mobility related policy control 27
6.1.2.2 UE policy control 28
6.1.2.2.1 General 28
6.1.2.2.2 Distribution of the policies to UE 29
6.1.2.3 Management of packet flow descriptions 31
6.1.2.3.1 PFD management 31
6.1.2.3.2 Packet Flow Description 33
6.1.2.4 Negotiation for future background data transfer 33
6.1.2.5 Policy Control Request Triggers relevant for AMF 35
6.1.3 Session management related policy control 37
6.1.3.1 General 37
6.1.3.2 Binding mechanism 37
6.1.3.2.1 General 37
6.1.3.2.2 Session binding 37
6.1.3.2.3 PCC rule authorization 38
6.1.3.2.4 QoS Flow binding 38
6.1.3.3 Reporting 39
6.1.3.4 Credit management 40
6.1.3.5 Policy Control Request Triggers relevant for SMF 41
6.1.3.6 Policy control 49
6.1.3.7 Service (data flow) prioritization and conflict handling 49
6.1.3.8 Termination action 50
6.1.3.9 Handling of packet filters provided to the UE by SMF 50
6.1.3.10 IMS emergency session support 50
6.1.3.11 Multimedia Priority Service support 51
6.1.3.12 Redirection 52
6.1.3.13 Resource sharing for different AF sessions 52
6.1.3.14 Traffic steering control 53
6.1.3.15 Resource reservation for services sharing priority 53
6.1.3.16 3GPP PS Data Off 54
6.1.3.17 Policy decisions based on spending limits 55
6.1.3.18 Event reporting from the PCF 56
6.1.3.19 Mission Critical Services support 59
6.1.3.20 Access Traffic Steering, Switching and Splitting 59
6.1.3.21 QoS Monitoring to assist URLLC Service 60
6.1.3.22 AF session with required QoS 61
6.1.3.23 Support of integration with Time Sensitive Networking 61
6.1.3.24 Policy control for redundant PDU Sessions 62
6.2 Network functions and entities 63
6.2.1 Policy Control Function (PCF) 63
6.2.1.1 General 63
6.2.1.1.1 Session management related functionality 63
6.2.1.1.2 Non-session management related functionality 64
6.2.1.2 Input for PCC decisions 64
6.2.1.3 Policy control subscription information management 67
6.2.1.4 V-PCF 70
6.2.1.5 H-PCF 70
6.2.1.6 Application specific policy information management 71
6.2.1.7 Usage monitoring 71

6.2.1.8 Sponsored data connectivity....72
6.2.2 Session Management Function (SMF)....72
6.2.2.1 General....72
6.2.2.2 Service data flow detection....74
6.2.2.3 Measurement....75
6.2.2.4 QoS control....76
6.2.2.5 Application detection....77
6.2.2.6 Traffic steering....77
6.2.2.7 Access Traffic Steering, Switching and Splitting....77
6.2.3 Application Function (AF)....77
6.2.4 Unified Data Repository (UDR)....78
6.2.5 Charging Function (CHF)....78
6.2.6 Void....78
6.2.7 Network Exposure Function (NEF)....78
6.2.8 Access and Mobility Management Function (AMF)....79
6.2.9 Network Data Analytics Function (NWDAF)....79
6.3 Policy and charging control rule....79
6.3.1 General....79
6.3.2 Policy and charging control rule operations....91
6.4 PDU Session related policy information....92
6.5 Access and mobility related policy information....98
6.6 UE policy information....99
6.6.1 Access Network Discovery & Selection Policy Information....99
6.6.1.1 General....99
6.6.1.2 UE selecting a WLANSP rule....99
6.6.1.3 UE procedure for selecting a WLAN access based on WLANSP rules....100
6.6.2 UE Route Selection Policy information....100
6.6.2.1 Structure Description....100
6.6.2.2 Configuration and Provision of URSP....104
6.6.2.3 UE procedure for associating applications to PDU Sessions based on URSP....104
6.6.3 V2X Policy information....105

Annex A (informative): URSP rules example....106

Annex B (informative): Deployment option to support of BSF and DRA coexistence due to network migration....110

Annex C (Normative): Support for Application Functions supporting Rx interface....111

Annex D (informative): PCC usage for sponsored data connectivity....113

D.1 General....113

D.2 Reporting for sponsored data connectivity....114

Annex E (informative): Change history....115

History....121

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.

Introduction

For references to TS 23.203 [4] made in this document,

- the IP-CAN session of TS 23.203 [4] maps to the PDU Session in 5GC.
- the APN of TS 23.203 [4] maps to DNN in 5GC.
- the IP-CAN bearer of TS 23.203 [4] maps to the QoS Flow in 5GC.
- The PCRF of TS 23.203 [4] maps to the PCF in 5GC.
- The PCEF of TS 23.203 [4] maps to the combination of SMF and UPF in 5GC.
- The BBF shall be considered as being located in the PCEF.
- TDF related description does not apply.
- NBIFOM related description does not apply.

1 Scope

The present document defines the Stage 2 policy and charging control framework for the 5G System specified in TS 23.501 [2] and TS 23.502 [3].

The policy and charging control framework encompasses the following high level functions:

- Flow Based Charging for network usage, including charging control and online credit control, for service data flows;
- Policy control for session management and service data flows (e.g. gating control, QoS control, etc.);
- Management for access and mobility related policies;
- Management of UE policy information.

Interworking with E-UTRAN connected to EPC is described in TS 23.501 [2].

TS 23.502 [3] contains the stage 2 procedures and flows for the policy and charging control framework and it is a companion specification to this specification.

TS 32.255 [21] contains the functional description of the converged offline and online charging functionality for the 5G System.

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 23.501: "Technical Specification Group Services and System Aspects; System Architecture for the 5G System".

[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 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 23.179: "Functional architecture and information flows to support mission-critical communication service; Stage 2".

[7] Void.

[8] 3GPP TS 32.240: "Charging management; Charging architecture and principles".

[9] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[10] 3GPP TS 23.161: "Network-Based IP Flow Mobility (NBIFOM); Stage 2".

[11] 3GPP TS 23.261: "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2".

[12] 3GPP TS 23.167: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; IP Multimedia Subsystem (IMS) emergency sessions".

[13] 3GPP TS 29.507: "Access and Mobility Policy Control Service; Stage 3".

[14] Void.

[15] 3GPP TS 22.011: "Service Accessibility".

[16] 3GPP TS 23.221: "Architectural requirements".

[17] 3GPP TS 29.551: "5G System; Packet Flow Description Management Service; Stage 3".

[18] 3GPP TS 32.421: "Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements".

[19] 3GPP TS 24.526: "UE Equipment (UE) policies for 5G System (5GS); Stage 3".

[20] 3GPP TS 32.291: "Charging management; 5G system, Charging service; stage 3".

[21] 3GPP TS 32.255: "Telecommunication management; Charging management; 5G Data connectivity domain charging; Stage 2".

[22] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[23] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[24] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services".

[25] 3GPP TS 23.216: "Single Radio Voice Call Continuity (SRVCC); Stage 2".

[26] 3GPP TS 23.272: "Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2".

[27] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[28] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[29] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[30] 3GPP TS 24.237: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".

[31] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia telephony; Media handling and interaction".

[32] 3GPP TS 29.510: "5G System; Network Function Repository 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], TS 23.501 [2], TS 23.502 [3] 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].

Application detection filter: A logic used to detect packets generated by an application based on extended inspection of these packets, e.g. header and/or payload information, as well as dynamics of packet flows. The logic is entirely internal to a UPF, and is out of scope of this specification.

Application identifier: An identifier referring to a specific application detection filter.

Application service provider: A business entity responsible for the application that is being / will be used by a UE, which may be either an AF operator or has an association with the AF operator.

Authorised QoS: The maximum QoS that is authorised for a service data flow. In the case of an aggregation of multiple service data flows within one QoS Flow, the combination of the "Authorised QoS" information of the individual service data flows is the "Authorised QoS" for the QoS Flow. It contains the 5QI and the data rate.

Binding: The association between a service data flow and the QoS Flow transporting that service data flow.

Binding mechanism: The method for creating, modifying and deleting bindings.

Charging control: The process of associating packets, belonging to a service data flow, to a charging key and applying online charging and/or offline charging, as appropriate.

Charging key: information used by the CHF for rating purposes.

Detected application traffic: An aggregate set of packet flows that are generated by a given application and detected by an application detection filter.

Dynamic PCC Rule: a PCC rule, for which the definition is provided to the SMF by the PCF.

Gating control: The process of blocking or allowing packets, belonging to a service data flow / detected application's traffic, to pass through to the UPF.

Monitoring key: information used by the SMF and PCF for usage monitoring control purposes as a reference to a given set of service data flows or application (s), that all share a common allowed usage on a per UE and DNN basis.

Non-3GPP access network selection information: It consists of ePDG identifier configuration, N3IWF identification and non-3GPP access node selection information, as defined in clause 6.3.6.1 in TS 23.501 [2].

Non-Seamless Offload: A capability of the UE to access the data networks via non-3GPP access (e.g. WLAN radio access) outside of a PDU Session.

Operator-controlled service: A service for which complete PCC rule information, including service data flow filter information, is available in the PCF through configuration and/or dynamic interaction with an AF.

Operating System (OS): Collection of UE software that provides common services for applications.

Operating System Identifier (OSId): An identifier identifying the operating system.

OS specific Application Identifier (OSAppId): An identifier associated with a given application and uniquely identifying the application within the UE for a given operating system.

Packet flow: A specific user data flow from and/or to the UE.

Packet Flow Description (PFD): A set of information enabling the detection of application traffic provided by a 3rd party service provider.

PCC decision: A PCF decision for policy and charging control provided to the SMF (consisting of PCC rules and PDU Session related attributes), a PCF decision for access and mobility related control provided to the AMF, a PCF decision for UE policy information provided to the UE or a PCF decision for background data transfer policy provided to the AF.

PCC rule: A set of information enabling the detection of a service data flow and providing parameters for policy control and/or charging control and/or other control or support information. The possible information is described in clause 6.3.1.

Policy control: The process whereby the PCF indicates to the SMF how to control the QoS Flow. Policy control includes QoS control and/or gating control.

Policy Control Request trigger report: a notification, possibly containing additional information, of an event which occurs that corresponds with a Policy Control Request trigger.

Policy Control Request trigger: defines a condition when the SMF shall interact again with the PCF.

Policy counter: A mechanism within the CHF to track spending applicable to a subscriber.

Policy counter identifier: A reference to a policy counter in the CHF for a subscriber.

Policy counter status: A label whose values are not standardized and that is associated with a policy counter's value relative to the spending limit(s) (the number of possible policy counter status values for a policy counter is one greater than the number of thresholds associated with that policy counter, i.e. policy counter status values describe the status around the thresholds). This is used to convey information relating to subscriber spending from CHF to PCF. Specific labels are configured jointly in CHF and PCF.

Policy Section: A Policy Section is identified by a Policy Section Identifier and consists of one or multiple URSP rule(s) or one or multiple WLANSP rule(s) or non-3GPP access network selection information or a combination of WLANSP rule(s) and non-3GPP access network selection information.

Predefined PCC Rule: a PCC rule that has been provisioned directly into the SMF by the operator.

Redirection: Redirect the detected service traffic to an application server (e.g. redirect to a top-up / service provisioning page).

Service data flow: An aggregate set of packet flows carried through the UPF that matches a service data flow template.

Service data flow filter: A set of packet flow header parameter values/ranges used to identify one or more of the packet flows in the UPF. The possible service data flow filters are defined in clause 6.2.2.2.

Service data flow filter identifier: A scalar that is unique for a specific service data flow (SDF) filter within a PDU Session.

Service data flow template: The set of service data flow filters in a PCC Rule or an application identifier in a PCC rule referring to an application detection filter in the SMF or in the UPF, required for defining a service data flow.

Service identifier: An identifier for a service. The service identifier provides the most detailed identification, specified for flow based charging, of a service data flow. A concrete instance of a service may be identified if additional AF information is available (further details to be found in clause 6.3.1).

Session based service: An end user service requiring application level signalling, which is separated from service rendering.

Spending limit: A spending limit is the usage limit of a policy counter (e.g. monetary, volume, duration) that a subscriber is allowed to consume.

Spending limit report: a notification, containing the current policy counter status generated from the CHF to the PCF.

Subscribed guaranteed bandwidth QoS: The per subscriber, authorized cumulative guaranteed bandwidth QoS which is provided by the UDR to the PCF.

Subscriber category: is a means to group the subscribers into different classes, e.g. gold user, silver user and bronze user.

UE Local Configuration: Information about the association of an application to either a PDU Session or to non-seamless Offload is configured in the Mobile Termination (MT) and in the Terminal Equipment (TE). For example, UE Local Configuration can include operator specific configuration (e.g. operator provided S-NSSAI(s)), or application specific parameters to set up a PDU Session or end user configuration for specific applications.

UE policy information: Policy information preconfigured in the UE and/or provisioned to the UE for access selection (i.e. ANDSP), PDU Session selection (i.e. URSP) and/or V2X communications (i.e. V2XP).

Uplink binding verification: The network enforcement of terminal compliance with the negotiated uplink traffic mapping to QoS Flows.

User Preferences On Non-3GPP Access Selection: The list of configuration parameters provided by a layer (e.g. application) above NAS and used by the UE for access network discovery and selection.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 23.501 [2], TS 23.502 [3], TS 23.316 [27] 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].

AMBR	Aggregated Maximum Bitrate
ANDSP	Access Network Discovery & Selection Policy
ARP	Allocation and Retention Priority
ASP	Application Service Provider
BDT	Background Data Transfer
BSF	Binding Support Function
CHF	CHarging Function
H-PCF	A PCF in the HPLMN
H-UDR	A UDR in the HPLMN
MPS	Multimedia Priority Service
NBIFOM	Network-based IP flow mobility
NSWO	Non-Seamless WLAN Offload
NWDAF	Network Data Analytics Function
OAM	Operation Administration and Maintenance
OCS	Online Charging System
PCC	Policy and Charging Control
PFD	Packet Flow Description
PFDF	Packet Flow Description Function
PRA	Presence Reporting Area
RAN	Radio Access Network
URSP	UE Route Selection Policy
V2XP	V2X Policy
V-PCF	A PCF in the VPLMN
V-UDR	A UDR in the VPLMN
vSRVCC	video Single Radio Voice Call Continuity
WLANSP	WLAN Selection Policy

4 High level architectural requirements

4.1 General requirements

It shall be possible to apply policy and charging control to any kind of 3GPP and non-3GPP accesses defined in TS 23.501 [2].

The policy and charging control framework shall support the roaming scenarios defined in TS 23.501 [2].

The policy and charging control shall be enabled on a per slice instance, per DNN, or per both slice instance and DNN basis.

NOTE: In single PCF deployment, the PCF will provide all mobility, UE access selection and PDU Session related policies that it is responsible for. In deployments where different PCFs support N15 and N7 respectively, no standardized interface between them is required in this release to support policy alignment.

The policy and charging control framework shall fulfil non-session management related requirements as defined in clause 4.2 and session management related requirements as defined in clause 4.3.

4.2 Non-session management related policy control requirements

4.2.1 Access and mobility related policy control requirements

The policy framework shall provide following functionality for the access and mobility enforcement:

- Policy Control Function (PCF) shall support interactions with the access and mobility policy enforcement in the AMF, through service-based interfaces.
- The PCF shall be able to provide Access and Mobility Management related policies to the AMF.
- The PCF shall be able to evaluate operator policies that are triggered by events received from the AMF.

4.2.2 UE policy control requirements

The 5GC shall be able to provide policy information from the PCF to the UE. Such UE policy information includes:

- Access Network Discovery & Selection Policy (ANDSP): It is used by the UE for selecting non-3GPP accesses network.
- UE Route Selection Policy (URSP): This policy is used by the UE to determine how to route outgoing traffic. Traffic can be routed to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session.
- V2X Policy (V2XP): This policy provides configuration parameters to the UE for V2X communication over PC5 reference point or over Uu reference point or both. V2X Policies are defined in TS 23.287 [28].

4.2.3 Network analytics information requirements

The PCF shall be able to collect directly network analytic information from the NWDAF. The NWDAF provides network data analytics (e.g. load level information on a network slice level) to PCF. The PCF shall be able to use those data in its policy decisions. The details are defined in clause 6.1.1.3.

4.2.4 Management of packet flow descriptions

Management of Packet Flow Descriptions (PFDs) refers to the capability to create, update or remove PFDs in the NEF (PFDF) and the distribution from the NEF (PFDF) to the SMF and finally to the UPF. This feature may be used when the UPF is configured to detect a particular application provided by an ASP.

NOTE 1: A possible scenario for the management of PFDs in the SMF is when an application, identified by an application detection filter in the UPF, deploys a new server or a reconfiguration occurs in the ASP network which impacts the application detection filters of that particular application.

NOTE 2: The management of application detection filters in the SMF can still be performed by using operation and maintenance procedures.

NOTE 3: This feature aims for both: to enable accurate application detection at the UPF and to minimize storage requirements for the UPF and the SMF.

The management of PFDs is supported in non-roaming and home-routed scenarios for those ASPs that have a business relation with the home operator.

4.2.5 SMF selection management related policy control requirements

The policy framework may provide following functionality for the SMF selection management for a PDU Session:

- The Policy Control Function (PCF) may support interactions with the SMF selection functionality in the AMF and the PCF may provide SMF selection management related policies to the AMF;
- The PCF may provide a policy to the AMF to contact PCF for performing DNN replacement of specific DNNs;

- The PCF may provide a policy to the AMF to contact PCF for performing DNN replacement for an unsupported DNN.

4.2.6 Support for non-session management related network capability exposure

Support for network capability exposure enables an AF (e.g. an external ASP) to request the following non-session management related policy control functionality from the NEF:

- Management of PFDs as defined in clause 4.2.4 and in clause 4.18 of TS 23.502 [3];
- Negotiations for future background data transfer as defined in clause 6.1.2.4 and in clause 4.16.7 of TS 23.502 [3];
- Applying a previously negotiated background data transfer policy to a UE or group of UEs as defined in clause 6.1.2.4 and in clause 4.15.6.8 of TS 23.502 [3];
- Traffic steering control for AF influenced traffic diversion, as defined in clause 4.3.7 and in clause 5.6.7 of TS 23.501 [2];
- Service specific parameter provisioning for V2X communication (see clause 5.20 of TS 23.501 [2] and clause 4.15.6.7 of TS 23.502 [3]);
- 5G VN group management (see clause 5.29 of TS 23.501 [2] and clause 4.15.6 of TS 23.502 [3]).

4.3 Session management related policy control requirements

4.3.1 General requirements

It shall be possible for the PCC framework to base decisions upon subscription information, Access Type and the RAT Type.

The PCC framework shall perform Gating Control and discard packets that don't match any service data flow of the active PCC rules. It shall also be possible for the operator to define PCC rules, with wild-carded service data flow filters, to allow sending or receiving packets that do not match any service data flow template of any other active PCC rules.

The PCC framework shall allow the charging control to be applied on a per service data flow and on a per application basis, independent of the policy control.

The PCC framework shall have a binding method that allows the unique association between service data flows and specific QoS Flow.

A single service data flow detection shall suffice for the purpose of both policy control and flow based charging.

A PCC rule may be predefined or dynamically provisioned at establishment and during the lifetime of a PDU Session. The latter is referred to as a dynamic PCC rule.

It shall be possible to take a PCC rule into service, and out of service, at a specific time of day, without any PCC interaction at that point in time.

It shall be possible to take DNN-related policy information into service, and out of service, once validity conditions specified as part of the DNN-related policy information are fulfilled or not fulfilled anymore, respectively, without any PCC interaction at that point in time.

PCC shall be enabled on a per DNN basis at the SMF. It shall be possible for the operator to configure the PCC framework to perform charging control, policy control or both for a DNN access.

The PCC framework shall allow the resolution of conflicts which would otherwise cause a subscriber's Subscribed Guaranteed Bandwidth QoS to be exceeded.

It should be possible to use PCC framework for handling IMS-based emergency service.

It shall be possible with the PCC framework, in real-time, to monitor the overall amount of resources that are consumed by a user and to control usage independently from charging mechanisms, the so-called usage monitoring control.

It shall be possible for the PCC framework to provide application awareness even when there is no explicit service level signalling.

The PCC framework shall support making policy decisions based on subscriber spending limits.

The PCC framework shall support making policy decisions for N6 traffic steering.

4.3.2 Charging related requirements

4.3.2.1 General

In order to allow for charging control on service data flow, the information in the PCC rule identifies the service data flow and specifies the parameters for charging control.

For the purpose of charging correlation between service data flow level and application level (e.g. IMS) as well as on-line charging support at the application level, applicable charging identifiers and Access Type identifiers shall be passed from the PCF to the AF, if such identifiers are available.

4.3.2.2 Charging models

The PCC charging shall support the following charging models for charging performed by SMF:

- Volume based charging;
- Time based charging;
- Volume and time based charging;
- Event based charging;
- No charging.

NOTE: The charging model - "No charging" implies that charging control is not applicable, and no charging records are generated.

4.3.2.3 Charging requirements

It shall be possible to apply different rates and charging models depending on a UE's roaming status.

It shall be possible to apply different rates based on the location of a UE.

It shall be possible to apply different rates for specific part of a service, e.g. allow the UE to download a certain volume for one rate, and after this volume has been reached continue with a different rate.

It shall be possible to apply different rates based on the time of day.

It shall be possible to enforce per service data flow, identified by PCC Rule, usage limits on a per UE basis.

It shall be possible to apply different rates depending on the access used to carry a Service Data Flow

It shall be possible to apply an online charging action upon Application Start/Stop events.

It shall be possible to indicate to the SMF that interactions with the CHF are not required for a PCC rule, i.e. to not perform accounting, credit control or recording of usage for the service data flow, in this case no charging information is generated.

4.3.2.4 Examples of Service Data Flow Charging

There are many different services that may be used within a network, including both user-user and user-network services. Service data flows from these services may be identified and charged in many different ways. A number of examples of configuring PCC rules for different service data flows are described below.

EXAMPLE 1: A network server provides an FTP service. The FTP server supports both the active (separate ports for control and data) and passive modes of operation. A PCC rule is configured for the service data flows associated with the FTP server for the user. The PCC rule uses a filter specification for the uplink that identifies packets sent to port 20 or 21 of the IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 20 or 21 of the IP address of the server.

EXAMPLE 2: A network server provides a "web" service. A PCC rule is configured for the service data flows associated with the HTTP server for the user. The PCC rule uses a filter specification for the uplink that identifies packets sent to port 80 of the IP address of the server, and the origination information is wildcarded. In the downlink direction, the filter specification identifies packets sent from port 80 of the IP address of the server.

EXAMPLE 3: An operator has a specific charging rate for user-user VoIP traffic over the IMS. A PCC rule is established for this service data flow. The filter information to identify the specific service data flow for the user-user traffic is provided by the P-CSCF (AF).

4.3.3 Policy control requirements

4.3.3.1 Gating control requirements

Gating control shall be applied by the UPF on a per service data flow basis.

To enable the PCF gating control decisions, the AF shall report session events (e.g. session termination, modification) to the PCF. For example, session termination, in gating control, may trigger the blocking of packets or "closing the gate".

Gating Control applies for service data flows of IP type.

4.3.3.2 QoS control requirements

4.3.3.2.1 QoS control at service data flow level

It shall be possible to apply QoS control on a per service data flow basis in the SMF, applicable for service data flows of both IP type and Ethernet type.

QoS control per service data flow allows the PCC framework to provide the SMF with the authorized QoS to be enforced for each specific service data flow. Criteria such as the QoS subscription information may be used together with policy rules such as, service-based, subscription-based, or predefined PCF internal policies to derive the authorized QoS to be enforced for a service data flow.

It shall be possible to apply multiple PCC rules, without application provided information, using different authorised QoS within a single PDU Session and within the limits of the Subscribed QoS profile.

4.3.3.2.2 QoS control at QoS Flow level

It shall be possible for the PCC framework to support control of QoS reservation procedures (UE-initiated or network-initiated). It shall be possible to determine the QoS to be applied in QoS reservation procedures (QoS control) based on the authorised QoS of the service data flows that are applicable to the QoS Flow and on criteria such as the QoS subscription information, service based policies, and/or predefined PCF internal policies.

It shall be possible for the SMF to determine the authorized QoS of a QoS Flow using the PCC rules associated to the QoS Flow, and the SMF shall be able to notify the PCF if the QoS Flow is removed or the GFBR of a QoS Flow can no longer (or can again) be guaranteed.

It shall be possible for the PCC framework to support control of QoS for the packet traffic of the PDU Session.

The PCC framework shall be able to provide policy control in the presence of NAT devices. This may be accomplished by providing appropriate address and port information to the PCF.

The enforcement of the control for QoS reservation procedures for a QoS Flow shall allow for a downgrading or an upgrading of the requested QoS as part of a UE-initiated QoS Flow establishment and modification. The PCC framework shall be able to provide a mechanism to initiate QoS Flow establishment and modification as part of the QoS control.

The PCC framework shall be able to handle QoS Flows that require a guaranteed bitrate (GBR bearers) and QoS Flows for which there is no guaranteed bitrate (non-GBR bearers).

4.3.3.2.3 QoS control at PDU Session level

It shall be possible for the PCF to provide the authorized Session-AMBR values, default 5QI/ARP combination for PDU Session of IP type, Ethernet type and unstructured type unconditionally or conditionally, i.e. per PDU Session type and/or RAT type.

It shall be possible for the PCF to request a change of the unconditional or conditional authorized Session-AMBR value(s) at a specific point in time.

4.3.3.3 Subscriber spending limits requirements

It shall be possible to enforce policies based on subscriber spending limits. The CHF shall maintain policy counter(s) to track spending for a subscription. These policy counters must be available in the CHF prior to their use over the N28 interface.

NOTE: The mechanism for provisioning the policy counters in the CHF is out of scope of this document.

The PCF shall request information regarding the subscriber's spending from the CHF, to be used as input for dynamic policy decisions for the subscriber, using subscriptions to spending limit reports. The CHF shall make information regarding the subscriber's spending available to the PCF using spending limit reports.

4.3.4 Usage monitoring control requirements

The requirements to monitor, both volume and time usage, and report the accumulated usage of network resources apply for PDU Sessions of type IP and Ethernet.

It shall be possible to apply usage monitoring for the accumulated usage of network resources on a per Session and user basis. This capability is required for enforcing dynamic policy decisions based on the total network usage in real-time.

The PCF that uses usage monitoring for making dynamic policy decisions shall set and send the applicable thresholds to the SMF for monitoring. The usage monitoring thresholds shall be based either on time, or on volume. The PCF may send both thresholds to the SMF. The SMF shall notify the PCF when a threshold is reached and report the accumulated usage since the last report for usage monitoring. If both time and volume thresholds were provided to the SMF, the accumulated usage since last report shall be reported when either the time or the volume thresholds are reached.

NOTE: There are reasons other than reaching a threshold that can cause the SMF to report accumulated usage to the PCF as defined in clause 6.2.2.3.

The usage monitoring capability shall be possible for an individual or a group of service data flow(s), or for all traffic of a PDU Session in the SMF. When usage monitoring for all traffic of a PDU Session is enabled, it shall be possible to exclude an individual SDF or a group of service data flow(s) from the usage monitoring for all traffic of this PDU Session. It shall be possible to activate usage monitoring both to service data flows associated with predefined PCC rules and dynamic PCC rules, including rules with deferred activation and/or deactivation times while those rules are active.

If service data flow(s) need to be excluded from PDU Session level usage monitoring and PDU Session level usage monitoring is enabled, the PCF shall be able to provide the an indication of exclusion from session level monitoring associated with the respective PCC rule(s).

It shall be possible to apply different usage monitoring depending on the access used to carry a Service Data Flow.

4.3.5 Application detection and control requirements

The application detection and control feature comprise the request to detect the specified application traffic, report to the PCF on the start or stop of application traffic and to apply the specified enforcement and charging actions.

The PCF shall instruct the SMF on which applications to detect and whether to report start or stop event to the PCF by activating the appropriate PCC rules in the SMF. Reporting notifications of start and stop of application detection to the PCF may be muted.

The report to the PCF shall include the report is for start or stop, the detected application identifier and, if deducible, the service data flow descriptions for the detected application traffic.

Upon receiving the report from SMF, the PCF may make policy decisions based on the information received and may send the corresponding updated or new PCC rules to the SMF.

In this release of the specification Application Detection and Control applies only to the IP PDU Session types.

4.3.6 Support for session management related network capability exposure

Support for network capability exposure enables an AF (e.g. an external ASP) to request the following session management related policy control functionality from the NEF:

- Set or change a chargeable party at AF session setup (see clauses 4.15.6.4 and 4.15.6.5 of TS 23.502 [3]);
- Set up an AF session with required QoS (see clause 6.1.3.22 and clause 4.15.6.6 of TS 23.502 [3]);
- Transfer of traffic characteristics of Time Sensitive Communication from the TSN AF (see clause 6.1.3.23).

4.3.7 Traffic steering control

Traffic Steering Control refers to the capability to activate/deactivate traffic steering policies from the PCF in the SMF for the purpose of:

- steering the subscriber's traffic to appropriate operator 3rd party service functions (e.g. NAT, antimalware, parental control, DDoS protection) in the N6-LAN or 5G-LAN type of services. This is supported in non-roaming and home-routed scenarios only.
- AF influenced traffic diversion which enables the routing of the user traffic matching the traffic filters provided in the PCC rule to a local Data Network identified by the DNAI per AF request. This is supported in non-roaming and LBO scenarios only, as described in clause 5.6.7 of TS 23.501 [2].

5 Architecture model and reference points

5.1 General

This specification describes the policy and charging control framework for the 5G system. The interaction between network functions is represented in two ways:

- A service-based representation, where network functions enable other authorized network functions to access their services. This representation also includes point-to-point reference points where necessary;
- A reference point representation, which shows that interactions exist between those network functions for which a reference point is depicted between them.

5.2 Reference architecture

5.2.1 Non-roaming architecture

The reference architecture of policy and charging control framework for the 5G System is comprised by the functions of the Policy Control Function (PCF), the Session Management Function (SMF), the User Plane Function (UPF), the Access and Mobility Management Function (AMF), the Network Exposure Functionality (NEF), the Network Data Analytics Function (NWDAF), the Charging Function (CHF), the Application Function (AF) and UDR (Unified Data Repository).

Figure 5.2.1-1 shows the service based representation and Figure 5.2.1-1a shows the reference point representation of the reference architecture of policy and charging control framework for the 5G System.

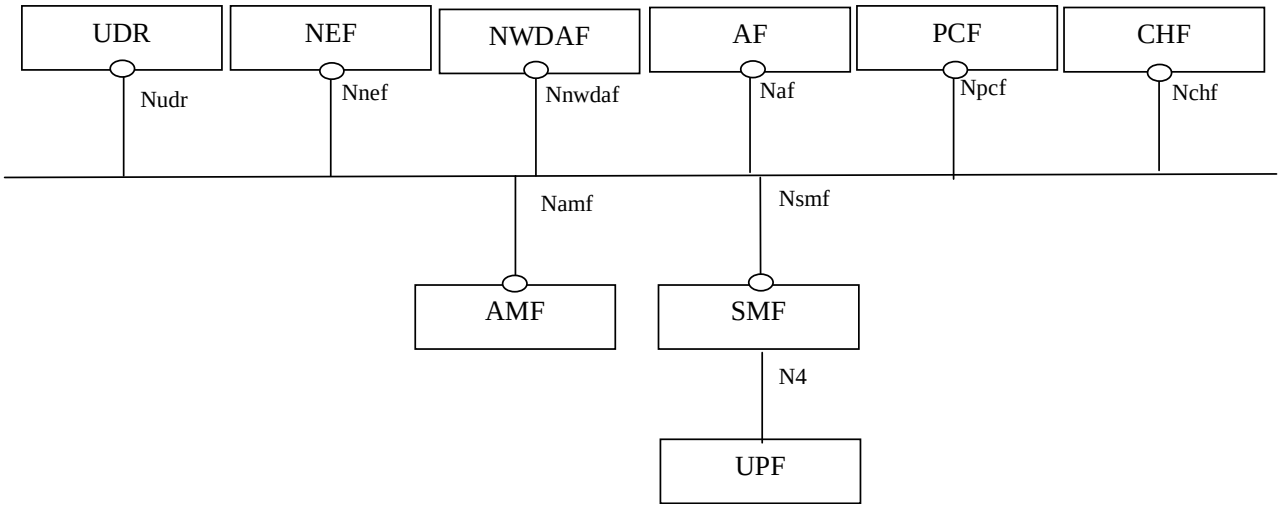

Figure 5.2.1-1: Overall non-roaming reference architecture of policy and charging control framework for the 5G System (service based representation)

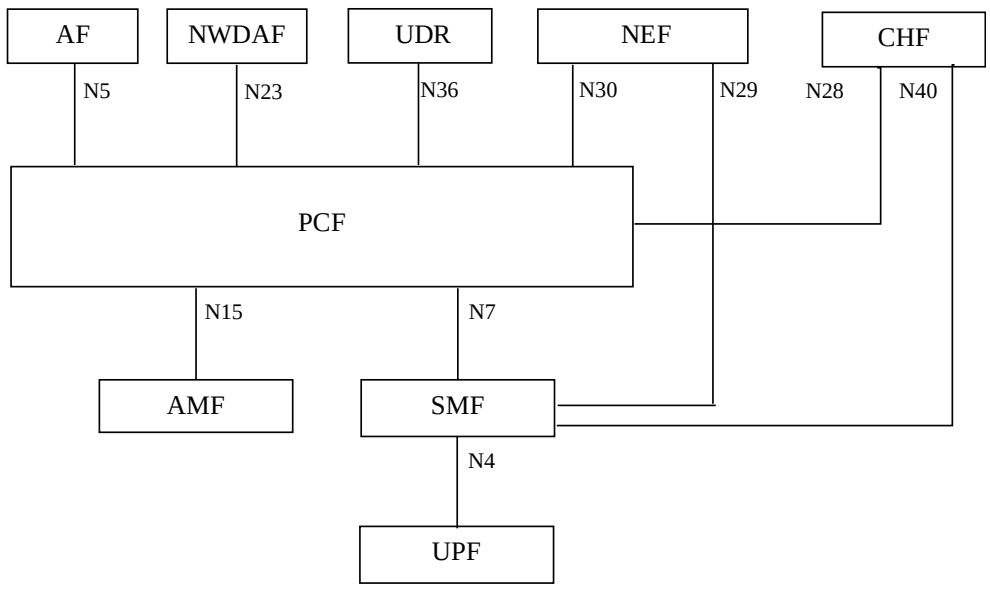

Figure 5.2.1-1a: Overall non-roaming reference architecture of policy and charging control framework for the 5G System (reference point representation)

NOTE 1: The N4 reference point is not part of the 5G Policy Framework architecture but shown in the figures for completeness. See TS 23.501 [2] for N4 reference point definition.

NOTE 2: How the PCF/NEF stores/retrieves information related with policy subscription data or with application data is defined in TS 23.501 [2].

The Nchf service for online and offline charging consumed by the SMF is defined in TS 32.240 [8].

The Nchf service for Spending Limit Control consumed by the PCF is defined in TS 23.502 [3].

5.2.2 Roaming architecture

Figure 5.2.2-1 shows the local breakout roaming policy framework architecture in 5G:

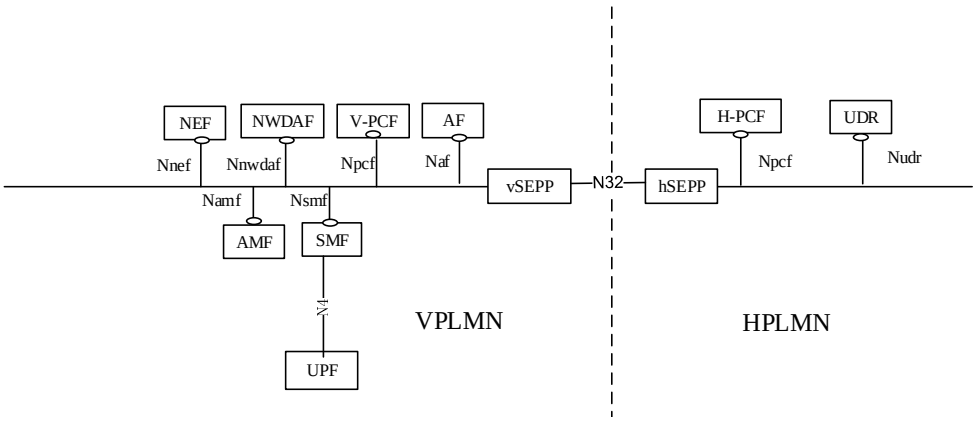

Figure 5.2.2-1: Overall roaming reference architecture of policy and charging control framework for the 5G System - local breakout scenario

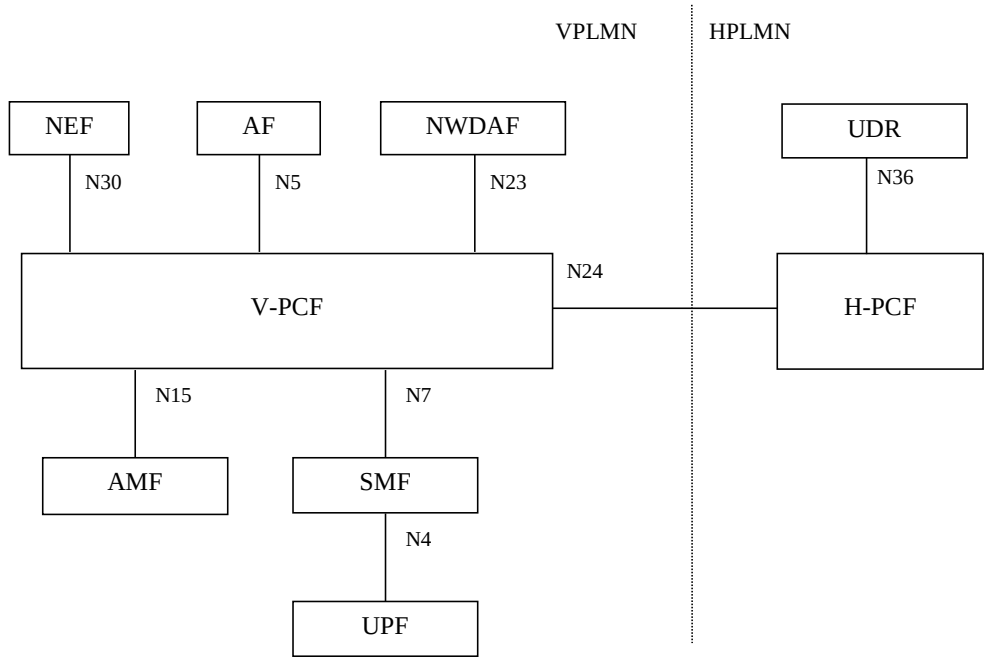

Figure 5.2.2-1a: Overall roaming reference architecture of policy and charging control framework for the 5G System - local breakout scenario (reference point representation)

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 for PCC Rule generation.

NOTE 2: In the LBO architecture, N24 can be used to deliver UE policy information from the PCF in the HPLMN to the PCF in the VPLMN. The PCF in the VPLMN can provide access and motility policy information without contacting the PCF in the HPLMN.

NOTE 3: In the LBO architecture, AF requests providing routing information for roamers targeting a DNN and S-NSSAI (targeting all roamers) or an External-Group-Identifier (identifying a group of roamers) are stored as Application Data in the UDR(in the VPLMN) by the NEF (in the VPLMN).

NOTE 4: For the sake of clarity, SEPPs are not depicted in the roaming reference point architecture figures.

Figure 5.2.2-2 shows the roaming policy framework architecture (home routed scenario) in 5G:

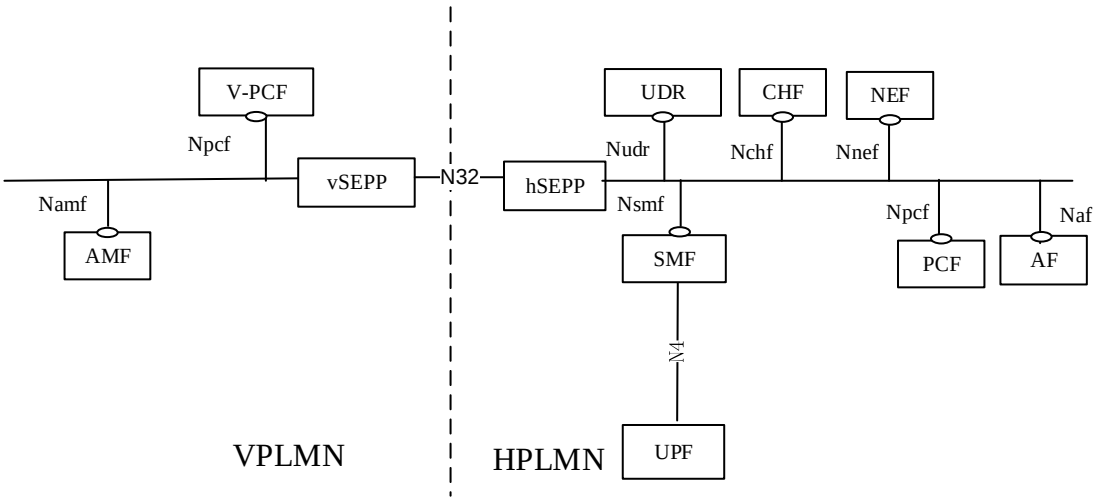

Figure 5.2.2-2: Overall roaming reference architecture of policy and charging control framework for the 5G System - home routed scenario

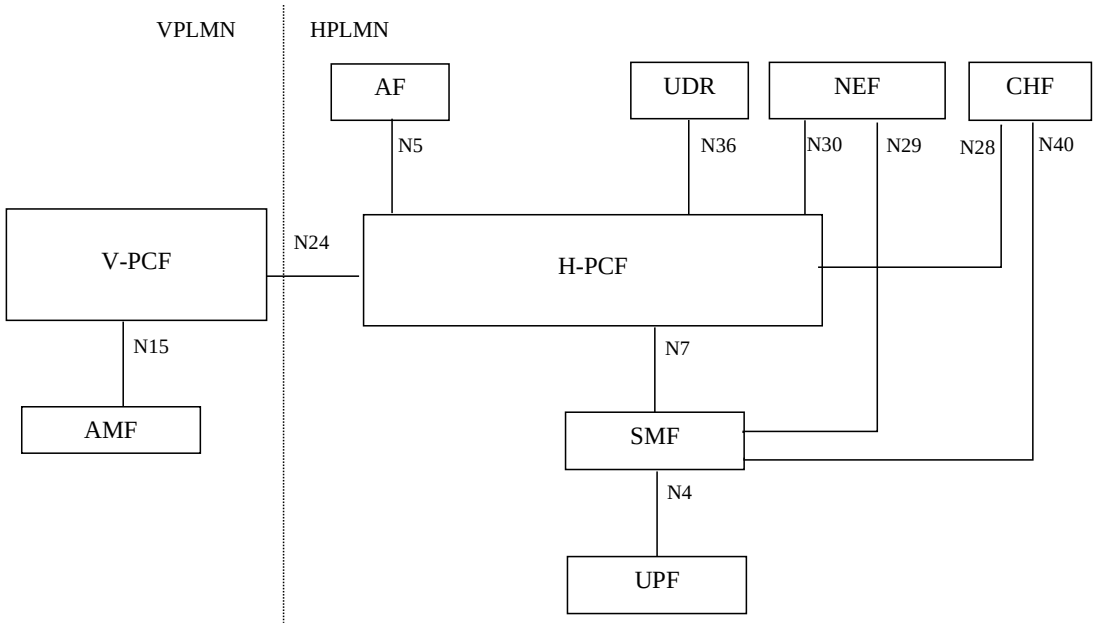

Figure 5.2.2-2a: Overall roaming reference architecture of policy and charging control framework for the 5G System - home routed scenario (reference point representation)

NOTE 5: All functional entities as described in Figure 5.2.1-1 non-roaming scenario, except NWDAF, applies also to the HPLMN in the home routed scenario above.

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

5.2.3 Void

5.3 Service-based interfaces and reference points

5.3.1 Interactions between PCF and AF

Npcf and Naf enable transport of application level session information and Ethernet port management information from AF to PCF. Such information includes, but is not limited to:

- IP filter information or Ethernet packet filter information to identify the service data flow for policy control and/or differentiated charging;
- media/application bandwidth requirements for QoS control;
- In addition, for sponsored data connectivity:
  - the sponsor's identification;
  - optionally, a usage threshold and whether the PCF reports these events to the AF;
  - information identifying the application service provider and application (e.g. SDFs, application identifier, etc.);
- information required to enable Application Function influence on traffic routing as defined in clause 5.6.7 of TS 23.501 [2];
- information required to enable setting up an AF session with required QoS as defined in clause 6.1.3.22;
- information required to enable setting up an AF session with support for Time Sensitive Networking (TSN) as defined in clause 6.1.3.23.

Npcf and Naf enable the AF subscription to notifications on PDU Session events, i.e. the events requested by the AF as described in clause 6.1.3.18 and the change of DNAI as defined in clause 5.6.7 of TS 23.501 [2].

The N5 reference point is defined for the interactions between PCF and AF in the reference point representation.

5.3.2 Interactions between PCF and SMF

Npcf and Nsmf enable the PCF to have dynamic control over the policy and charging behaviour at a SMF.

Npcf and Nsmf enable the signalling of policy and charging control decisions and support the following functionality:

- Creation of a SM Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Request for policy and charging control decision from the SMF to the PCF when a Policy Control Request Trigger related to Session Management has been met;
- Provision of policy and charging control decision from the PCF to the SMF;
- Deletion of a SM Policy Association as defined in clause 4.16 of TS 23.502 [3].

The N7 reference point is defined for the interactions between PCF and SMF in the reference point representation.

5.3.3 Interactions between PCF and AMF

Npcf and Namf enable the PCF to provide Access and Mobility Management related policies to the AMF and support the following functionality:

- Creation of an AM Policy Association as defined in clause 4.16 of TS 23.502 [3];

- Request for access and mobility management related policies from the AMF to the PCF when a Policy Control Request Trigger related to Access and Mobility Management has been met;
- Provision of access and mobility management decision from the PCF to the AMF;
- Deletion of an AM Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Creation of an UE Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Notification of changes to the PCF when a Policy Control Request Trigger related to UE access selection and PDU Session selection has been met;
- Request for DNN replacement from the AMF to the PCF when a Policy Control Request Trigger related to SMF selection management has been met;
- Provision of DNN replacement decision from the PCF to the AMF;
- Deletion of an UE Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Handling of transparent delivery UE policy information from PCF to the UE via the AMF.

The N15 reference point is defined for the interactions between PCF and AMF in the reference point representation.

5.3.4 Interactions between V-PCF and H-PCF

For roaming scenario, the interactions between V-PCF and H-PCF through Npcf enables:

- Creation of an UE Policy Association as defined in clause 4.16 of TS 23.502 [3];
- Relay of notification of changes from the V-PCF in the VPLMN to the H-PCF as defined in clause 4.16 of TS 23.502 [3];
- Provision of UE policy information to the V-PCF in the VPLMN;
- Deletion of an UE Policy Association as defined in clause 4.16 of TS 23.502 [3].

The N24 reference point is defined for the interactions between V-PCF and H-PCF in the reference point representation.

5.3.5 Interactions between PCF and UDR

The Nudr enables the PCF to access policy control related subscription information and application specific information stored in the UDR. The Nudr interface supports the following functions:

- request for policy control related subscription information and application specific information from the UDR;
- provisioning of policy control related subscription information and application specific information to the UDR;
- notifications from the UDR on changes in the policy control related subscription information;
- subscription to the UDR for the AF requests targeting a DNN and S-NSSAI or a group of UEs (roaming UEs for LBO case) identified by an Internal Group Identifier;
- notifications from the UDR on the update of AF requests targeting a DNN and S-NSSAI or a group of UEs (roaming UEs for LBO case) identified by an Internal Group Identifier.

The N36 reference point is defined for the interactions between PCF and UDR in the reference point representation.

5.3.6 Interactions between SMF and CHF

The interactions between SMF and CHF enable online and offline charging.

The N40 reference point is defined for the interactions between SMF and CHF in the reference point representation.

Since the N40 reference point resides between the SMF and CHF in the HPLMN, home routed roaming and non-roaming scenarios are supported in the same manner.

NOTE: The functionality of this interface/reference point is defined in TS 32.240 [8].

5.3.7 Void

5.3.8 Interactions between PCF and CHF

The Nchf enables the PCF to access policy counter status information relating to subscriber spending from CHF and support the following functionality:

- Request for reporting of policy counter status information from PCF to CHF and subscribe to or unsubscribe from spending limit reports (i.e. notifications of policy counter status changes);
- Report of policy counter status information upon a PCF request from CHF to PCF;
- Notification of spending limit reports from CHF to PCF;
- Cancellation of spending limit reporting from PCF to CHF.

The N28 reference point is defined for the interactions between PCF and CHF in the reference point representation.

Since the N28 reference point resides between the PCF and CHF in the HPLMN, home routed roaming and non-roaming scenarios are supported in the same manner.

NOTE: In this Release of the specification, there is no support by the Nchf_SpendingLimitControl service between the PCF in VPLMN and the CHF in the HPLMN.

5.3.9 Interactions between SMF and NEF

Nsmf and Nnef enable transport of PFDs from the NEF (PFDF) to the SMF for a particular application identifier or for a set of application identifiers. It is achieved with the support of the following functionality:

- Creation, updating and removal of individual or the whole set of PFDs from the NEF (PFDF) to the SMF;
- Confirmation of creation, updating and removal of PFDs from the SMF to the NEF (PFDF).

NOTE: The interactions between the SMF and the NEF (PFDF) for transporting PFDs are not related to any PDU Session.

The N29 reference point is defined for the interactions between SMF and NEF (PFDF) in the reference point representation.

5.3.10 Interactions between NEF and PCF

Npcf and Nnef enable the negotiation of policy and charging control behaviour between PCF and NEF by supporting the following functionality:

- service specific policy and charging control;
- sponsor data connectivity including usage monitoring;
- AF-influenced traffic steering authorization;
- subscription and reporting of events for the event exposure;
- negotiations for future background data transfer.

The N30 reference point is defined for the interactions between PCF and NEF in the reference point representation.

5.3.11 Interactions between NWDAF and PCF

The Nnwdaf enables the PCF to subscribe to and be notified on slice load level analytics. The following information are notified by the NWDAF:

- Identifier of network slice instance;
- Load level information of network slice instance.

NOTE: How this information is used by the PCF is not standardized in this release of the specification.

The Nnwdaf enables the PCF to request or subscribe to and be notified on observed service experience (i.e. the average observed Service MoS) as described in clause 6.4 of TS 23.288 [24].

The Nnwdaf enables the PCF to request or subscribe to and be notified on network performance as described in clause 6.6 of TS 23.288 [24].

The Nnwdaf enables the PCF to request or subscribe to and be notified on UE related analytics as described in clause 6.7 of TS 23.288 [24].

The N23 reference point is defined for the interactions between NWDAF and PCF in the reference point representation.

6 Functional description

6.1 Overall description

6.1.1 General

6.1.1.1 PCF Discovery and Selection

The procedures for PCF Discovery and Selection by the AMF and by the SMF are described in TS 23.501 [2].

The procedure to ensure that an AF reaches the PCF selected for a PDU Session is described in clause 6.1.1.2.

6.1.1.2 Binding an AF request targeting an UE address to the relevant PCF

6.1.1.2.1 General

When multiple and separately addressable PCFs have been deployed, a network functionality is required in order to ensure that an AF needing to send policies about UE traffic identified by an UE address can reach over N5 the PCF holding the corresponding PDU Session information. This network functionality has the following characteristics:

- It has information about the user identity, the DNN, the UE (IP or MAC) address(es), the S-NSSAI and the selected PCF address for a certain PDU Session.
  - For IP PDU Session type, it shall receive information when an IP address is allocated or released for a PDU Session.
  - For Ethernet PDU Sessions supporting binding of AF request based on MAC address, it shall receive information when a MAC address is detected as being used by the UE over the PDU Session (this detection takes place at the UPF under control of SMF and is defined in clause 5.8.2 of TS 23.501 [2]). In addition, it receives the DS-TT port MAC address in case of IEEE TSN integration (as described in clause 5.28.2 of TS 23.501 [2]).
- The functionality determines the PCF address and if available the associated PCF instance ID and PCF set ID, selected by the PCF discovery and selection function described in TS 23.501 [2], according to the information provided by the AF or the NEF.

A private IPv4 address may be allocated to different PDU Sessions, e.g.:

- The same UE IPv4 address is allocated to different PDU Sessions to the same DNN and different S-NSSAI;

- The same UE IPv4 address is allocated to different PDU Sessions to the same S-NSSAI and different DNN.

In the case of private IPv4 address being used for the UE, the AF or the NEF may send DNN S-NSSAI, in addition, in Npcf_PolicyAuthorization_Create request and Nbsf_Management_Discovery request. The DNN and S-NSSAI can be used by the PCF for session binding, and they can be also used to help selecting the correct PCF.

6.1.1.2.2 The Binding Support Function (BSF)

The BSF has the following characteristics:

- For a certain PDU Session, the BSF stores internally information about the user identity, the DNN, the UE (IP or MAC) address(es), the S-NSSAI, the selected PCF address and if available the associated PCF instance ID, PCF set ID and the level of binding (see clause 6.3.1.0 of TS 23.501 [2]).

NOTE 1: Only NF instance or NF set Level of Binding indication are supported at the BSF.

- The PCF registers, updates and removes the stored information in the BSF using the Nbsf management service operations defined in TS 23.502 [3].

  - The PCF ensures that it is updated each time an IP address is allocated or de-allocated to the PDU Session or, for Ethernet PDU Sessions supporting binding of AF request based on MAC address, each time it has been detected that a MAC address is used or no more used by the UE in the PDU Session.

  - Based on operator's policies and configuration, the PCF determines whether the same PCF shall be selected for the SM Policy associations to the same UE ID, S-NSSAI and DNN combination in the non-roaming or home-routed scenario.

NOTE 2: This applies to usage monitoring.

- The selected PCF (if needed) downloads the user profile from the UDR as described in clause 4.16.4 step 2 of TS 23.502 [3]. If usage monitoring is enabled for the user, and based on operator's policies, the PCF checks if the BSF has already existing PCF serving the combination of SUPI, S-NSSAI, DNN.

  - If no such PCF is found the PCF shall register itself to the BSF as described above in this clause.

  - Else if an existing PCF is found for the above combination, the PCF shall return to the SMF the available information about the existing PCF and a redirection indication.

NOTE 3: The assumption is that for DNN, S-NSSAI combinations where usage monitoring be applied, the same BSF instance or the same BSF SET is selected for all UE PDU Sessions to the same DNN, S-NNSAI.

- For retrieval binding information, any NF, such as NEF or AF, that needs to discover the selected PCF address(es), and if available, the associated PCF instance ID, PCF set ID and level of binding (see clause 6.3.1.0 of TS 23.501 [2]) for the tuple (UE address, DNN, S-NSSAI, SUPI, GPSI) (or for a subset of this Tuple) uses the Nbsf management service discovery service operation defined in TS 23.502 [3].

- The NF may discover the BSF via NRF or based on local configuration. When registering the NF profile in NRF, the Range(s) of UE IPv4 addresses, Range(s) of UE IPv6 prefixes supported by the BSF and optionally, the DNN list, S-NSSAI(s) or IP domain list as described in TS 29.510 [32], may be provided to NRF.

- If the NF received a PCF set ID or a PCF instance ID with an indication of level of binding as result of the Nbsf management service discovery service operation, it should use that information as NF set level or NF instance level Binding Indication to route requests to the PCF as defined in clause 6.3.1.0 of TS 23.501 [2] and according to the following provisions:

  - For the NF set level of binding, the NF will receive a PCF set ID but no PCF instance ID. If an NF is not able to reach the received PCF address(es) and applies direct discovery, it should query the NRF for PCF instances within the PCF set and select another instance.

  - For the NF instance level of binding, the NF will receive a PCF set ID and a PCF instance ID. If an NF is not able to reach the received PCF address(es) and applies direct discovery, it should query the NRF for PCF service instances within the PCF and select another instance.

- The NF should provide a Routing Binding Indication based on the received PCF set ID, level of binding and possible PCF instance ID in requests it sends to the PCF.

- For an ongoing NF service session, the PCF may provide Binding indication to the NF (see clause 6.3.1.0 of TS 23.501 [2]). This Binding indication shall then be used instead of any PCF information received from the BSF.

- If a new PCF instance is selected, the new PCF should invoke Nbsf_Management_Update service operation to update the binding information in BSF.

The BSF may be deployed standalone or may be collocated with other network functions, such as PCF, UDR, NRF, SMF.

NOTE 4: Collocation allows combined implementation.

6.1.1.3 Policy decisions based on network analytics

Policy decisions based on network analytics allow PCF to perform policy decisions taking into account the analytics information provided by the NWDAF. The PCF subscribes/unsubscribes to Analytics information as defined in TS 23.288 [24].

The following Analytics IDs are relevant for Policy decisions: "Load level information", "Service Experience", "Network Performance" and "Abnormal behaviour". The PCF may subscribe to notifications of network analytics related to "Load Level Information" using the Nnwdaf_AnalyticsSubscription_Subscribe service operation including the Analytics ID "Load level information", the Analytics Filter "S-NSSAI" and the Analytics Reporting Information set to a load level threshold value. The PCF is notified when the load level of the Network Slice Instance reaches the threshold, and then the PCF may verify if the RFSP index value needs to be modified for a SUPI for which an AM Policy Association is created; this is based on operator policies in the PCF, as defined in clause 6.1.2.1.

The PCF may subscribe to notifications of network analytics related to "Service Experience" using the Nnwdaf_AnalyticsSubscription_Subscribe service operation including the Analytics ID "Service Experience", the Target of Analytics Reporting "any UE" and the Analytics Filter including one or more "Application ID(s)". The PCF is notified on the Service Experience statistics or predictions including, for each Application Id, the list of SUPIs for which Service Experience is provided. In addition, both spatial and time validity may be provided as well as the confidence of the prediction. The PCF may check the 5QI values assigned to the Application, the number of UEs affected and may use this as input to calculate and update the authorized QoS for a service data flow template.

The NWDAF service to retrieve the service experience (i.e. the average observed Service MoS) is described in clause 6.4 of TS 23.288 [24].

The PCF may subscribe to notifications of network analytics related to "Network Performance" using the Nnwdaf_AnalyticsSubscription_Subscribe service operation including the Analytics ID "Network Performance", the Target of Analytics Reporting "Internal Group Id" and the Analytics Filter including the Area of Interest. The PCF is notified on the Network Performance statistics or predictions including the Area of Interest. In addition, the confidence of the prediction may be provided. The PCF may use this information as input to calculate the background data transfer policies that are negotiated with the ASP, as defined in clause 6.1.2.4.

The NWDAF services to retrieve "Network Performance" as described in clause 6.6 of TS 23.288 [24].

The PCF may subscribe to notifications of network analytics related to "Abnormal behaviour" using the Nnwdaf_AnalyticsSubscription_Subscribe service operation including the Analytics ID "Abnormal behaviour", the Target of Analytics Reporting "SUPI", "Internal Group Id" or "any UE" and the Analytics Filter including the expected analytics type or the list of Exceptions IDs and per each Exception Id a possible threshold and other Analytics Filter Information if needed. The list of Exception IDs is specified in TS 23.288 [24]. The PCF may use "Unexpected UE location" as input to determine the Service Area Restrictions defined in clause 6.1.2.1, "Suspicion of DDoS attack" or "Too frequent Service Access" to request the SMF to terminate the PDU Session as defined in clause 6.1.3.6, "Wrong destination address" to perform gating of a service data flow as defined in clause 6.1.3.6 and "Unexpected long-live/large rate flows" to perform QoS related policies such as gating or policing as defined in clause 6.2.1.1.

The NWDAF services to retrieve UE related analytics are described in clause 6.7 of TS 23.288 [24].

The PCF may also use the network analytics as input to its policy decision to apply operator defined actions for example for the UE context(s) or PDU Session(s).

6.1.2 Non-session management related policy control

6.1.2.1 Access and mobility related policy control

The access and mobility policy control encompasses the management of service area restrictions, the management of the RFSP functionalities and UE-AMBR, and the management of the SMF selection. This clause defines the management of service area restrictions and RFSP Index for a UE registered over 3GPP access. The management of service area restrictions for a 5G-RG or a FN-CRG using W-5GAN are specified in TS 23.316 [27].

The management of service area restrictions enables the PCF of the serving PLMN (e.g. V-PCF in roaming case) to modify the service area restrictions used by AMF as described in clause 5.3.4 of TS 23.501 [2].

A UE's subscription may contain service area restrictions, which may be further modified by PCF based on operator defined policies at any time, either by expanding a list of allowed TAIs or by reducing a non-allowed TAIs or by increasing the maximum number of allowed TAIs. Operator defined policies in the PCF may depend on input data such as UE location, time of day, information provided by other NFs, etc.

The AMF may report the subscribed service area restrictions received from UDM during Registration procedure or when the AMF changed, the conditions for reporting are that local policies in the AMF indicate that Access and Mobility Control is enable. The AMF reports the subscribed service area restrictions to the PCF also when the policy control request trigger for service area restrictions change, as described in clause 6.1.2.5, is met. The AMF receives the modified service area restrictions from the PCF. The AMF stores them then use it to determine mobility restriction for a UE. The PCF may indicate the AMF that there is an unlimited service area.

The service area restrictions consist of a list of allowed TAI(s) or a list of non-allowed TAI(s) and optionally the maximum number of allowed TAIs.

NOTE 1: The enforcement of the service area restrictions is performed by the UE, when the UE is in CM-IDLE state or in CM-CONNECTED state when in RRC Inactive, and in the RAN/AMF when the UE is in CM-CONNECTED state.

The management of the RFSP Index enables the PCF to modify the RFSP Index used by the AMF to perform radio resource management functionality as described in clause 5.3.4 of TS 23.501 [2]. PCF modifies the RFSP Index based on operator policies that take into consideration e.g. accumulated usage, load level information per network slice instance etc. The subscribed RFSP Index may be further adjusted by the PCF based on operator policies at any time.

For radio resource management, the AMF may report the subscribed RFSP Index received from UDM during the Registration procedure or when the AMF changed. The conditions for reporting are that local policies in the AMF indicate that Access and Mobility Control is enable. The AMF reports the subscribed RFSP Index to the PCF when the subscription to RFSP Index change to the PCF is met. The AMF receives the modified RFSP Index from the PCF.

NOTE 2: The enforcement of the RFSP Index is performed in the RAN.

Upon change of AMF, the source AMF informs the PCF that the UE context was removed in the AMF in the case of inter-PLMN mobility.

The management of UE-AMBR enables the PCF to provide the UE-AMBR information to AMF based on serving network policy. The AMF may report the subscribed UE-AMBR received from UDM. The conditions for reporting are that the PCF provided Policy Control Request Triggers to the AMF to report subscriber UE-AMBR change. The AMF receives the modified UE-AMBR from the PCF. The AMF provides a UE-AMBR value of the serving network to RAN as specified in clause 5.7.2.6 of TS 23.501 [2].

The management of the SMF selection enables the PCF to instruct the AMF to contact the PCF during the PDU Session Establishment procedure to perform a DNN replacement, as specified in clause 5.6.1 of TS 23.501 [2]. To indicate the conditions to check whether to contact the PCF at PDU Session establishment (as specified in clause 6.1.2.5), the PCF provides the Policy Control Request Triggers SMF selection management and, if necessary Change of the Allowed NSSAI, together with SMF selection management related policy control information (see clause 6.5) during UE Registration procedure and at establishment of the AM Policy Association.

The PCF may update SMF selection management information based on PCF local decision or upon being informed about a new Allowed NSSAI. The AMF applies the updated SMF selection management information to new PDU Sessions only, i.e. already established PDU Sessions are not affected.

6.1.2.2 UE policy control

6.1.2.2.1 General

The 5GC shall be able to provide policy information from the PCF to the UE. Such UE policy information includes:

1) Access Network Discovery & Selection Policy (ANDSP): It is used by the UE for selecting non-3GPP accesses and for selection of the N3IWF in the PLMN. The structure and the content of this policy are specified in clause 6.6.1.

2) UE Route Selection Policy (URSP): This policy is used by the UE to determine if a detected application can be associated to an established PDU Session, can be offloaded to non-3GPP access outside a PDU Session, or can trigger the establishment of a new PDU Session. The structure and the content of this policy are specified in clause 6.6.2. A URSP rule includes one Traffic descriptor that specifies the matching criteria and one or more of the following components:

   2a) SSC Mode Selection Policy (SSCMSP): This is used by the UE to associate the matching application with SSC modes.

   2b) Network Slice Selection Policy (NSSP): This is used by the UE to associate the matching application with S-NSSAI.

   2c) DNN Selection Policy: This is used by the UE to associate the matching application with DNN.

   2d) PDU Session Type Policy: This is used by the UE to associate the matching application with a PDU Session Type.

   2e) Non-Seamless Offload Policy: This is used by the UE to determine that the matching application should be non-seamlessly offloaded to non-3GPP access (i.e. outside of a PDU Session).

   2f) Access Type preference: If the UE needs to establish a PDU Session for the matching application, this indicates the preferred Access Type (3GPP or non-3GPP or Multi-Access).

3) V2X Policy (V2XP): This policy provides configuration parameters to the UE for V2X communication over PC5 reference point or over Uu reference point or both. V2X Policies are defined in clause 5.1.2.1 and clause 5.1.3.1 of TS 23.287 [28].

The ANDSP and URSP may be pre-configured in the UE or may be provisioned to UE from PCF. The pre-configured policy shall be applied by the UE only when it has not received the same type of policy from PCF.

The methods of configuring V2XP to the UE, including (pre-)configuration and provisioning, and the priority of the same type of parameters acquired from different sources are defined in clause 5.1.1 of TS 23.287 [28].

The PCF selects the UE policy information applicable for each UE based on local configuration, and operator policies taking into consideration the information defined in clause 6.2.1.2.

In the case of a roaming UE, the V-PCF may retrieve UE policy information from the H-PCF over N24/Npcf. When the UE is roaming and the UE has valid rules from both HPLMN and VPLMN the UE gives priority to the valid ANDSP rules from the VPLMN.

The UE policy information shall be provided from the PCF to the AMF via N15/Namf interface and then from AMF to the UE via the N1 interface as described in clause 4.2.4.3 of TS 23.502 [3]. The AMF shall not change the UE policy information provided by PCF.

The PCF is responsible for delivery of UE policy. If the PCF is notified about UE policy information delivery failure (e.g. because of UE unreachable), the PCF may provide a new trigger "Connectivity state changes" in Policy Control Request Trigger of UE Policy Association to AMF as defined in clause 4.16.12.2 of TS 23.502 [3]. After reception of the Notify message indicating that the UE enters the CM-Connected state, the PCF may retry to deliver the UE policy information.

NOTE 1: For backward compatibility the PCF may subscribe the "Connectivity state changes (IDLE or CONNECTED)" event in Rel-15 AMF as defined in clause 5.2.2.3 of TS 23.502 [3].

If due to UE Local Configurations, a UE application requests a network connection using Non-Seamless Offload, the UE shall use Non-Seamless Offload for this application without evaluating the URSP rules. Otherwise, the UE shall select the PDU Session or Non-Seamless Offload in the following order:

- If the UE has an URSP rule (except the URSP rule with the "match all" Traffic descriptor) that matches the application as defined in clause 6.6.2.3, the UE shall perform the association of the application to the corresponding PDU Session or to Non-Seamless Offload according to this rule; Otherwise,

- If no URSP rule is applicable for the application (except the URSP rule with the "match all" Traffic descriptor), the UE shall perform the association of the application to a PDU Session according to the applicable UE Local Configurations, if any. If the UE attempts to establish a new PDU Session according to the UE Local Configurations and this PDU Session Establishment request is rejected by the network, then the UE shall perform the association of the application to a PDU Session or to Non-Seamless Offload according to the URSP rule with the "match all" Traffic descriptor; Otherwise,

NOTE 2: It is assumed that the S-NSSAI(s) in the UE Local Configurations are operator-provided S-NSSAI(s). The provision of the S-NSSAI(s) is not specified.

NOTE 3: The application layer is not allowed to set the S-NSSAI when the UE establishes a PDU Session based on the UE Local Configurations.

NOTE 4: Any missing information in the UE Local Configurations needed to build the PDU Session Establishment request can be the appropriate corresponding component from the URSP rule with the "match all" Traffic descriptor.

- If neither the UE Local Configurations nor the URSP rules are applicable for the application (except the URSP rule with the "match all" Traffic descriptor), the UE shall perform the association of the application to a PDU Session or to Non-Seamless Offload according to the URSP rule with the "match all" Traffic descriptor.

For the existing PDU Session(s), the UE shall examine the URSP rules within the UE policy information in order to determine whether the existing PDU Session(s) (if any) are maintained or not. If not, then the UE may initiate a PDU Session release procedure for the PDU Session(s) that cannot be maintained.

If there are multiple IPv6 prefixes within the PDU Session, then the IPv6 multi-homed routing rules, described in clause 5.8.2.2.2 in TS 23.501 [2], on the UE shall be used to select which IPv6 prefix to route the traffic of the application.

NOTE 5: For the case that an application cannot be associated to any PDU Session, the UE can inform the application that association of the application to PDU Session fails.

6.1.2.2.2 Distribution of the policies to UE

The UE policy control enables the PCF to provide UE access selection related policy information, PDU Session related policy information and V2X Policy information to the UE, i.e. UE policies, that includes Access network discovery & selection policy (ANDSP) or UE Route Selection Policy (URSP) or V2X Policy (V2XP) or their combinations using Npcf and Namf service operations.

The PCF may be triggered to provide the UE policy information during UE Policy Association Establishment and UE Policy Association Modification procedures as defined in clause 4.16.11 and clause 4.16.12 of TS 23.502 [3].

NOTE 1: The PCF can install a PCC Rule and activate start and stop of application detection in the SMF. When the same PCF is selected for SM policy association control and UE policy association control, the reporting of start and stop of an application can trigger the installation or update of a URSP rule in the UE to send the application traffic to the PDU Session as defined in the URSP rule.

NOTE 2: The PCF can subscribe to the UDR on service specific information change, which will be taken into consideration by the PCF to determine the updated V2XP as defined in clause 4.15.6.7 of TS 23.502 [3].

Operator defined policies in the PCF may depend on input data such as UE location, time of day, information provided by other NFs, etc. as defined in clause 6.2.1.2.

The PCF includes the UE policy information delivered to the UE into a Policy Section identified by a Policy Section Identifier (PSI). The PCF may divide the UE policy information into different Policy Sections, each one identified by a

PSI. Each Policy Section provides a list of self-contained UE policy information to the UE, via AMF. The PCF ensures that a Policy Section is under a predefined size limit, known by the PCF.

NOTE 3: The size limit to allow the policy information to be delivered using NAS transport is specified in TS 29.507 [13]. The size limit is configured in the PCF.

A list of self-contained UE policy information implies that:

- when the PCF delivers URSP rules to the UE, the PCF provides the list of URSP rules in the order of precedence and without splitting a URSP rule across Policy Sections;
- when the PCF delivers V2XP to the UE, the PCF provides the list of V2XP in the order of precedence and without splitting a V2XP across Policy Sections;
- when the PCF delivers WLANSP rules, the list of WLANSP rules are provided in the order of priority and without splitting a WLANSP rule across Policy Sections;
- when the PCF delivers the non-3GPP access network selection information, the whole list of non-3GPP access network selection information (as defined in clause 6.6.1.1) is provided in one Policy Section.

It is up to PCF decision how to divide the UE policy information into Policy Sections as long as the requirements for the predefined size limit and the self-contained content (described above) are fulfilled.

NOTE 4: The Policy Section list can be different per user. One PSI and its corresponding content can be the same for one or more users.

NOTE 5: The PCF may, for example, assign the URSP as one whole Policy Section, or it may subdivide the information in the URSP into multiple Policy Sections by assigning one or several URSP rules to each Policy Section.

The PLMN ID is provided to the UE together with UE policy information and it is used to indicate which PLMN a Policy Section list belongs to.

The AMF forwards the UE policy information transparently to the UE. If the (H-)PCF decides to split the UE policies to be sent to the UE, the PCF provides multiple Policy Sections separately to the AMF and then AMF uses UE configuration Update procedure for transparent UE policies delivery procedure to deliver the policies to the UE, this is defined in clauses 4.2.4.3 and clause 4.16 of TS 23.502 [3].

NOTE 6: The AMF does not need to understand the content of the UE policy, rather send them to the UE for storage.

The UE shall update the stored UE policy information with the one provided by the PCF as follows (details are specified in TS 24.501 [22]):

- If the UE has no Policy Sections with the same PSI, the UE stores the Policy Section;
- If the UE has an existing Policy Section with the same PSI, the UE replaces the stored Policy Section with the received information;
- The UE removes the stored Policy Section if the received information contains only the PSI.

The UE keeps the received UE policies stored even when registering in another PLMN. The number of UE policies to be kept stored in the UE for PLMNs other than the HPLMN is up to UE implementation. If necessary, e.g. the number of UE policies stored in UE for PLMNs exceeds the maximum value, the UE may remove earlier stored UE policy in UE.

The ANDSP for VPLMN, if provided within the UE policy in the UE Configuration Update procedure described in clause 4.2.4.3 of TS 23.502 [3], applies to the equivalent PLMN(s) indicated in the last received list of equivalent PLMNs in Registration Accept.

At Initial Registration or the Registration to 5GS when the UE moves from EPS to 5GS:

- The UE provides the list of stored PSIs which identify the Policy Sections associated to the home PLMN and the visited PLMN (if the UE is roaming) that are currently stored in the UE. If USIM is changed, the UE does not provide any PSI. If no policies are stored in the UE for the home PLMN, the UE does not provide any PSI

associated to the home PLMN. If the UE is roaming and has policies for the home PLMN but no associated policies for the visited PLMN the UE includes only the list of PSIs associated to the home PLMN.

- UE may indicate its ANDSP support to the PCF. If it is received, the PCF shall take it into account for the determination on whether to provide the ANDSP to the UE. The PCF does not provide ANDSP rules to the UE if the UE does not indicate support for ANDSP.

- The UE may also provide the OSId.

The UE may trigger an Initial registration with the list of stored PSIs to request a synchronization for example if the UE powers up without USIM being changed.

During Initial Registration, the (H-)PCF retrieves the list of PSIs and its content stored in the (H-)UDR for this SUPI while the V-PCF (in the roaming scenario) retrieves the list of PSIs and its content stored in the V-UDR for the PLMN ID of this UE (alternatively, the V-PCF can have this information configured locally).

NOTE 7: The PSI list and content stored/configured for a PLMN ID can be structured according to e.g. location areas (e.g. TAs, PRAs). The V-PCF can then provide PSIs and its content only if they correspond to the current UE location.

In the roaming scenario, the V-PCF shall also forward any UE provided PSIs that are associated to the home PLMN to the H-PCF.

When the PCF (i.e. the (H-)PCF as well as the V-PCF) receives a list of PSIs associated to the PLMN of the PCF from the UE, the PCF compares the list of PSIs provided by the UE and the list of PSIs retrieved from the UDR. In addition, the PCF checks whether the list of PSIs provided by the UE or its content needs to be updated according to operator policies, e.g. change of Location and/or time. If the two lists of PSIs are different or an update is necessary according to operator policies (which includes the case that the UE did not provide a list of PSIs associated to the PLMN of the PCF), the PCF provides the changes in the list of PSIs or the corresponding content to the AMF which forwards them to the UE.

The (H-)PCF maintains the latest list of PSIs delivered to each UE as part of the information related to the Policy Association until the UE policy association termination request is received from the AMF. Then the (H-)PCF stores the latest list of PSIs and its contents in the (H-)UDR using the Nudr_DM_Update including DataSet "Policy Data" and Data Subset "Policy Set Entry".

The (H-)PCF may use the PEI provided by the AMF and/or the OSId provided by the UE, to determine the operating system of the UE.

If the PEI, the OSId or the indication of UE support for ANDSP is available to the PCF, the PCF stores them in the UDR using Nudr_DM_Create including DataSet "Policy Data" and Data Subset "UE context policy control data" when such information is received from the UE in the UE Policy Container.

If the (H-)PCF is not able to determine the operating system of the UE, and if the (H-)PCF requires to deliver URSP rules that contain Application descriptors as Traffic Descriptors, then the Traffic Descriptors of such URSP rules include multiple instances of Application descriptors each associated to supported UE operating systems by the network operator implementation.

If the (H-)PCF determines the operating system of the UE and if the (H-)PCF requires to deliver URSP rules that contain Application descriptors as Traffic Descriptors, then the Traffic Descriptors of such URSP rules include the Application descriptors associated with the operating system determined by the PCF.

NOTE 8: If the PCF does not take into account the received PEI and/or OSId then the PCF can send URSP rules containing application traffic descriptors associated to multiple operating systems.

6.1.2.3 Management of packet flow descriptions

6.1.2.3.1 PFD management

The Management of Packet Flow Descriptions enables the UPF to perform accurate application detection when PFD(s) are provided by an ASP and then to apply enforcement actions as instructed in the PCC Rule.

The operator is able to configure pre-defined PCC Rules in the SMF or dynamic PCC Rules in the PCF that include at least an application identifier for service data flow detection, charging control information, i.e. charging key and

optionally the Sponsor identifier or the ASP identifier or both. Depending on the service level agreements between the operator and the Application Server Provider, it may be possible for the ASP to provide individual PFDs or the full set of PFDs for each application identifier maintained by the ASP to the SMF via the PFD Management service in the NEF (PFDF). The PFDs become part of the application detection filters in the SMF/UPF and therefore are used as part of the logic to detect traffic generated by an application. The ASP may remove or modify some or all of the PFDs which have been provided previously for one or more application identifiers. The SMF may report the application stop to the PCF for an application instance identifier as defined in clause 5.8.2.8.4 of TS 23.501 [2] if the removed/modified PFD in SMF/UPF results in that the stop of the application instance is not being able to be detected.

NOTE 1: PFD management is optionally supported in the NEF and the SMF.

The ASP manages (provision, update, delete) the PFDs through the NEF (PFDF). The PFD(s) are transferred to the SMF through the NEF (PFDF). The PFDF is a logical functionality in the NEF which receives PFD(s) from the ASP through the NEF, stores the PFD(s) in the UDR and provides the PFD(s) to the SMF(s) either on the request from ASP PFD management through NEF (PFDF) (push mode) or on the request from SMF (pull mode). The PFDF functionality is a service provided by the NEF.

The ASP may provide/update/remove PFDs with an allowed delay to the NEF (PFDF). Upon reception of the request from the ASP, the NEF (PFDF) shall check if the ASP is authorized to provide/update/remove those PFD(s) and request the allowed delay. The NEF (PFDF) may be configured with a minimum allowed delay based on SLA to authorize the allowed delay provided by the ASP. When ASP and requested allowed delay are successfully authorized, the NEF (PFDF) shall translate each external application identifier to the corresponding application identifier known in the core network. The NEF (PFDF) stores the PDF(s) into the UDR.

NOTE 2: The Allowed Delay is an optional parameter. If the Allowed Delay is included, it indicates that the requested PFD(s) should be deployed within the time interval indicated by the Allowed Delay.

The PFDs may be retrieved by SMF from NEF (PFDF) in "pull" mode or may be provisioned from NEF (PFDF) to the SMF in "push" mode.

When the "push" mode is used, the NEF (PFDF) retrieves from the UDR the PFDs for each application identifier and distributes them to those SMFs that enable access to those applications. There are three methods to provision PFD(s) from the NEF (PFDF) to the SMF:

a) Push of whole PFD(s) that can be accessed by the NEF (PFDF) according to operator configuration in NEF (PFDF) (e.g. provision per day according to operator configuration);

b) Selective push of an ASP change in the PFD set (i.e. ASP changes the PFD set while operator configuration defines when to push);

c) Selective push of an ASP change in the PFD set according to ASP request (i.e. ASP indicates to push changes in a PFD set within the time interval indicated by the Allowed Delay).

When the "pull" mode is used, at the time a PCC Rule with an application identifier for which PFDs are not available is activated or provisioned, the SMF requests all PFDs for that application identifier from the NEF (PFDF), and NEF (PFDF) retrieves them from the UDR. The PFD(s) retrieved for an application identifier from the NEF (PFDF) are cached in the SMF, and the SMF maintains a caching timer associated to the PFD(s) to control how long the PFD(s) are valid. When the caching timer expires:

- If there are still active PCC rules that refer to the corresponding application identifier, the SMF reloads the PFD(s) from the NEF (PFDF) and provides it to the UPF over N4;

- If there's no active PCC rule that refers to the corresponding application identifier or the SMF removes the last PCC rule that refers to the corresponding application identifier, the SMF removes the PFD(s) identified by the application identifier and informs the UPF to remove the PFD(s) identified by the application identifier over N4.

NOTE 3: It is assumed that all SMF(s) and PFD (s) in an operator network are configured with the same default caching time value to be applied for all application identifiers.

When the "pull" mode is used, the NEF (PFDF) may provide to the SMF a caching time value per application identifier. The SMF receives the caching time value together with the PFD(s) from the NEF (PFDF) over N29 and applies this value for the application identifier instead of the configured default caching time value. If no caching time value is received from NEF (PFDF), the SMF uses the configured default caching time value.

NOTE 4: The configuration of a caching time value per application identifier in NEF (PFDF) is based on the SLA between the operator and the ASP.

When only "pull" mode is used in one PLMN for an application identifier, if the Allowed Delay is shorter than the caching time value stored for this application identifier, or shorter than the default caching time if no application-specific caching time is stored, the NEF (PFDF) may still store the PFD(s) to the UDR. The NEF (PFDF) shall provide an indication that the PFD(s) were stored and the caching time value to the ASP when informing that the Allowed Delay could not be met.

When either "pull" mode or "push" mode is used, if there's any update of the PFD(s) received and there are still active application detection rules in the UPF for the application identifier, the SMF shall provision the updated PFD set corresponding to the application identifier to the UPF.

NOTE 5: SMF should 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.

If the PFDs are managed by local O&M procedures, PFD retrieval is not used; otherwise, the PFDs retrieved from NEF (PFDF) overrides any PFDs pre-configured in the SMF. The SMF shall manage the pre-configured PFDs and PFDs provided by the NEF (PFDF) at the UPF as defined in clause 5.8.2.8.4 of TS 23.501 [2]. The SMF may differentiate the need for PFD retrieval based on operator configuration in the SMF.

The AF requests including an application identifier may trigger the activation or provisioning of a PCC Rule in the SMF by the PCF based on operator policies.

6.1.2.3.2 Packet Flow Description

PFD (Packet Flow Description) is a set of information enabling the detection of application traffic.

Each PFD may be identified by a PFD id. A PFD id is unique in the scope of a particular application identifier. Conditions for when PFD ID is included in the PFD is described in TS 29.551 [17]. There may be different PFD types associated to an application identifier.

A PFD include the following information:

- PFD id; and
- one or more of the following:
  - 3-tuple(s) including protocol, server side IP address and port number;
  - the significant parts of the URL to be matched, e.g. host name;
  - a Domain name matching criteria and information about applicable protocol(s).

NOTE 1: Based on the agreement between AF and mobile operator, the PFD can be designed to convey proprietary extension for proprietary application traffic detection mechanisms.

NOTE 2: How the PFD(s) are used in service flow detection is specified in clause 6.2.2.2.

6.1.2.4 Negotiation for future background data transfer

The AF may contact the PCF via the NEF (and Npcf_BDTPolicyControl_Create service operation) to request a time window and related conditions for future background data transfer.

NOTE 1: The NEF may contact any PCF in the operator network.

The AF request shall contain an ASP identifier, the volume of data to be transferred per UE, the expected amount of UEs, the desired time window, the External Group Identifier and optionally, Network Area Information, MAC address or IP 3-tuple to identify the Application server, request for notification. The AF provides as Network Area Information either a geographical area (e.g. a civic address or shapes), or an area of interest that includes a list of TAs or list of NG-RAN nodes and/or a list of cell identifiers. When the AF provides a geographical area, then the NEF maps it based on local configuration into of a short list of TAs and/or NG-RAN nodes and/or cells identifiers that is provided to the PCF.

The NEF may map the ASP id based on local configuration into the DNN, S-NSSAI that is provided to the PCF. The request for notification is an indication that the ASP accepts that the BDT policy can be re-negotiated using the BDT warning notification procedure described in clause 4.16.7.3 of TS 23.502 [3].

NOTE 2: A 3rd party application server is typically not able to provide any specific network area information and if so, the AF request is for the whole operator network.

The PCF shall first retrieve all existing BDT policies stored for any ASP from the UDR. The PCF may retrieve analytics on "Network Performance" from NWDAF following the procedure and services described in TS 23.288 [24]. Afterwards, the PCF shall determine, based on the information provided by the AF, the analytics on "Network Performance" if available and other available information (e.g. network policy and existing BDT policies) one or more BDT policies. The PCF may be configured to map the ASP identifier into a target DNN and slicing information (i.e. S-NSSAI), that is used if the NEF did not provide the DNN, S-NSSAI to the PCF.

A BDT policy consists of a recommended time window for the background data transfer, a reference to a charging rate for this time window and optionally a maximum aggregated bitrate (indicating that the charging according to the referenced charging rate is only applicable for the aggregated traffic of all involved UEs that stays below this value). Finally, the PCF shall provide the candidate list of BDT policies or the selected BDT policy to the AF via NEF together with the Background Data Transfer Reference ID. If the AF received more than one BDT policy, the AF shall select one of them and inform the PCF about the selected BDT policy.

NOTE 3: The maximum aggregated bitrate (optionally provided in a BDT policy) is not enforced in the network. The operator may apply offline CDRs processing (e.g. combining the accounted volume of the involved UEs for the time window) to determine whether the maximum aggregated bitrate for the set of UEs was exceeded by the ASP and charge the excess traffic differently.

NOTE 4: It is assumed that the 3rd party application server is configured to understand the reference to a charging rate based on the agreement with the operator.

The selected BDT policy together with the Background Data Transfer Reference ID, the network area information, the volume of data to be transferred per UE, the expected amount of UEs, ASP Id, MAC address or IP 3-tuple to identify the Application server, the one or more route selection component (DNN, S-NSSAI), the desired time window, the Network Area Information (if provided by the AF) and whether the AF accepts BDT policy re-negotiation or not is stored by the PCF in the UDR as Data Set "Policy Data" and Data Subset "Background Data Transfer data". The same or a different PCF can retrieve this BDT policy and corresponding related information from the UDR and take them into account for future decisions about BDT policies related to the same or other ASPs.

When the AF wants to apply the Background Data Transfer Policy to an existing session, then the AF will, at the time the BDT is about to start, provide, for each UE, the Background Data Transfer Reference ID together with the AF session information to the PCF (via the N5 interface). The PCF retrieves the corresponding BDT policy from Policy Data Set in the UDR and derives the PCC rules for the BDT according to this transfer policy.

When the AF wants to apply the Background Data Transfer Policy to a future session, then the AF provides, to the NEF, the Background Data Transfer Reference ID together with the External Identifier (i.e. GPSI) or External Group Identifier of the UE(s) that are to be subject to the policy. The NEF translates the External Group Identifier into the Internal Group Identifier or the External Identifier into a SUPI. The NEF stores the Background Data Transfer Reference ID, in the UDR as Application Data Set and Background Data transfer data Subset for an Internal Group Identifier or a SUPI and the ASP id requesting to apply the Background Data transfer Policy to a future session for the UE(s). A PCF that serves the UE(s) (i.e. the PCF that serves the UE for UE Policies) may retrieve the Background Data Transfer Reference ID by retrieving the UE's Application Data from the UDR or by subscribing to notifications of changes to the UEs' Application Data in the UDR. Furthermore, the PCF retrieves the specific Background Data Transfer Policy and if available MAC address or IP 3-tuple to identify the Application server based on the received Background Data Transfer Reference ID stored as Policy Data Set from the UDR.

When the PCF determines to send the Background Data Transfer Policy information to the UE as part of a URSP rule, the PCF will store the policy in the UDR as part of the UE's Policy Set Entry and will use the associated S-NSSAI and DNN associated with the ASP id stored in the Application Data to store the Background Data Transfer Reference ID in the UE's PDU Session policy control subscription information (see clause 6.2.1.3). The PCF uses local policies to decide if and when the Background Data Transfer Policy information is going to be sent to the UE as Validation Criteria in the RSD part of the URSP rule (see clause 6.6.2.1). The UE uses Validation Criteria to determine whether or not a PDU Session should be established. The Time Window and Location Criteria are not required to be checked again during the lifetime of the PDU Session.

The PCF may, based on operator configuration, trigger the UE Configuration Update procedure when the policy is selected, or the PCF may wait until receiving a notification from the AMF that the UE has entered the Tracking Area or Presence Area where the policy applies, and/or the PCF may wait until the time window when the policy applies is approaching. The UE's support of the Validation Criteria in a URSP rule is optional.

NOTE 5: If a non-supporting UE receives Validation Criteria, it ignores the URSP rule.

When the PDU Session is established, the PCF that serves the PDU Session will use the Background Data Transfer Reference ID in the UE's PDU Session policy control subscription information (see clause 6.2.1.3) to retrieve the corresponding BDT policy (i.e. Time Window and/or Location Criteria) from the UDR and derives the PCC rules for the BDT according to this transfer policy.

NOTE 6: The AF will typically contact the PCF for the individual UEs to request sponsored connectivity for the BDT.

NOTE 7: A transfer policy is only valid until the end of its time window. The removal of outdated transfer policies from the UDR is up to implementation.

The PCF may reject corresponding SM Policy Association, as described in clause 4.16.4 of TS 23.502 [3], if Validation condition is not satisfied. And based on this feedback, SMF will reject the PDU Session setup.

After successful PDU Session setup, PCF may trigger PDU Session release when Validation condition is not satisfied.

The PCF may subscribe to analytics on "Network Performance" from NWDAF for the area of interest and time window of a BDT policy following the procedure and services described in TS 23.288 [24] indicating a Reporting Threshold in the Analytics Reporting information. The value for the Reporting Threshold is set by the PCF based on operator configuration. When the NWDAF determines that the network performance goes below the threshold, the NWDAF notifies the PCF with the network performance analytics in the area of interest and time window. When the PCF gets the notification from the NWDAF, the PCF may try to re-negotiate the affected BDT policies with AFs that accepted BDT policy re-negotiation. To do this, the PCF retrieves all the BDT policies together with their additionally stored AF provided information (e.g. their corresponding desired time window) from the UDR, identifies the BDT policies that are not desirable anymore due to the degradation of the network performance and tries to calculate new candidate BDT policies for the ASP(s) to select from. If the PCF does not find any new candidate BDT policy or the related AF did not accept BDT policy re-negotiation, the previously negotiated BDT policy shall be kept and no interaction with the ASP shall occur. If the PCF finds one or more new candidate BDT policies, the PCF notifies the related ASP(s) on both the BDT policy that is not valid any longer and the candidate BDT policies via NEF.

The PCF invalidates the BDT policy stored in the UDR for the corresponding BDT reference ID while the BDT policy re-negotiation is ongoing. The PCF shall reject a PDU Session request corresponding to an invalid BDT policy.

When the AF receives the notification, the AF may select one of the BDT policies included in the candidate list, and then inform the PCF about the selected BDT policy. The PCF stores the newly selected BDT policy into the UDR for the corresponding Background Data Transfer Reference ID and removes the BDT policy that is no longer valid. As a consequence, the PCF identifies the UEs for which the BDT policy was already applied and updates URSP rules with the new Validation Criteria as described in clause 4.16.12.2 of TS 23.502 [3].

NOTE 8: A PCF can subscribe to notifications on changes in BDT policy in UDR. Upon reception of such notification the PCF has also to identify the UEs for which the BDT policy was already applied and update URSP rules with the new Validation Criteria as described in clause 4.16.12.2 of TS 23.502 [3].

If the AF does not select one of the BDT policies included in the candidate list, the PCF removes the BDT policy stored in the UDR together with the corresponding Background Data Transfer Reference ID and all related information. As a consequence, the PCF identifies the UEs for which the background transfer policy was already applied and removes the URSP rules corresponding to the BDT policy using the procedure described in clause 4.16.12.2 of TS 23.502 [3].

NOTE 9: The PCF can also remove the no longer valid BDT policy after an operator configurable time for the case that the AF does not respond.

6.1.2.5 Policy Control Request Triggers relevant for AMF

The Policy Control Request Triggers relevant for AMF and 3GPP access type are listed in table 6.1.2.5-1 and define the conditions when the AMF shall interact again with PCF after the AM Policy Association Establishment or UE Policy Association Establishment.

The PCF provides Policy Control Request Triggers to the AMF indicating a specific UE (i.e. SUPI or PEI) in the Policy Association establishment and modification procedures defined in the TS 23.502 [3]. The Policy Control Request Triggers are transferred from the old AMF to the new AMF when the AMF changes.

The PCR triggers are not applicable any longer at termination of the AM Policy Association or termination of UE Policy Association.

Table 6.1.2.5-1: Policy Control Request Triggers relevant for AMF and 3GPP access type

Policy Control Request Trigger	Description	Condition for reporting
Location change (tracking area)	The tracking area of the UE has changed.	PCF (AM Policy, UE Policy)
Change of UE presence in Presence Reporting Area	The UE is entering/leaving a Presence Reporting Area	PCF (AM Policy, UE Policy)
Service Area restriction change	The subscribed service area restriction information has changed.	PCF (AM Policy)
RFSP index change	The subscribed RFSP index has changed	PCF (AM Policy)
Change of the Allowed NSSAI	The Allowed NSSAI has changed	PCF (AM Policy)
UE-AMBR change	The subscribed UE-AMBR has changed	PCF (AM Policy)
PLMN change	The UE has moved to another operators' domain.	PCF (UE Policy)
SMF selection management	UE request for an unsupported DNN or UE request for a DNN within the list of DNN candidates for replacement per S-NSSAI	PCF (AM Policy)
Connectivity state changes	The connectivity state of UE is changed	PCF (UE Policy)

NOTE: In the following description of the Policy Control Request Triggers relevant for AMF and 3GPP access type, the term trigger is used instead of Policy Control Request Trigger where appropriate.

If the Location change trigger are armed, the AMF shall activate the relevant procedure which reports any changes in location as explained in clause 5.6.11 of TS 23.501 [2] by subscribing with the Npcf_AMPolicyAssociation service or Npcf_UEPolicyAssociation service. The reporting is requested to the level indicated by the trigger (i.e. Tracking Area). The AMF reports that the Location change trigger was met and the Tracking Area identifier.

If the Change of UE presence in Presence Reporting Area trigger is armed, i.e. the PCF subscribed to reporting change of UE presence in a Presence Reporting Area, including a list of PRA ids. In addition, for "UE-dedicated Presence Reporting Area" a short list of TAs and/or NG-RAN nodes and/or cells identifiers is included. Then, the AMF shall activate the relevant procedure which reports any Change of UE presence in Area of Interest as explained in clause 5.6.11 of TS 23.501 [2]. The reporting is requested for the specific condition when target UE moved into a specified PRA. The AMF reports the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s) to the PCF.

The Service Area restriction change trigger and the RFSP index change trigger shall trigger the AMF to interact with the PCF for all changes in the Service Area restriction or RFSP index data received in AMF from UDM. The reporting includes that the trigger is met and the subscribed Service Area restriction or the subscribed RFSP index provided to AMF by UDM, as described in clause 6.1.2.1.

The Change of the Allowed NSSAI trigger shall trigger the AMF to interact with the PCF if the Allowed NSSAI has been changed. The reporting includes that the trigger is met and the new Allowed NSSAI. The PCF may update RFSP index and/or SMF selection management related policy control information (described in clause 6.5) in the AMF based on the Allowed NSSAI.

The UE-AMBR change trigger shall trigger the AMF to interact with the PCF for all changes in the subscribed UE-AMBR data received in AMF from UDM. The reporting includes that the trigger is met and the subscribed UE-AMBR provided to AMF by UDM, as described in clause 6.1.2.1.

If the PLMN change trigger is armed, the AMF shall report it to the PCF to trigger the update of V2X service authorization parameters to the UE as defined in clause 6.2.2 of TS 23.287 [28]. The reporting includes the event with the serving PLMN ID.

If the SMF selection management trigger is set, then the AMF shall contact the PCF when the AMF detects that the UE requested an unsupported DNN and the PCF indicated DNN replacement of unsupported DNNs in the Access and

mobility management related policy control information (see clause 6.5). The PCF shall select a DNN and provide the selected DNN to the AMF.

If the SMF selection management trigger is set, then the AMF shall contact the PCF when the UE requested a DNN within the list of DNN candidates for replacement for the S-NSSAI indicated in the Access and mobility management related policy control information (see clause 6.5). The PCF shall select the DNN and provide the selected DNN to the AMF.

If the Connectivity state changes trigger is set, then the AMF shall notify the PCF when the UE connectivity state is changed e.g. from IDLE to CONNECTED. The AMF then reset the trigger.

6.1.3 Session management related policy control

6.1.3.1 General

The session management related policy control functionality of the Policy and Charging control framework for the 5G system provides the functions for policy and charging control as well as event reporting for service data flows.

The PCF evaluates operator policies that are triggered by events received from the AF, from the SMF, from the AMF and from the CHF as well as changes in User subscription Profile.

NOTE 1: The details for credit management and reporting are defined in SA WG5 specification.

NOTE 2: In single PCF deployment, the PCF will provide all mobility, access and session related policies that it is responsible for. In deployments where different PCFs support N15 and N7 respectively, no standardized interface between them is required in this release to support policy alignment.

NOTE 3: Policy control in multiple administrative areas is not defined in this release.

NOTE 4: Events received from the AF include changes in global policy related instructions (as described in clause 5.6.7 of TS 23.501 [2]).

The following clauses describe the most relevant session management related functionality in detail.

6.1.3.2 Binding mechanism

6.1.3.2.1 General

The binding mechanism is the procedure that associates a service data flow (defined in a PCC rule by means of the SDF template), to the QoS Flow deemed to transport the service data flow. For service data flows belonging to AF sessions, the binding mechanism shall also associate the AF session information with the QoS Flow that is selected to carry the service data flow.

NOTE 1: The relation between AF sessions and rules depends only on the operator configuration. An AF session can be covered by one or more PCC rules, if applicable (e.g. one rule per media component of an IMS session).

NOTE 2: The PCF may authorize dynamic PCC rules for service data flows without a corresponding AF session.

The binding mechanism includes three steps:

1. Session binding;
2. PCC rule authorization; and
3. QoS Flow binding.

6.1.3.2.2 Session binding

Session binding is the association of the AF session information to one and only one PDU Session. The PCF shall perform the session binding, which may take the following PDU Session parameters into account:

a) For an IP type PDU Session, the UE IPv4 address and/or IPv6 network prefix, in addition when using W-5GAN the description in TS 23.316 [27] applies;

   For an Ethernet type PDU Session, the UE MAC address(es);

b) The UE identity (e.g. SUPI), if present;

c) The information about the Data Network (DN) the user is accessing, i.e. DNN, if present.

Once it has determined the impacted PDU Session, the PCF shall identify the PCC rules affected by the AF session information, including new PCC rules to be installed and existing PCC rules to be modified or removed.

Session Binding applies for PDU Sessions of IP type. It may also apply to Ethernet PDU Session type but only when especially allowed by PCC related Policy Control Request triggers.

6.1.3.2.3 PCC rule authorization

PCC Rule authorization is the selection of the 5G QoS parameters, described in clause 5.7.2 of TS 23.501 [2], for the PCC rules.

The PCF shall perform the PCC rule authorization for dynamic PCC rules belonging to AF sessions that have been selected in step 1, as described in clause 6.1.3.2.2, as well as for PCC rules without corresponding AF sessions.

For the authorization of a PCC rule the PCF shall consider any 5GC specific restrictions, subscription information and other information available to the PCF. Each PCC rule receives a set of QoS parameters that are supported by the specific Access Network. The authorization of a PCC rule associated with an emergency service shall be supported without subscription information. The PCF shall apply local policies configured for the emergency service.

6.1.3.2.4 QoS Flow binding

QoS Flow binding is the association of a PCC rule to a QoS Flow within a PDU Session. The binding is performed using the following binding parameters:

- 5QI;
- ARP;
- QNC (if available in the PCC rule);
- Priority Level (if available in the PCC rule);
- Averaging Window (if available in the PCC rule);
- Maximum Data Burst Volume (if available in the PCC rule).

When the PCF provisions a PCC Rule, the SMF shall evaluate whether a QoS Flow with QoS parameters identical to the binding parameters exists unless the PCF requests to bind the PCC rule to the QoS Flow associated with the default QoS rule. If no such QoS Flow exists, the SMF derives the QoS parameters, using the parameters in the PCC Rule, for a new QoS Flow, binds the PCC Rule to the QoS Flow and then proceeds as described clause 5.7.1.5 of TS 23.501 [2] to establish the new QoS Flow. If a QoS Flow with QoS parameters identical to the binding parameters exists, the SMF binds the PCC Rule to this QoS Flow and proceeds as described clause 5.7.1.5 of TS 23.501 [2] to modify the QoS Flow unless local policies or the below mentioned conditions (which QoS Flow binding shall ensure), require the establishment of a new QoS Flow following the actions described above.

NOTE 1: For PCC rules containing a delay critical GBR 5QI value, the SMF can bind PCC Rules with the same binding parameters to different QoS Flows to ensure that the GFBR of the QoS Flow can be achieved with the Maximum Data Burst Volume of the QoS Flow.

The SMF shall identify the QoS Flow associated with the default QoS rule based on the fact that the PCC rule(s) bound to this QoS Flow contain:

- 5QI and ARP values that are identical to the PDU Session related information Authorized default 5QI/ARP; or
- a Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters Indication.

NOTE 2: The Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters Indication has to be used whenever the PDU Session related information Authorized default 5QI/ARP (as described in clause 6.3.1) cannot be directly used as the QoS parameters of the QoS Flow associated with the default QoS rule, for example when a GBR 5QI is used or the 5QI priority level has to be changed.

When a QoS Flow associated with the default QoS rule exists, the PCF can request that a PCC rule is bound to this QoS Flow by including the Bind to QoS Flow associated with the default QoS rule Indication in a dynamic PCC rule. In this case, the SMF shall bind the dynamic PCC rule to the QoS Flow associated with the default QoS rule (i.e. ignoring the binding parameters) and keep the binding as long as this indication remains set. When the PCF removes the association of a PCC rule to the QoS Flow associated with the default QoS rule, a new binding may need to be created between this PCC rule and a QoS Flow based on the binding mechanism described above.

The binding created between a PCC Rule and a QoS Flow causes the downlink part of the service data flow to be directed to the associated QoS Flow at the UPF (as described in clause 5.7.1 of TS 23.501 [2]). In the UE, the QoS rule associated with the QoS Flow (which is generated by the SMF and explicitly signalled to the UE as described in clause 5.7.1 of TS 23.501 [2]) instructs the UE to direct the uplink part of the service data flow to the QoS Flow in the binding.

Whenever the binding parameters of a PCC rule changes, the binding of this PCC rule shall be re-evaluated, i.e. the binding mechanism described above is performed again. The re-evaluation may, for a PCC rule, result in a new binding with another QoS Flow. If the PCF requests the same change of the binding parameter value(s) for all PCC rules that are bound to the same QoS Flow, the SMF should not re-evaluate the binding of these PCC rules and instead, modify the QoS parameter value(s) of the QoS Flow accordingly.

NOTE 3: A QoS change of the PDU Session related information Authorized default 5QI/ARP values doesn't cause the QoS Flow rebinding for PCC rules with the Bind to QoS Flow associated with the default QoS rule Indication set.

When the PCF removes a PCC Rule, the SMF shall remove the association of the PCC Rule to the QoS Flow. If the last PCC rule that is bound to a QoS Flow is removed, the SMF shall delete the QoS Flow.

When a QoS Flow is removed, the SMF shall remove the PCC rules bound to this QoS Flow and report to the PCF that the PCC Rules bound to a QoS Flow are removed.

The QoS Flow binding shall also ensure that:

- when the PCF provisions a PCC rule, and if the PCC rule contains a TSC Assistance Container, the PCC rule is bound to a new QoS Flow and no other PCC rule is bound to this QoS Flow. Whenever the TSC Assistance container of an existing PCC rule is changed, the binding of this PCC rule shall not be re-evaluated.

- if a dynamic value for the Core Network Packet Delay Budget (defined in clause 5.7.3.4 of TS 23.501 [2]) is used, PCC rules with the same above binding parameters but different PDU Session anchors (i.e. the corresponding service data flows which have different CN PDBs) are not bound to the same QoS Flow.

NOTE 4: Different PDU Session anchors can exist if the DNAI parameter of PCC rules contains multiple DNAIs.

- For MA PDU Session, PCC rules for GBR or delay critical GBR service data flows allowed on different access are not bound to the same QoS Flow even if the PCC rules contain the same binding parameters.

NOTE 5: For MA PDU Session, the GBR or delay critical GBR resource for a service data flow is allocated only in one access (as described in clause 5.32.4 of TS 23.501 [2]).

- When the PCF provisions a PCC rule with Alternative QoS parameter Set(s), the PCC rule is bound to a new QoS Flow and no other PCC rule is bound to this QoS Flow.

- When the PCF provisions a PCC rule with QoS Monitoring Policy, the PCC rule is bound to a new QoS Flow and no other PCC rules is bound to this QoS Flow.

NOTE 6: The binding of PCC rule with QoS Monitoring policy to a new QoS flow is only applicable to the Per QoS Flow per UE QoS Monitoring (as described in clause 5.33.3.2 of TS 23.501 [2]).

6.1.3.3 Reporting

Reporting refers to the differentiated PDU Session resource usage information (measured at the UPF) being reported by the SMF to the CHF.

NOTE 1: Reporting usage information to the CHF is distinct from credit management. Hence multiple PCC rules may share the same charging key for which one credit is assigned whereas reporting may be at higher granularity if serviced identifier level reporting is used.

The SMF shall report usage information for online and offline charging.

The SMF shall report usage information for each charging key value.

For service data flow charging, for the case of sponsored data connectivity, the reports for offline charging shall report usage for each charging key, Sponsor Identity and Application Service Provider Identity combination if Sponsor Identity and Application Service Provider Identifier have been provided in the PCC rules.

NOTE 2: Usage reports for online charging that include Sponsor Identity and Application Service Provider Identity is not within scope of the specification in this release. Online charging for sponsored data connectivity can be based on charging key as described in Annex X.

The SMF shall report usage information for each charging key/service identifier combination if service identifier level reporting is requested in the PCC rule.

NOTE 3: For reporting purposes when charging is performed by the SMF:

a) the charging key value identifies a service data flow if the charging key value is unique for that particular service data flow, and

b) if the service identifier level reporting is present then the service identifier value of the PCC rule together with the charging key identify the service data flow.

Charging information shall be reported based on the result from the service data flow detection and measurement on a per PDU Session basis.

A report may contain multiple containers, each container associated with a charging key, charging key and Sponsor Identity (in the case of sponsored connectivity) or charging key/service identifier.

6.1.3.4 Credit management

The credit management applies only for service data flow with online charging method and shall operate on a per charging key basis. The SMF should initiate one charging session with the CHF for each PDU Session subject to charging, in order to perform credit management within the charging session.

NOTE 1: Independent credit control for an individual service/application may be achieved by assigning a unique charging key value in the corresponding PCC rule.

The SMF shall request a credit for each charging key occurring in a PCC rule. It shall be up to operator configuration whether the SMF shall request credit in conjunction with the PCC rule being activated or when the first packet corresponding to the service is detected. The CHF may either grant or deny the request for credit. The CHF shall strictly control the rating decisions.

NOTE 2: The term 'credit' as used here does not imply actual monetary credit, but an abstract measure of resources available to the user. The relationship between this abstract measure, actual money, and actual network resources or data transfer, is controlled by the CHF.

During PDU Session establishment and modification, the SMF shall request credit using the information after applying policy enforcement action (e.g. upgraded or downgraded QoS information), if applicable, even though the SMF has not signalled this information to the AMF or RAN.

The events trigger information which may be received from the CHF, causing the SMF to perform a usage reporting and credit request to CHF when the event occurs are specified in TS 32.255 [21].

The CHF may subscribe to Change of UE presence in Presence Reporting Area at any time during the life time of the charging session as described in TS 32.255 [21].

If the PCF set the Out of credit event trigger (see clause 6.1.3.5), the SMF shall inform the PCF about the PCC rules for which credit is no longer available together with the applied termination action.

6.1.3.5 Policy Control Request Triggers relevant for SMF

The Policy Control Request Triggers relevant for SMF define the conditions when the SMF shall interact again with PCF after a PDU Session establishment as defined in the Session Management Policy Establishment and Session Management Policy Modification procedure as defined in TS 23.502 [3].

The PCR triggers are not applicable any longer at termination of the SM Policy Association.

The access independent Policy Control Request Triggers relevant for SMF are listed in table 6.1.3.5-1.

The differences with table 6.2 and table A.4.3-2 in TS 23.203 [4] are shown, either "none" means that the parameter applies in 5GS or "removed" meaning that the parameter does not apply in 5GS, this is due to the lack of support in the 5GS for this feature or "modified" meaning that the parameter applies with some modifications defined in the parameter.

Table 6.1.3.5-1: Access independent Policy Control Request Triggers relevant for SMF

Policy Control Request Trigger	Description	Difference compared with table 6.2 and table A.4.3-2 in TS 23.203 [4]	Conditions for reporting	Motivation
PLMN change	The UE has moved to another operators' domain.	None	PCF	
QoS change	The QoS parameters of the QoS Flow has changed.	Removed		Only applicable when binding of bearers was done in PCRF.
QoS change exceeding authorization	The QoS parameters of the QoS Flow has changed and exceeds the authorized QoS.	Removed		Only applicable when binding of bearers was done in PCRF.
Traffic mapping information change	The traffic mapping information of the QoS profile has changed.	Removed		Only applicable when binding of bearers was done in PCRF.
Resource modification request	A request for resource modification has been received by the SMF.	None	SMF always reports to PCF	
Routing information change	The IP flow mobility routing information has changed (when IP flow mobility as specified in TS 23.261 [11] applies) or the PCEF has received Routing Rules from the UE (when NBIFOM as specified in TS 23.161 [10] applies).	Removed		Not in 5GS yet.
Change in Access Type (NOTE 8)	The Access Type and, if applicable, the RAT Type of the PDU Session has changed.	None	PCF	
EPS Fallback	EPS fallback is initiated	Added	PCF	
Loss/recovery of transmission resources	The Access type transmission resources are no longer usable/again usable.	Removed		Not in 5GS yet.
Location change (serving cell) (NOTE 6)	The serving cell of the UE has changed.	None	PCF	
Location change (serving area) (NOTE 2)	The serving area of the UE has changed.	None	PCF	
Location change (serving CN node) (NOTE 3)	The serving core network node of the UE has changed.	None	PCF	
Change of UE presence in Presence Reporting Area (see NOTE 1)	The UE is entering/leaving a Presence Reporting Area.	None	PCF	Only applicable to PCF
Out of credit	Credit is no longer available.	None	PCF	
Reallocation of credit	Credit has been reallocated after the former Out of credit indication.	Added	PCF	
Enforced PCC rule request	SMF is performing a PCC rules request as instructed by the PCF.	None	PCF	
Enforced ADC rule request	TDF is performing an ADC rules request as instructed by the PCRF.	Removed		ADC Rules are not applicable.
UE IP address change	A UE IP address has been allocated/released.	None	SMF always reports allocated or released UE IP addresses	

UE MAC address change	A new UE MAC address is detected or a used UE MAC address is inactive for a specific period.	New	PCF	
Access Network Charging Correlation Information	Access Network Charging Correlation Information has been assigned.	None	PCF	
Usage report (NOTE 4)	The PDU Session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons.	None	PCF	
Start of application traffic detection and Stop of application traffic detection (NOTE 5)	The start or the stop of application traffic has been detected.	None	PCF	
SRVCC CS to PS handover	A CS to PS handover has been detected.	Removed		No support in 5GS yet
Access Network Information report	Access information as specified in the Access Network Information Reporting part of a PCC rule.	None	PCF	
Credit management session failure	Transient/Permanent failure as specified by the CHF.	None	PCF	
Addition / removal of an access to an IP-CAN session	The PCEF reports when an access is added or removed.	Removed		No support in 5GS yet
Change of usability of an access	The PCEF reports that an access becomes unusable or usable again.	Removed		No support in 5GS yet
3GPP PS Data Off status change	The SMF reports when the 3GPP PS Data Off status changes.	None	SMF always reports to PCF	
Session AMBR change	The Session-AMBR has changed.	Added	SMF always reports to PCF	
Default QoS change	The subscribed QoS has changed.	Added	SMF always reports to PCF	
Removal of PCC rule	The SMF reports when the PCC rule is removed.	Added	SMF always reports to PCF	
Successful resource allocation	The SMF reports to the PCF that the resources for a PCC rule have been successfully allocated.	Added	PCF	
GFBR of the QoS Flow can no longer (or can again) be guaranteed	The SMF notifies the PCF when receiving notifications from RAN that GFBR of the QoS Flow can no longer (or can again) be guaranteed.	Added		
UE resumed from suspend state	The SMF reports to the PCF when it detects that the UE is resumed from suspend state.	None	PCF	Only applicable to EPC IWK
Change of DN Authorization Profile Index	The DN Authorization Profile Index received from DN-AAA has changed.	Added	SMF always reports to PCF	
5GS Bridge information available (NOTE 7)	SMF has detected new 5GS Bridge information, which may contain, Bridge ID, UE-DS-TT residence time and Ethernet port (port number and MAC address).	Added	PCF	

QoS Monitoring for URLLC	The SMF notifies the PCF of the QoS Monitoring information (e.g. UL packet delay, DL packet delay or round trip packet delay).	Added	PCF	
DDN Failure event Subscription with Traffic Descriptor	The SMF requests PCF to provide or remove policies if it received an event subscription or cancellation for DDN Failure event including traffic descriptors. The SMF provides the traffic descriptors to the PCF for policy evaluation.	Added	PCF	
DDD Status event Subscription with Traffic Descriptor	The SMF requests PCF to provide or remove policies if it received an event subscription or cancellation for DDD Status event including traffic descriptors. The SMF provides the traffic descriptors and the requested type(s) of notifications (notifications about downlink packets being buffered, and/or discarded) to the PCF for policy evaluation.	Added	PCF	
QoS constraints change	The QoS constraints in the VPLMN have been provided or changed.	Added	SMF always reports to PCF	
NOTE 1: The maximum number of PRA(s) per UE per PDU Session is configured in the PCF. The PCF may have independent configuration of the maximum number for Core Network pre-configured PRAs and UE-dedicated PRAs. The exact number(s) should be determined by operator in deployment. NOTE 2: This trigger reports change of Tracking Area in both 5GS and EPC interworking. NOTE 3: This trigger reports change of AMF in 5GC, change between ePDG and Serving GW in EPC, change between Serving GWs in EPC, or change between EPC and 5GC. In HR roaming case, if the AMF change is unknown by the H-SMF, then the AMF change is not reported. NOTE 4: Usage is defined as either volume or time of user plane traffic. NOTE 5: The start and stop of application traffic detection are separate event triggers, but received under the same subscription from the PCF. NOTE 6: Location change of serving cell can increase signalling load on multiple interfaces. Hence it is recommended that any such serving cell changes only applied for a limited number of subscribers avoiding extra signalling load. NOTE 7: UE-DS-TT Residence Time is only provided if a DS-TT port is detected. NOTE 8: For MA PDU Session this trigger reports the current used Access Type(s) and RAT type(s) upon any change of Access Type and RAT type.				

NOTE 1: In the following description of the access independent Policy Control Request Triggers relevant for SMF, the term trigger is used instead of Policy Control Request Trigger where appropriate.

When the EPS Fallback trigger is armed by the PCF, the SMF shall report the event to the PCF when a QoS Flow with 5QI=1 is rejected due to EPS Fallback.

When the Location change trigger is armed, the SMF shall subscribe to the AMF for reports on changes in location to the level indicated by the trigger. If credit-authorization triggers and Policy Control Request Triggers require different levels of reporting of location change for a single UE, the location to be reported should be changed to the highest level of detail required. However, there should be no request being triggered for PCC rules update to the PCF if the report received is more detailed than requested by the PCF.

NOTE 2: The access network may be configured to report location changes only when transmission resources are established in the radio access network.

The Resource modification request trigger shall trigger the PCF interaction for all resource modification requests not tied to a specific QoS Flow received by SMF. The resource modification request received by SMF may include request for guaranteed bit rate changes for a traffic aggregate and/or the association/disassociation of the traffic aggregate with a 5QI and/or a modification of the traffic aggregate.

The enforced PCC rule request trigger shall trigger a SMF interaction to request PCC rules from the PCF for an established PDU Session. This SMF interaction shall take place within the Revalidation time limit set by the PCF in the

PDU Session related policy information. The SMF reports that the enforced PCC rule request trigger was met and the enforced PCC Rules.

NOTE 3: The enforced PCC rule request trigger can be used to avoid signalling overload situations e.g. due to time of day based PCC rule changes.

The UE IP address change trigger shall trigger a SMF interaction with the PCF if a UE IP address is allocated or released during the lifetime of the PDU Session. The SMF reports that the UE IP address change trigger was met and the new or released UE IP address.

The UE MAC address change trigger shall trigger a SMF interaction with the PCF if a new UE MAC address is detected or a used UE MAC address is inactive for a specific period during the lifetime of the Ethernet type PDU Session. The SMF reports that the UE MAC address change trigger was met and the new or released UE MAC address.

NOTE 4: The SMF instructs the UPF to detect new UE MAC addresses or used UE MAC address is inactive for a specific period as described in TS 23.501 [2].

The Access Network Charging Correlation Information trigger shall trigger the SMF to report the assigned access network charging identifier for the PCC rules that are accompanied with a request for this trigger at activation. The SMF reports that the Access Network Charging Correlation Information trigger was met and the Access Network Charging Correlation Information.

If the Usage report trigger is set and the volume or the time thresholds, earlier provided by the PCF, are reached, the SMF shall report this situation to the PCF. If both volume and time thresholds were provided and the thresholds, for one of the measurements, are reached, the SMF shall report this situation to the PCF and the accumulated usage since last report shall be reported for both measurements.

The management of the Presence Reporting Area (PRA) functionality enables the PCF to subscribe to reporting change of UE presence in a particular Presence Reporting Area.

NOTE 5: PCF decides whether to subscribe to AMF or to SMF for those triggers that are present in both tables 6.1.2.5-2 and 6.1.3.5-1. If the Change of UE presence in Presence Reporting Area trigger is available on both AMF and SMF, PCF should not subscribe to both AMF and SMF simultaneously.

Upon every interaction with the SMF, the PCF may activate / deactivate reporting changes of UE presence in Presence Reporting Area by setting / unsetting the corresponding trigger by providing the PRA Identifier(s) and additionally the list(s) of elements comprising the Presence Reporting Area for UE-dedicated Presence Reporting Area(s).

The SMF shall subscribe to the UE Location Change notification from the AMF by providing an area of interest containing the PRA Identifier(s) and additionally the list(s) of elements provided by the PCF as specified in clause 5.6.11 of TS 23.501 [2] and clause 5.2.2.3.1 of TS 23.502 [3].

When the Change of UE presence in Presence Reporting Area trigger is armed, i.e. when the PCF subscribes to reporting change of UE presence in a particular Presence Reporting Area and the reporting change of UE presence in this Presence Reporting Area was not activated before, the SMF subscribes to the UE mobility event notification service provided by the AMF for reporting of UE presence in Area of Interest which reports when the UE enters or leaves a Presence Reporting Area (an initial report is received when the PDU Session specific procedure is activated). The SMF reports the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s), and indication(s) if the corresponding Presence Reporting Area(s) is set to inactive by the AMF to the PCF.

NOTE 6: The serving node (i.e. AMF in 5GC or MME in EPC/EUTRAN) can activate the reporting for the PRAs which are inactive as described in the TS 23.501 [2].

When PCF modifies the list of PRA id(s) to change of UE presence in Presence Reporting Area for a particular Presence Reporting Area(s), the SMF removes or adds the PRA id(s) provided in the UE mobility event notification service provided by AMF for reporting of UE presence in Area Of Interest. When the PCF unsubscribes to reporting change of UE presence in Presence reporting Area, the SMF unsubscribes to the UE mobility event notification service provided by AMF for reporting of UE presence in Area Of Interest, unless subscriptions to AMF remains due to other triggers.

The SMF stores PCF subscription to reporting for changes of UE presence in Presence Reporting Area and notifies the PCF with the PRA Identifier(s) and indication(s) whether the UE is inside or outside the Presence Reporting Area(s) based on UE location change notification in area of interest received from the serving node according to the corresponding subscription.

NOTE 7: The SMF can also be triggered by the CHF to subscribe to notification of UE presence in PRA from the AMF, and notifies the CHF when receiving reporting of UE presence in PRA from the AMF, referring to TS 32.291 [20].

If PCF is configured with a PRA identifier referring to the list of PRA Identifier(s) within a Set of Core Network predefined Presence Reporting Areas as defined in TS 23.501 [2], it activates the reporting of UE entering/leaving each individual PRA in the Set of Core Network predefined Presence Reporting Areas, without providing the complete set of individual PRAs.

When a PRA set identified by a PRA Identifier was subscribed to report changes of UE presence in Presence Reporting Area by the PCF, the SMF additionally receives the PRA Identifier of the PRA set from the AMF, along with the individual PRA Identifier(s) belonging to the PRA set and indication(s) of whether the UE is inside or outside the individual Presence Reporting Area(s), as described in TS 23.501 [2].

When the Out of credit detection trigger is set, the SMF shall inform the PCF about the PCC rules for which credit is no longer available together with the applied termination action.

When the Reallocation of credit detection trigger is set, the SMF shall inform the PCF about the PCC rules for which credit has been reallocated after credit was no longer available and the termination action was applied.

The Start of application traffic detection and Stop of application traffic detection triggers shall trigger an interaction with PCF once the requested application traffic is detected (i.e. Start of application traffic detection) or the end of the requested application traffic is detected (i.e. Stop of application traffic detection) unless it is requested within a specific PCC Rule to mute such interaction for solicited application reporting or unconditionally in the case of unsolicited application reporting. The application identifier and service data flow descriptions, if deducible, shall also be included in the report. An application instance identifier shall be included in the report both for Start and for Stop of application traffic detection when service data flow descriptions are deducible. This is done to unambiguously match the Start and the Stop events.

At PCC rule activation, modification and deactivation the SMF shall send, as specified in the PCC rule, the User Location Report and/or UE Timezone Report to the PCF.

NOTE 8: At PCC rule deactivation the User Location Report includes information on when the UE was last known to be in that location.

If the trigger for Access Network Information reporting is set, the SMF shall check the need for access network information reporting after successful installation/modification or removal of a PCC rule or upon termination of the PDU Session. The SMF shall check the Access Network Information report parameters (User Location Report, UE Timezone Report) of the PCC rules and report the access network information to the PCF. The SMF shall not report any subsequent access network information updates received from the PDU Session without any previous updates of related PCC rule unless the associated QoS Flow or PDU Session has been released.

If the SMF receives a request to install/modify or remove a PCC rule with Access Network Information report parameters (User Location Report, UE Timezone Report) set the SMF shall initiate a PDU Session modification to retrieve the current access network information of the UE and forward it to the PCF afterwards.

If the Access Network Information report parameter for the User Location Report is set and the user location (e.g. cell) is not available to the SMF, the SMF shall provide the serving PLMN identifier to the PCF.

The Credit management session failure trigger shall trigger a SMF interaction with the PCF to inform about a credit management session failure and to indicate the failure reason, and the affected PCC rules.

NOTE 9: As a result, the PCF may decide about e.g. PDU Session termination, perform gating of services, switch to offline charging, change rating group, etc.

NOTE 10: The Credit management session failure trigger applies to situations wherein the PDU Session is not terminated by the SMF due to the credit management session failure.

The default QoS change triggers shall trigger the PCF interaction for all changes in the default QoS data received in SMF from the UDM.

The Session AMBR change trigger shall trigger the SMF to provide the Session-AMBR to the PCF containing the DN authorised Session AMBR if received from the DN-AAA, or the Subscribed Session-AMBR received from the UDM as described in clause 5.6.6 of TS 23.501 [2].

The default QoS change trigger reports a change in the default 5QI/ARP retrieved by SMF from UDM, as explained in clause 5.7.2.7 of TS 23.501 [2].

If the PCC Rules bound to a QoS Flow are removed when the corresponding QoS Flow is removed or the PCC rules are failed to be enforced, the SMF shall report this situation to the PCF. The PCF may then provide the same or updated PCC rules for the established PDU Session.

If the trigger for successful resource allocation is set and the PCF has also provided an indication that a specific PCC rule is subject to this trigger, the SMF shall report to the PCF when the resources associated to this PCC rule have been successfully allocated. The SMF shall report resource allocation failure always to the PCF, independently of this trigger.

If the GFBR of the QoS Flow can no longer (or can again) be guaranteed trigger is armed, the SMF shall check the need for reporting to the PCF when the SMF receives an explicit notification from (R)AN indicating that GFBR of the QoS Flow can no longer (or can again) be guaranteed or when the condition described in clause 5.7.2.4 of TS 23.501 [2] is met during the handover. The SMF shall report that GFBR of the QoS Flow can no longer (or can again) be guaranteed accordingly to the PCF for those PCC rules which are bound to the affected QoS Flow and have the QoS Notification Control (QNC) parameter set. If additional information is received with the notification from NG-RAN (see clause 5.7.2.4 of TS 23.501 [2]), the SMF shall also provide to the PCF the reference to the Alternative QoS parameter set corresponding to the Alternative QoS Profile referenced by NG-RAN. If NG-RAN has indicated that the lowest priority Alternative QoS Profile cannot be fulfilled, the SMF shall indicate to the PCF that the lowest priority Alternative QoS parameter set cannot be fulfilled.

In an interworking scenario between 5GS and EPC/E-UTRAN, as explained in clause 4.3 of TS 23.501 [2], the PCF may subscribe via the SMF also to the Policy Control Request Triggers described in clause 6.1.2.5 when the UE is served by the EPC/E-UTRAN.

The change of DN Authorization Profile Index shall trigger a SMF interaction to send DN Authorization Profile Index to retrieve a list of PCC Rules (as defined in clause 6.3) and/or PDU Session related policy (as defined in clause 6.4) for an established PDU Session.

If the trigger for 5GS Bridge information available is armed, the SMF shall report the 5GS Bridge information when the SMF has determined or updated the 5GS Bridge information, e.g. when SMF has detected an Ethernet port which supports exchange of Ethernet Port Management Information Containers or received Bridge Management Information Container or Port Management Information Container. If a new manageable Ethernet DS-TT port is detected, the SMF provides 5GS Bridge ID, the port number and optionally MAC address of the related port of the related PDU Session to the PCF. If the SMF has received UE-DS-TT Residence Time then the SMF also provides UE-DS-TT Residence Time to the PCF. If the SMF has received the Bridge Management Information Container from NW-TT or Port Management Information Container from NW-TT or DS-TT, the SMF also provides Bridge Management Information Container or Port Management Information Container and related port number to the PCF.

When the QoS Monitoring for URLLC trigger is set, the SMF shall indicate the RAN and the UPF to perform the measurement of the QoS parameters based on the PCC rule information for QoS Monitoring as defined in clause 4.3.3.2 of TS 23.502 [3]. Upon receiving the QoS Monitoring report from the UPF, the SMF sends the measurement report to the PCF.

If the Policy Control Request Trigger "DDN Failure event subscription with Traffic Descriptor" or "DDD Status event subscription with Traffic Descriptor" is set, the SMF shall request policies if it received a subscription or cancellation of notifications for availability after DDN Failure event with traffic descriptor or DDD Status event with traffic descriptor, respectively. The SMF indicates whether it is a subscription or cancellation event and provides the received Traffic Descriptor as well as the requested type(s) of notifications (notifications about downlink packets being buffered, and/or discarded) to the PCF. When the SMF indicates a subscription event, the PCF checks whether an installed PCC rule exists for the received Traffic Descriptor and if so, the PCF sets the Downlink Data Notification Control information of that PCC rule according to the requested type(s) of notifications. Otherwise, the PCF provides a new PCC Rule with the received Traffic Descriptor in the SDF Template, the Downlink Data Notification Control information set according to the requested type(s) of notifications and other PCC Rule information set to the same values as in the existing PCC rule that previously matched the traffic. When the new PCC has to be bound to the QoS Flow associated with the default QoS rules, the PCF sets the "Bind to QoS Flow associated with the default QoS rule" parameter. From now on, the PCF needs to keep the PCC rule for the DDD event detection fully synchronized with the existing PCC rule that previously matched the traffic for all other policy and charging control settings to ensure the same user experience and traffic treatment according to the operator policy. When the SMF indicates a cancellation event, the PCF removes the Downlink Data Notification Control information in the installed PCC Rule or removes the PCC Rule if a new PCC rule has been provided during the subscription event and this PCC rule is no longer necessary for any other policy enforcement.

NOTE 11: Downlink Data Delivery (DDD) status event and DDN Failure event are specified in clause 4.15.3 of TS 23.502 [3].

The QoS constraints change trigger shall trigger a SMF interaction with the PCF if QoS constraints are received by the SMF during the lifetime of the PDU Session. The SMF reports that the QoS constraints change trigger was met and the new QoS constraints.

6.1.3.6 Policy control

QoS control refers to the authorization and enforcement of the maximum QoS that is authorized for a service data flow, for a QoS Flow or for the PDU Session. A service data flow may be either of IP type or of Ethernet type. PDU Sessions may be of IP type or Ethernet type or unstructured.

The PCF, in a dynamic PCC Rule, associates a service data flow template to an authorized QoS that is provided in a PCC Rule to the SMF. The PCF may also activate a pre-defined PCC Rule that contains that association.

The authorized QoS for a service data flow template shall include a 5QI and the ARP. For a 5QI of GBR or Delay-critical GBR resource type, the authorized QoS shall also include the MBR, GBR and may include the QoS Notification Control parameter (for notifications when authorized GFBR can no longer (or can again) be fulfilled). For 5QI of Non-GBR resource type, the authorized QoS may include the MBR and the Reflective QoS Control parameter. The 5QI value can be standardized (i.e. referring to QoS characteristics as defined in clause 5.7.3 of TS 23.501 [2]), pre-configured (i.e. referring to QoS characteristics configured in the RAN) or dynamically assigned (i.e. referring to QoS characteristics provided by the PCF as Explicitly signalled QoS Characteristics in the PDU Session related policy information described in clause 6.4).

NOTE 1: Further details, special cases and additional parameters are described in clause 6.3.1.

QoS control also refers to the authorization and enforcement of the Session-AMBR and default 5QI/ARP combination. The PCF may provide the Authorized Session-AMBR and the Authorized default 5QI and ARP combination as part of the PDU Session information for the PDU Session to the SMF. The Authorized Session-AMBR and Authorized default 5QI/ARP values takes precedence over other values locally configured or received at the SMF.

In home routed roaming, the H-SMF may provide the QoS constraints received from the VPLMN (defined in clause 4.3.2.2.2 of TS 23.502 [3]) to the H-PCF. The H-PCF ensures that the Authorized Session-AMBR value does not exceed the Session-AMBR value provided by the VPLMN and the Authorized default 5QI/ARP contains a 5QI and ARP value supported by the VPLMN. If no QoS constraints are provided the H-PCF considers that no QoS constraints apply unless operator policies define any. The PCF shall also consider the QoS constraints for the setting of the Subsequent Authorized default 5QI/ARP and Subsequent Authorized Session-AMBR.

For policy control, the AF interacts with the PCF and the PCF interacts with the SMF as instructed by the AF. For certain events related to policy control, the AF shall be able to give instructions to the PCF to act on its own, i.e. based on the service information currently available. The following events are subject to instructions from the AF:

- The authorization of the service based on incomplete service information;

NOTE 2: The QoS authorization based on incomplete service information is required for e.g. IMS session setup scenarios with available resources on originating side and a need for resource reservation on terminating side.

- The immediate authorization of the service;

- The gate control (i.e. whether there is a common gate handling per AF session or an individual gate handling per AF session component required);

- The forwarding of QoS Flow level information or events (see clause 6.1.3.18).

To enable the binding functionality, the UE and the AF shall provide all available flow description information (e.g. source and destination IP address and port numbers and the protocol information).

6.1.3.7 Service (data flow) prioritization and conflict handling

Service pre-emption priority enables the PCF to resolve conflicts where the activation of all requested active PCC rules for services would result in a cumulative authorized QoS which exceeds the Subscribed Guaranteed bandwidth QoS.

NOTE 1: For example, the PCF may use the pre-emption priority of a service, the activation of which would cause the subscriber's authorized QoS to be exceeded. If this pre-emption priority is greater than that of any one or more active PCC rules, the PCF can determine whether the deactivation of any one or more such rules would allow the higher pre-emption priority PCC rule to be activated whilst ensuring the resulting cumulative QoS does not exceed a subscriber's Subscribed Guaranteed Bandwidth QoS.

If such a determination can be made, the PCF may resolve the conflict by deactivating those selected PCC rules with lower pre-emption priorities and accepting the higher priority service information from the AF. If such a determination cannot be made, the PCF may reject the service information from the AF.

NOTE 2: Normative PCF requirements for conflict handling are not defined. Alternative procedures may use a combination of pre-emption priority and AF provided priority indicator.

6.1.3.8 Termination action

The termination action indicates the action which the SMF instructs the UPF to perform for all PCC rules of a Charging key for which credit is no longer available. The functional description for termination actions is described in TS 32.255 [21].

The SMF shall revert the termination action related instructions for the UPF for all PCC rules of a Charging key when credit is available again.

6.1.3.9 Handling of packet filters provided to the UE by SMF

Traffic mapping information is signalled to the UE by the SMF in the Packet Filter Sets of QoS rules as defined in TS 23.501 [2].

The network shall ensure that the traffic mapping information signalled to UE reflects the QoS Flow binding of PCC rules, except for those extending the inspection beyond what can be signalled to the UE. The PCC rules may restrict what traffic is allowed compared to what is explicitly signalled to the UE. The PCF may, per service data flow filter, indicate that the SMF is required to explicitly signal the corresponding traffic mapping information to the UE, e.g. for the purpose of IMS precondition handling at the UE. In absence of that indication, it is an SMF decision whether to signal the traffic mapping information that is redundant from a traffic mapping point of view.

For QoS Flow for services with no uplink IP flows, there is no need to provide any UL filter to the UE that effectively disallows any useful packet flows in uplink direction.

The default QoS rule will either contain a Packet Filter Set that allows all UL packets or a Packet Filter Set that is generated from the UL SDF filters (and from the DL SDF filters if they are available) which have an indication to signal corresponding traffic mapping information to the UE.

NOTE: If multiple PCC rules with an indication to signal corresponding traffic mapping information to the UE are bound to the QoS Flow associated with the default QoS rule, it is up to SMF implementation which one will be chosen to generate the default QoS rule. If the PCC rule that is chosen to generate the default QoS rule is removed/deactivated, another PCC rule bound to the QoS Flow associated with the default QoS rule will be used instead and the default QoS rule would be updated accordingly.

In the case of interworking with E-UTRAN connected to EPC, the specific aspects of the handling of packet filters at the SMF are described in clause 4.11.1 of TS 23.502 [3].

6.1.3.10 IMS emergency session support

PDU Sessions for IMS Emergency services are provided by the serving network to support IMS emergency when the network is configured to support emergency services. Emergency services are network services provided through an Emergency DNN and may not require a subscription depending on operator policies and local regulatory requirements. For emergency services, the architecture for the non-roaming case is the only applicable architecture model.

For emergency services, the N36 reference point does not apply. Emergency services are handled locally in the serving network.

For a PDU Session serving an IMS emergency session, the PCF makes authorization and policy decisions that restrict the traffic to emergency destinations, IMS signalling and the traffic to retrieve user location information (in the user plane) for emergency services. A PDU Session serving an IMS emergency session shall not serve any other service and

shall not be converted to/from any PDU Session serving other services. The PCF shall determine based on the DNN if a PDU Session concerns an IMS emergency session.

The PCC Rule Authorization function selects QoS parameters that allow prioritization of IMS Emergency sessions. If an IMS Emergency session is prioritized the QoS parameters in the PCC Rule shall contain an ARP value that is reserved for intra-operator use of IMS Emergency services. The PCF does not perform subscription check; instead it utilizes the locally configured operator policies to make authorization and policy decisions.

NOTE 1: Reserved value range for intra-operator use is defined in TS 23.501 [2].

For an emergency DNN, the PCF does not perform subscription check; instead it utilizes the locally configured operator policies to make authorization and policy decisions.

It shall be possible for the PCF to verify that the IMS service information is associated with a UE IP address belonging to an emergency DNN. If the IMS service information does not contain an emergency related indication and the UE IP address is associated with an emergency DNN, the PCF shall reject the IMS service information provided by the P-CSCF (and thus to trigger the release of the associated IMS session), see TS 23.167 [12].

In addition, the PCF shall provide the IMEI and the subscriber identifiers (IMSI, MSISDN) (if available), received from the SMF at PDU Session establishment, if so requested by the P-CSCF.

If the PCF removes all PCC Rules with a 5QI other than the default 5QI and the 5QI used for IMS signalling, the SMF shall start a configurable inactivity timer (e.g. to enable PSAP Callback session). When the configured period of time expires the SMF shall terminate the PDU Session serving the IMS Emergency session as defined in TS 23.502 [3]. If the SMF receives new PCC rule(s) with a 5QI other than the default 5QI and the 5QI used for IMS signalling for the PDU Session serving the IMS Emergency session, the SMF shall cancel the inactivity timer.

6.1.3.11 Multimedia Priority Service support

Multimedia Priority Services (MPS) is defined in TS 23.501 [2], TS 23.502 [3] and in TS 23.228 [5], utilising the architecture defined for 5GS.

Subscription data for MPS is provided to PCF through the N36/Nudr. To support MPS service, the PCF shall subscribe to changes in the MPS subscription data for Priority PDU connectivity service. Dynamic invocation for MPS provided from an AF using the Priority indicator over N5/Npcf takes precedence over MPS subscription.

For dynamic invocation of MPS service, the PCF shall generate the corresponding PCC rule(s) with the ARP and 5QI parameters as appropriate for the prioritized service, as defined in TS 23.501 [2].

Whenever one or more AF sessions of an MPS service are active within the same PDU Session, the PCF shall ensure that the ARP priority level of the QoS Flow for signalling as well as the QoS Flow associated with the default QoS rule is at least as high as the highest ARP priority level used by any authorized PCC rule belonging to an MPS service. If the ARP pre-emption capability is enabled for any of the authorized PCC rules belonging to an MPS service, the PCF shall also enable the ARP pre-emption capability for the QoS Flow for signalling as well as the QoS Flow associated with the default QoS rule.

In the case of IMS MPS, in addition to the above, the following QoS Flow handling applies:

- At reception of the indication from subscription information that the IMS Signalling Priority is set for the PDU Session or at reception of service authorization from the P-CSCF (AF) including an MPS session indication and the service priority level as defined in TS 23.228 [5], the PCF shall (under consideration of the requirement described in clauses 5.16.5 and 5.22.3 in TS 23.501 [2]) modify the ARP in all the PCC rules that describe the IMS signalling traffic to the value appropriate for IMS Multimedia Priority Services, if upgrade of the QoS Flow carrying IMS Signalling is required. To modify the ARP of the QoS Flow associated with the default QoS rule the PCF shall modify the Authorized default 5QI/ARP.

- When the PCF detects that the P-CSCF (AF) released all the MPS session and the IMS Signalling Priority is not set for the PDU Session the PCF shall consider changes of the requirement described in clauses 5.16.5 and 5.22.3 in TS 23.501 [2] and modify the ARP in all PCC rules that describe the IMS signalling traffic to an appropriate value according to PCF decision. The PCC rules bound to the QoS Flow associated with the default QoS rule have to be changed accordingly.

NOTE: To keep the PCC rules bound to this QoS Flow, the PCF can either modify the ARP of these PCC rules accordingly or set the Bind to QoS Flow associated with the default QoS rule.

The Priority PDU connectivity service targets the ARP and/or 5QI of the QoS Flows, enabling the prioritization of all traffic on the same QoS Flow.

For non-MPS service, the PCF shall generate the corresponding PCC rule(s) as per normal procedures (i.e. without consideration whether the MPS Priority PDU connectivity service is active or not), and shall upgrade the ARP/5QI values suitable for MPS when the Priority PDU connectivity service is invoked. When the Priority PDU connectivity service is revoked, the PCF shall change the ARP/5QI values modified for the Priority PDU connectivity service to an appropriate value according to PCF decision.

The PCF shall, at the activation of the Priority PDU connectivity service:

- modify the ARP of PCC rules installed before the activation of the Priority PDU connectivity service to the ARP as appropriate for the Priority PDU connectivity service under consideration of the requirement described in clause 5.16.5 of TS 23.501 [2]; and

- if modification of the 5QI of the PCC rule(s) is required, modify the 5QI of the PCC rules installed before the activation of the Priority PDU connectivity service to the 5QI as appropriate for this service.

The PCF shall, at the deactivation of the Priority PDU connectivity service modify any 5QI and ARP value to the value according to the PCF policy decision.

For PCC rules modified due to the activation of Priority PDU connectivity service:

- modify the ARP to an appropriate value according to PCF decision under consideration of the requirement described in clauses 5.16.5 and 5.22.3 in TS 23.501 [2]; and

- if modification of the 5QI of PCC rule(s) is required, modify the 5QI to an appropriate value according to PCF decision.

6.1.3.12 Redirection

Redirection of uplink application traffic is an option applicable in SMF or in UPF.

PCF may control redirection by provisioning and modifying dynamic PCC rules over the N7 interface, or activate/deactivate the predefined redirection policies in SMF. The PCF may enable/disable redirection and set a redirect destination for every dynamic PCC rule. Redirect information (redirection enabled/disabled and redirect destination) within a PCC Rule instructs the SMF whether or not to perform redirection towards a specific redirect destination. The redirect destination may be provided as part of the dynamic PCC Rule, or may be preconfigured in the SMF or UPF. A redirect destination provided in a dynamic PCC Rule overrides the redirect destination preconfigured in the SMF or UPF for this PCC Rule.

6.1.3.13 Resource sharing for different AF sessions

The P-CSCF (i.e. AF) may indicate to the PCF that media of an AF session may share resources with media belonging to other AF sessions according to TS 23.228 [5]. For every media flow, the P-CSCF may indicate that the media flow may share resources in both directions or in one direction only (UL or DL).

The PCF makes authorization and policy decisions for the affected AF sessions individually and generates a PCC rule for every media flow in any AF session.

If the PCF received identical indication(s) for resource sharing for multiple AF sessions, the PCF may request the SMF to realize resource sharing for the corresponding set of PCC rules. The PCF provides a DL and/or UL sharing indication with the same value for those PCC rules that are candidate to share resources according to the direction of resource sharing indicated by the AF.

For each direction, the SMF shall take the highest GBR value from each set of PCC rules related with the same sharing indication for this direction and bound to the same QoS Flow and uses that value as input for calculating the GFBR of the QoS Flow. For each direction, the SMF may take the MBR value of the most demanding PCC rule included in each set of PCC rules related with the same sharing indication for this direction and bound to the same QoS Flow and uses that as input for calculating the MFBR of the QoS Flow.

The AF session termination or modification procedure that removes media flows triggers the removal of the corresponding PCC rules from the SMF. The SMF shall recalculate the GFBR (and MFBR) value of the QoS Flow whenever a set of PCC rules with the same sharing indication changes.

Resource sharing is applied as long as there are at least two active PCC rules with the same sharing indication bound to the same QoS Flow.

Resource sharing for different AF sessions is possible only if the P-CSCF, the PCF and the SMF support it.

NOTE: This procedure assumes that applications/service logic must do the necessary coordination, e.g. pause sending or employ gating, to avoid service data flows interfering and to ensure that multiple flows comply with the combined QoS parameters.

6.1.3.14 Traffic steering control

Traffic steering control is triggered by the PCF initiated request and consists of steering the detected service data flows matching application detection filters or service data flow filter(s) in PCC Rules. The traffic steering control consists in:

- diverting (at DNAI(s) provided in PCC rules) traffic matching traffic filters provided by the PCF, as described in clause 5.6.7 of TS 23.501 [2].

- applying a specific N6 traffic steering policy for the purpose of steering the subscriber's traffic to appropriated N6 service functions deployed by the operator or a 3rd party service provider as described below.

The PCF uses one or more pieces of information such as network operator's policies, user subscription, user's current RAT, network load status, application identifier, time of day, UE location, DNN, related to the subscriber session and the application traffic as input for selecting a traffic steering policy.

The PCF controls traffic steering by provisioning and modifying traffic steering control information in PCC rules. Traffic steering control information consists of a traffic description and a reference to a traffic steering policy that is configured in the SMF.

The SMF instructs the UPF to perform necessary actions to enforce the traffic steering policy referenced by the PCF. The actual traffic steering applies at the UPF. For enforcing the traffic steering policy, the UPF may support traffic steering related functions as defined by other standard organizations. The mechanism used for routing the traffic over N6 is out of 3GPP scope.

6.1.3.15 Resource reservation for services sharing priority

An AF may indicate to the PCF that a media flow of an AF session is allowed to use the same priority as media flows belonging to other AF sessions (instead of the service priority provided for this media flow). In this case, the AF will provide a priority sharing indicator in addition to the application identifier and the service priority. For MCPTT, the service priority and the priority sharing indicator are defined in TS 23.179 [6]. The priority sharing indicator is used to indicate what media flows are allowed to share priority.

The PCF makes authorization and policy decisions for the affected AF sessions individually and generates a PCC rule for every media flow as specified in clause 6.1.1.3. The application identifier and the service priority are used to calculate the ARP priority. The AF may also provide suggested pre-emption capability and vulnerability values per media flow to the PCF. The ARP pre-emption capability and the ARP pre-emption vulnerability are set according to operator policies and regulatory requirements, also taking into consideration the application identifier and suggested values, when provided by the AF. The priority sharing indicator is stored for later use.

For PCC rules with the same 5QI assigned and having an associated priority sharing indicator, the PCF shall try to make authorization and policy decisions taking the priority sharing indicator into account and modify the ARP of these PCC rules as follows, (the original ARP values are stored for later use):

- The modified ARP priority is set to the highest of the original priority among all the PCC rules that include the priority sharing indicator;

- The modified ARP pre-emption capability is set if any of the original PCC rules have the ARP pre-emption capability set;

- The modified ARP pre-emption vulnerability is set if all the original PCC rules have the ARP pre-emption vulnerability set.

If the PCF receives an indication that a PCC rule provisioning or modification failed (due to resource reservation failure) then, the PCF may apply pre-emption and remove active PCC rules from the SMF and then retry the PCC rule

provisioning or modification. If the PCF does not apply pre-emption, the AF is notified using existing procedures that the resource reservation for the new media flow failed.

The AF may optionally provide pre-emption control information, including pre-emption capability and vulnerability values, in addition to the priority sharing indicator to the PCF. If so, the PCF shall apply pre-emption and remove active PCC rules according to this information when receiving an indication that a PCC rule provisioning or modification failed. The pre-emption control information indicates:

- whether media flows sharing priority are candidates to being pre-empted taking into account pre-emption capability and vulnerability values;
- how to perform pre-emption among multiple potential media flow candidates of same priority: most recently added media flow, least recently added media flow, media flow with highest requested bandwidth in the AF request.

6.1.3.16 3GPP PS Data Off

This feature, when activated by the user, prevents traffics via 3GPP access except for 3GPP PS Data Off Exempt Services. The 3GPP PS Data Off Exempt Services are a set of operator services, defined in TS 22.011 [15] and TS 23.221 [16], that are the only allowed services in both downlink and uplink direction when the 3GPP PS Data Off feature has been activated by the user.

When PCF is deployed, it shall be able to configure the list(s) of 3GPP PS Data Off Exempt Services for 3GPP access, and the Policy Control Request Trigger of 3GPP PS Data Off status change used to inform the PCF from SMF about every change of the 3GPP PS Data Off status.

NOTE 1: The PCF can be configured with a list(s) of 3GPP PS Data Off Exempt Services per DNN. The list(s) of 3GPP PS Data Off Exempt Services for an DNN can also be empty, or can allow for any service within that DNN, according to operator policy.

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 [5]. Policies configured in the PCF need to ensure that IMS services are allowed when the 3GPP Data Off status of the UE is set to "activated", e.g. by treating any service within a well-known IMS DNN as 3GPP PS Data Off Exempt Services.

When the PCF is informed about the activation of 3GPP PS Data Off, it shall update the PCC rules in such a way that for 3GPP access only packets for services belonging to the list(s) of 3GPP PS Data Off Exempt Services are forwarded while all other packets are discarded. Packets sent over non-3GPP access are not affected, and in the case of MA PDU Session, this is ensured by the MA PDU Session Control policy, e.g. for packets not belonging to the 3GPP Data Off Exempt Services, PCF provides PCC rule containing Steering Mode "Active-Standby" with active access as non-3GPP access and no standby access for downlink and uplink direction.

NOTE 3: For non MA PDU Sessions, in order for the SMF/UPF to prevent the services that do not belong to the list(s) of 3GPP PS Data Off Exempted Services, if the services are controlled by dynamic PCC rules, the PCF could modify the PCC rules by setting the gate status to "closed" for downlink and optionally uplink direction in all active dynamic PCC rules or remove those dynamic PCC rules. If the services are controlled by predefined PCC rules, the PCF can deactivate those predefined PCC rules. PCC rule with wild-carded service data flow filters can be among the PCC rules that are modified, removed or deactivated in that manner. In this case, it can be necessary that the PCF at the same time installs or activates PCC rules for data-off exempt services.

NOTE 4: For example, for non MA PDU Sessions, four PCC rules (A, B, C, D) are active for a PDU Session with PCC rule A representing a 3GPP PS Data Off Exempt Service. When 3GPP PS Data Off is activated, the PCF could either modify PCC rules B, C and D if they are dynamic PCC rules by closing the gate in downlink and optionally uplink direction or remove/deactivate PCC rules B, C and D if they are predefined PCC rules. PCC rule A does not need to be changed as it represents 3GPP PS Data Off Exempt Service. Assuming that PCC rule B contained wild-carded service data flow filters which has enabled some 3GPP PS Data Off Exempt Service is removed or deactivated, an additional PCC rule E can be installed or activated as well to enable downlink and optionally uplink traffic for that 3GPP PS Data Off Exempt Service.

NOTE 5: The network configuration can ensure that at least one PCC Rule is activated for the PDU Session when Data Off is activated in order to avoid deletion of an existing PDU Session or in order not to fail a PDU Session establishment.

When the PCF receives service information from the AF, in addition to what is specified in clause 6.2.1, PCF shall check if the requested service information belongs to the 3GPP PS Data Off Exempt Services. If the requested service belongs to 3GPP PS Data Off Exempt Services or if the service traffic can be sent over non-3GPP access, PCF shall continue as specified in clause 6.2.1. If the requested service doesn't belong to the 3GPP PS Data Off Exempt Services and the PDU Session is established only over 3GPP access, PCF shall reject the service request.

When the PCF is informed about the deactivation of 3GPP PS Data Off, it shall perform policy control decision as specified in clause 6.2.1 and perform PCC rule operations as specified in clause 6.3.2 to make sure that the services are allowed according to user's subscription and operator policy (irrespective of whether they belong to the list(s) of 3GPP PS Data Off Exempt Services).

When PCF is not deployed, predefined PCC rules, can be configured in the SMF, on a per DNN basis, to ensure the following:

- when the SMF is informed about activation of 3GPP PS Data Off, the SMF shall update the predefined PCC rule in a way that for 3GPP access only downlink and optionally uplink packets for services belonging to the list(s) of 3GPP PS Data Off Exempt Services are forwarded while all other downlink and uplink packets are discarded. Packets sent over non-3GPP access are not affected, and in the case of MA PDU Session, this is ensured by the MA PDU Session Control policy, e.g. for packets not belonging to the 3GPP Data Off Exempt Services, the SMF applies predefined PCC rule containing Steering Mode "Active-Standby" with active access as non-3GPP access and no standby access for downlink and uplink direction; and

- When SMF is informed about deactivation of 3GPP PS Data Off, the SMF ensures in UPF downlink and uplink packets are forwarded according to the operator policy for the subscriber.

NOTE 6: For example, for non MA PDU Sessions the SMF can be configured with two sets of predefined PCC rules: one set for UE 3GPP PS Data Off status "inactive" and another set for UE 3GPP PS Data Off status "active". The set of predefined PCC rules for UE 3GPP PS Data Off status "active" can be equivalent to the set of predefined PCC rules for UE with 3GPP PS Data Off status "inactive" with the following two differences: All services belonging to the list(s) of 3GPP PS Data Off Exempt Services can be represented by PCC rule(s) which allows the traffic to pass while in all other PCC rules (not belonging to the list(s) of 3GPP PS Data Off Exempt Services) the gate status can be "closed" for downlink and optionally uplink direction. When the SMF is informed about the change of UE 3GPP PS Data Off status, it can replace the currently active set of predefined PCC rules with the other set of predefined PCC rules.

When the UE 3GPP PS Data Off status is "active" and a handover from one access-system to another occurs, the PCF or the SMF when PCF is not deployed performs the above operations so that the downlink and optionally uplink traffic for services not belonging to the list(s) of 3GPP PS Data Off Exempt Services is only prevented via the 3GPP access.

6.1.3.17 Policy decisions based on spending limits

Policy decisions based on spending limits is a function that allows PCF taking actions related to the status of policy counters that are maintained in the CHF.

The PCF uses the CHF selection mechanism defined in TS 23.501 [2] to select the CHF that provides policy counters for spending limits for a PDU Session. The PCF shall also provide the selected CHF address(es) to the SMF in the PDU Session related policy information.

The identifiers of the policy counters that are relevant for a policy decision in the PCF may be stored in the PCF or possibly in UDR. The PCF is configured with the actions associated with the policy counter status that is received from CHF.

The PCF may retrieve the status of policy counters in the CHF using the Initial or Intermediate Spending Limit Report Retrieval Procedure. The CHF provides the current status of the policy counters to the PCF. The CHF may in addition provide one or more pending statuses for a policy counter together with the time they have to be applied. The PCF shall immediately apply the current status of a policy counter. A pending status of a policy counter shall autonomously become the current status of a policy counter at the PCF when the indicated corresponding time is reached. Subsequently provided information for pending statuses of a policy counter shall overwrite the previously received information.

The PCF may subscribe to spending limit reporting for policy counters from the CHF using the Initial or Intermediate Spending Limit Report Retrieval procedure. If spending limit reporting for a policy counter is enabled, the CHF shall notify the PCF of changes in the status of this policy counter (e.g. daily spending limit of $2 reached) and optionally pending statuses of this policy counter together with their activation time (e.g. due to a billing period that will expire at

midnight). The PCF may cancel spending limit reporting for specific policy counter(s) using the Intermediate Spending Limit Report Retrieval procedure, or for all policy counter(s) using the Final Spending Limit Report Retrieval procedure.

The PCF uses the status of each relevant policy counter, and optional pending policy counter statuses if known, as input to its policy decision to apply operator defined actions, e.g. change the QoS (e.g. downgrade Session-AMBR), modify the PCC Rules to apply gating or change charging conditions.

The CHF may report to the PCF the removal of the subscriber from the CHF system, and the PCF shall remove all the policy counters of the subscriber accordingly.

6.1.3.18 Event reporting from the PCF

The AF may subscribe/unsubscribe to notifications of events from the PCF for the PDU Session to which the AF session is bound.

The events that can be subscribed by the AF are listed in Table 6.1.3.18-1.

Table 6.1.3.18-1: Events relevant for reporting from the PCF

Event	Description	Conditions for reporting	Availability for Rx PDU Session (NOTE 2)	Availability for N5 PDU Session	Availability for Bulk Subscription (NOTE 1)
PLMN Identifier Notification	The PLMN identifier where the UE is currently located.	AF	Yes	Yes	Yes
Change of Access Type	The Access Type and, if applicable, the RAT Type of the PDU Session has changed.	AF	Yes	Yes	Yes
EPS fallback	EPS fallback is initiated	AF	Yes	Yes	No
Signalling path status	The status of the resources related to the signalling traffic of the AF session.	AF	Yes	Yes	No
Access Network Charging Correlation Information	The Access Network Charging Correlation Information of the resources allocated for the AF session.	AF	Yes	Yes	No
Access Network Information Notification	The user location and/or timezone when the PDU Session has changed in relation to the AF session.	AF	Yes	Yes	No
Reporting Usage for Sponsored Data Connectivity	The usage threshold provided by the AF has been reached; or the AF session is terminated.	AF	Yes	Yes	No
Service Data Flow deactivation	The resources related to the AF session are released.	AF	Yes	Yes	No
Resource allocation outcome	The outcome of the resource allocation related to the AF session.	AF	Yes	Yes	No
QoS targets can no longer (or can again) be fulfilled	The QoS targets can no longer (or can again) be fulfilled by the network for (a part of) the AF session.	AF	No	Yes	No
QoS Monitoring parameters	The QoS Monitoring parameter(s) (e.g. UL packet delay, DL packet delay or round trip packet delay) are reported to the AF according to the QoS Monitoring reports received from the SMF.	AF	No	Yes	No
Out of credit	Credit is no longer available.	AF	Yes	Yes	No
Reallocation of credit	Credit has been reallocated after the former Out of credit indication.	AF	Yes	Yes	No
5GS Bridge information Notification (NOTE 3)	5GS Bridge information that has been received by PCF from SMF.	AF	No	Yes	No

NOTE 1: Additional parameters for the subscription as well as reporting related to these events are described in TS 23.502 [3].
NOTE 2: Applicability of Rx is described in Annex C.
NOTE 3: 5GS Bridge information is described in clause 6.1.3 UE-DS-TT Residence Time is only provided if a DS-TT port is detected.

If an AF requests the PCF to report the PLMN identifier where the UE is currently located, then the PCF shall provide the PLMN identifier to the AF if available. Otherwise, the PCF shall provision the corresponding PCC rules, and the Policy Control Request Trigger to report PLMN change to the SMF. The PCF shall, upon receiving the PLMN identifier from the SMF forward this information to the AF.

If an AF requests the PCF to report on the change of Access Type, the PCF shall provide the corresponding Policy Control Request Trigger to the SMF to enable the report of the Change in Access Type to the PCF. The PCF shall, upon

reception of information about the Access Type the user is currently using and upon indication of change of Access Type, notify the AF on changes of the Access Type and forward the information received from the SMF to the AF. The change of the RAT Type shall also be reported to the AF, even if the Access Type is unchanged. For MA PDU Session the Access Type information may include two Access Type information that the user is currently using.

If an AF requests the PCF to report on the signalling path status, for the AF session, the PCF shall, upon indication of removal of PCC Rules identifying signalling traffic from the SMF report it to the AF.

If an AF requests the PCF to report Access Network Charging Correlation Information, the PCF shall provide to the AF the Access Network Charging Correlation Information, which allows to identify the usage reports that include measurements for the Service Data Flow(s), once the Access Network Charging Correlation Information is known at the PCF.

If an AF requests the PCF to report Access Network Information (i.e. the User Location Report and/or the UE Timezone Report) at AF session establishment, modification or termination, the PCF shall set the Access Network Information report parameters in the corresponding PCC rule(s) and provision them together with the corresponding Policy Control Request Trigger to the SMF. For those PCC rule(s) based on preliminary service information the PCF may assign the 5QI and ARP of the QoS Flow associated with the default QoS rule to avoid signalling to the UE.

NOTE: The PCF can also use the dynamic or pre-defined PCC Rules related to the IMS signalling to request Access Network Information reporting. This can be used to support e.g., regulatory requirements for SMS over IP, where the IMS network (i.e., P-CSCF) needs to retrieve the user location and/or UE Time Zone information. Note that due to regulatory requirements, the Access Network Information can be requested for SMS over IP, impacting a large number of PDU Sessions, that can lead to significant increase in signalling load when the Access Network Information is requested from AMF.

The PCF shall, upon receiving an Access Network Information report corresponding to the AF session from the SMF, forward the Access Network Information as requested by the AF (if the SMF only reported the serving PLMN identifier to the PCF, as described in clause 6.1.3.5, the PCF shall forward it to the AF). For AF session termination the communication between the AF and the PCF shall be kept alive until the PCF report is received.

If an AF requests the PCF to report the Usage for Sponsored Data Connectivity, the PCF shall provision the corresponding PCC rules, and the Policy Control Request Trigger to the SMF. If the usage threshold provided by the AF has been reached or the AF session is terminated, the PCF forwards such information to the AF.

If an AF requests the PCF to report the Service Data Flow deactivation, the PCF shall report the release of resources corresponding to the AF session. The PCF shall, upon being notified of the removal of PCC Rules corresponding to the AF session from the SMF, forward this information to the AF. The PCF shall also forward, if available, the reason why the resources are released, the user location information and the UE Timezone.

If an AF requests the PCF to report the Resource allocation outcome, the PCF shall report the outcome of the resource allocation of the Service Data Flow(s) related to the AF session. The AF may request to be notified about successful or failed resource allocation. In this case, the PCF shall instruct the SMF to report the successful resource allocation trigger (see clause 6.1.3.5). If the SMF has notified the PCF that the resource allocation of a Service Data Flow is successful and the currently fulfilled QoS matches an Alternative QoS parameter set (as described in clause 6.2.2.1), the PCF shall also provide to the AF the QoS reference parameter corresponding to the Alternative QoS parameter set referenced by the SMF.

If an AF requests the PCF to report when the QoS targets can no longer (or can again) be fulfilled for a particular media flow, the PCF shall set the QNC indication in the corresponding PCC rule(s) that includes a GBR or delay critical GBR 5QI value and provision them together with the corresponding Policy Control Request Trigger to the SMF. At the time, the SMF notifies that GFBR can no longer (or can again) be guaranteed for a QoS Flow to which those PCC Rule(s) are bound, the PCF shall report to the AF the affected media flow and provides the indication that QoS targets can no longer (or can again) be fulfilled. If additional information is received with the notification from SMF (see clause 5.7.2.4 of TS 23.501 [2]), the PCF shall also provide to the AF the QoS reference parameter corresponding to the Alternative QoS parameter set referenced by the SMF. If the SMF has indicated that the lowest priority Alternative QoS parameter set cannot be fulfilled, the PCF shall indicate to the AF that the lowest priority QoS reference of the Alternative Service Requirements cannot be fulfilled.

If the AF has subscribed to be notified of the QoS Monitoring information, the PCF further sends the QoS Monitoring report to the AF.

If an AF requests the PCF to report on the Out of credit event for the associated service data flow(s), the PCF shall inform the AF (when it gets informed by the SMF) that credit is no longer available for the services data flow(s) related to the AF session together with the applied termination action.

If an AF requests the PCF to report on the Reallocation of credit event for the associated service data flow(s), the PCF shall inform the AF (when it gets informed by the SMF) that credit has been reallocated after credit was no longer available and the termination action was applied for the service data flow(s) related to the AF session.

If an AF requests the PCF to report on the event of the 5GS Bridge information Notification, the PCF shall, upon reception of the 5GS Bridge information (refer to clause 6.1.3.23) from the SMF, forward this information to the TSN AF. When the PCF has received the Bridge Management Information Container or Port Management Information Container and related port number from SMF, the PCF also provides Bridge Management Information Container or Port Management Information Container and related port number to the TSN AF. The PCF can arm the trigger of 5GS Bridge information available to SMF based on local policy without an AF request. When SMF has reported the 5GS Bridge information and no TSN AF session exists, the PCF forward this information to a pre-configured TSN AF.

6.1.3.19 Mission Critical Services support

Mission Critical Services are defined in TS 23.501 [2], TS 23.502 [3] and in TS 23.280 [23], utilising the architecture defined for 5GS.

Subscription data for MCX services are provided to PCF through the N36/Nudr. To support MCX services, the PCF shall subscribe to changes in the MCX services subscription data for Priority PDU connectivity service. Dynamic invocation for MCX services provided from an AF using the Priority indicator over N5/Npcf takes precedence over the MCX services subscription.

For MCX services the session management relate policy control functionality of the Policy and Charging control framework for the 5G system is as defined in clause 6.1.3.11 for Multimedia Priority Service.

6.1.3.20 Access Traffic Steering, Switching and Splitting

As specified in TS 23.501 [2], the Access Traffic Steering, Switching and Splitting (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.

The PCF is informed of the ATSSS capabilities of a MA PDU Session by the SMF, as defined in clause 5.32.2 of TS 23.501 [2]. The ATSSS capabilities are both the Steering Mode and the Steering Functionality.

The PCF control of Access Traffic Steering, Switching and Splitting for a detected service data flow (SDF) is enabled by including Multi-Access PDU (MA PDU) Session Control information in the PCC rule. This allows the PCF to control:

- The Steering Mode that is used to steer/switch/split the detected SDF. The available Steering Modes are defined in TS 23.501 [2].
- The Steering Functionality that is used for the detected SDF, e.g. the MPTCP functionality or the ATSSS-LL functionality defined in TS 23.501 [2].
- Charging information depending on what Access Type is used for a detected SDF.
- Usage Monitoring information depending on what Access Type is used for a detected SDF.

The rest of the information in the PCC Rule apply to the SDF as such and are not dependent on what Access Type is used for a packet.

The MA PDU Session Control information in the PCC rules is used by the SMF in order to create applicable N4 rules for the UPF and ATSSS rules for the UE, as described in TS 23.501 [2]. The ATSSS rules are sent to UE via NAS when the MA PDU Session is created or updated by the SMF/PCF, as described in TS 23.501 [2] and TS 23.502 [3].

When MA PDU Session Control Information is provided to the SMF within a PCC Rule, the (H-)PCF provides both the Service Data Flow templates to identify a Service Data Flow in the UPF and if the Service Data Flow template includes an application identifier, then the corresponding Application descriptors to identify the application traffic in the UE is also included.

The (H-) PCF may use the OSid stored in the UDR as DataSet "Policy Data" and Data Subset "UE context policy control data" to determine the OSAppId supported by the OSid. The (H-)PCF may also provide multiple Application descriptors to identify application traffic in the UE, this is determined by the (H-)PCF local policies that indicates e.g. the operating system supported by the UE. If no OSid is available in the UDR, the (H-)PCF may use the PEI to determine the OSid supported by the UE.

NOTE 1: If the (H-)PCF does not take into account the received PEI and/or OSId then the (H-)PCF can send PCC rules containing application traffic descriptors associated to multiple operating systems.

The Traffic Descriptor in the ATSSS rule is generated by the SMF from the SDF template of the PCC rule. If the SDF template contains SDF filters, the SMF uses the UL SDF filters for the generation of the IP descriptors or Non-IP descriptors, respectively. If the SDF template contains an application identifier, the SMF includes the Application descriptors received from the PCF as part of the MA PDU Session information in the PCC Rule within the Traffic Descriptors in the ATSSS rule.

The PCF may also provide URSP rules to the UE for instructing the UE to establish a MA PDU Session, as described in clause 6.6.2.

The PCF control of PDU Session level Usage Monitoring depending on what access type is used to carry the traffic is enabled by providing Usage Monitoring control related information per access in the PDU Session related policy control information (as described in clause 6.4).

If the MA PDU Session is capable of MPTCP and ATSSS-LL with any Steering Mode in the downlink and MPTCP and ATSSS-LL with Active-Standby in the uplink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule contains a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to "Active-Standby" for the uplink direction, and the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to any supported steering mode for the downlink direction.

If the MA PDU Session is capable of MPTCP with any Steering Mode in the downlink, ATSSS-LL with any steering mode except Smallest Delay steering mode in the downlink, and MPTCP and ATSSS-LL with Active-Standby in the uplink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule contains a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to "Active-Standby" for the uplink direction, and the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to any supported steering mode except Smallest Delay steering mode for the downlink direction.

If the MA PDU Session is capable of MPTCP and ATSSS-LL with Active-Standby in the uplink and downlink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule contains a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to "Active-Standby" for the uplink direction and the downlink direction.

If the MA PDU Session is capable of MPTCP and ATSSS-LL with any Steering Mode in the uplink and downlink, then the PCF shall provide a PCC Rule for non-MPTCP traffic. This PCC Rule may contain a "match all" SDF template, the lowest precedence, the Steering Functionality set to "ATSSS-LL" and the Steering Mode set to any supported steering mode for the uplink direction and for the downlink direction.

These PCC Rules are used by the SMF to generate an ATSSS rule for the UE and an N4 rule for the UPF to route the non-MPTCP traffic of the MA PDU Session in the uplink and downlink direction respectively.

NOTE 2: The PCF can also use the ATSSS capability of the MA PDU Session to provide PCC Rules containing SDF template for some specific non-MPTCP traffic other than the PCC Rule containing a "match all" SDF template. This allows the operator to apply different policies e.g. charging key to non-MPTCP traffic other than the non-MPCTP traffic matching the "match all" PCC Rule.

6.1.3.21 QoS Monitoring to assist URLLC Service

The QoS Monitoring for URLLC refers to the real time packet delay measurement between the UE and the UPF for a QoS Flow corresponding to an URLLC service.

The PCF generates the authorized QoS Monitoring policy for the service data flow based on the QoS Monitoring request if received from the AF. The QoS Monitoring policy includes the following:

- QoS parameters to be measured (DL, UL or round trip packet delay);
- frequency of reporting (event triggered, periodic):

- if the reporting frequency is event triggered:
  - the corresponding reporting threshold to each QoS parameter;
  - minimum waiting time between subsequent reports;
- the reporting period;

- information about the target of the QoS Monitoring reports (e.g. either to the PCF or the AF indicated as Notification Target Address + Notification Correlation ID as specified in clause 4.15.1 of TS 23.502 [3]).

The PCF includes the authorized QoS Monitoring policy in the PCC rule and provides it to the SMF.

6.1.3.22 AF session with required QoS

The AF may request that a data session to a UE is set up with a specific QoS (e.g. low latency or jitter) and priority handling. The AF can request the network to provide QoS for the AF session based on the service requirements with the help of a QoS reference parameter which refers to pre-defined QoS information. When the PCF authorizes the service information from the AF and generates a PCC rule, it derives the QoS parameters of the PCC rule based on the service information and the indicated QoS reference parameter.

NOTE 1: A SLA has to be in place between the operator and the ASP defining the possible QoS levels and their charging rates. For each of the possible pre-defined QoS information sets, the PCF needs to be configured with the corresponding QoS parameters and their values as well as the appropriate Charging key (or receive this information from the UDR).

The AF may change the QoS by providing a different QoS reference parameter while the AF session is ongoing. If this happens, the PCF shall update the related QoS parameter sets in the PCC rule accordingly.

If the PCF gets informed about Policy Control Request Triggers relevant for the AF session, the PCF shall inform the AF about it as defined in clause 6.1.3.18.

If an AF session can adjust to different QoS parameter combinations, the AF may provide Alternative Service Requirements containing one or more QoS reference parameters in a prioritized order (which indicates the preference of the QoS requirements with which the service can operate). If so, the AF shall also subscribe to receive notifications from the PCF for successful resource allocation and when the QoS targets can no longer (or can again) be fulfilled as described in clause 6.1.3.18.

When the PCF authorizes the service information from the AF and generates a PCC rule, it shall also derive Alternative QoS parameter sets for this PCC rule based on the QoS reference parameters in the Alternative Service Requirements.

The PCF shall enable QoS Notification Control and include the derived Alternative QoS parameter sets (in the same prioritized order indicated by the AF) in the PCC rule sent to the SMF. When the PCF notifies the AF that QoS targets can no longer be fulfilled, the PCF shall include the QoS reference parameter corresponding to the Alternative QoS parameter set referenced by the SMF or an indication that the lowest priority QoS reference of the Alternative Service Requirements cannot be fulfilled (as described in clause 6.1.3.18).

NOTE 2: The AF behaviour is out of the scope of this TS but can include adaptation to the change of QoS (e.g. rate adaptation) as well as application layer signalling with the UE.

The AF may change the Alternative Service Requirements while the AF session is ongoing. If this happens, the PCF shall update the Alternative QoS parameter sets in the PCC rule accordingly.

The AF may indicate to the PCF that the UE does not need to be informed about changes related to Alternative QoS Profiles. With this indication received from the AF, the PCF decides whether to disable the notifications to the UE when changes related to the Alternative QoS Profiles occur and sets the Disable UE notifications at changes related to Alternative QoS Profiles parameter in the PCC rule accordingly.

6.1.3.23 Support of integration with Time Sensitive Networking

Time Sensitive Networking (TSN) support is defined in TS 23.501 [2], where the 5GS represents logical TSN bridge(s) based on the defined granularity model. The TSN AF and PCF interact to perform QoS mapping as described in clause 5.28.4 of TS 23.501 [2].

The PCF provides the following parameters to the TSN AF:

- 5GS Bridge information:
  - 5GS Bridge ID;
  - UE-DS-TT Residence time;
  - port number of the Ethernet port of DS-TT;
  - MAC address of the Ethernet port of DS-TT (i.e. DS-TT port MAC address).
- Port Management Information Container and the related port number.
  - Bridge Management Information Container.

The TSN AF may use this information to construct IEEE 802.1 managed objects, to interwork with IEEE 802.1 TSN networks, as described in TS 23.501 [2] and TS 23.502 [3].

The TSN AF requests related to TSN configuration are sent on the AF session associated with the DS-TT port MAC address. The TSN AF decides the TSN QoS information (i.e. priority, delay, maximum TSC Burst Size and Maximum Flow Bitrate) and TSC Assistance Container based on the received configuration information of 5GS Bridge from the CNC as defined in clause 5.28.2 of TS 23.501 [2], the bridge delay information at the TSN AF and the UE-DS-TT Residence time.

The PCF receives a request from the TSN AF that may include:

- Flow Descriptions including Ethernet Packet Filters (e.g. Ethernet PCP, VLAN ID, destination MAC address of the TSN stream);
- TSN QoS Parameters for the service data flow:
  - TSC Assistance Container: describes the TSC stream traffic characteristics (burst arrival time, periodicity, (both in reference to TSN GM), and Flow direction needed for TSCAI determination (as described in clauses 5.27 and 5.28 of TS 23.501 [2]);
  - TSN QoS information, i.e. priority, maximum TSC Burst Size, delay and Maximum Flow Bitrate.
- Port Management Information Container and related Port number;
- Bridge Management Information Container.

The PCF performs Session binding using the DS-TT port MAC address, and then the PCF derives the 5QI based on the TSN QoS information and the PCF shall consider the delay parameter provided by the TSN AF for deriving the 5QI. The PCF generates a PCC Rule with service data flow filter (including Ethernet Packet Filter set as in clause 5.7.6.3 of TS 23.501 [2]) derived from the Flow Descriptions provided by the TSN AF, the mapped 5QI, ARP, GBR and MBR and the associated TSC Assistance Container as received from the AF. The PCF derives the 5QI value as defined in clause 5.27.3 of TS 23.501 [2], the PCF derives the GBR using the Maximum Flow Bitrate provided by the TSN AF and the ARP is assigned a value preconfigured for TSN services. The SMF binds the PCC Rule to a QoS Flow as defined in clause 6.1.3.2.4.

NOTE: TSC burst size can represent the maximum burst size of the TSN streams that have been aggregated.

6.1.3.24 Policy control for redundant PDU Sessions

As specified in clause 5.33.2.1 of TS 23.501 [2], in order to support highly reliable URLLC services, two redundant PDU Sessions over the 5G network may be established such that the 5GS sets up the user plane paths of the two redundant PDU Sessions to be disjoint. The Policy control for redundant PDU Session specifies that the PCF may request traffic redundancy for the PDU Session (e.g. when some of the allowed services require redundancy).

The PCF provides to the SMF the indication on whether the PDU Session is a redundant PDU Session or not based on operator policies. The SMF follows the procedure defined in TS 23.501 [2] to establish redundant PDU Sessions depending on the indication from the PCF.

6.2 Network functions and entities

6.2.1 Policy Control Function (PCF)

6.2.1.1 General

6.2.1.1.1 Session management related functionality

The PCF provides the following session management related functionality:

- Policy and charging control for a service data flows;
- PDU Session related policy control;
- PDU Session event reporting to the AF.

The PCF provides authorized QoS for a service data flow and other network control regarding service data flow detection, gating, QoS and charging (except credit management) towards the SMF.

The PCF uses the service information received from the AF (e.g. SDP information or other available application information) and/or the subscription information received from the UDR to calculate the proper QoS authorization (QoS class identifier, bitrates). The PCF may also take into account the requested QoS received from the SMF and the analytics information (e.g. analytics related to "Service Experience") received from the NWDAF.

NOTE 1: The PCF provides always the maximum values for the authorized QoS even if the requested QoS is lower than what can be authorized.

The PCF may check that the service information provided by the AF is consistent with both the operator defined policies and the related subscription information as received from the UDR during PDU Session establishment before storing the service information. The PCF may reject the request received from the AF when the service information is not consistent with either the related subscription information or the operator defined policies and may indicate, in the response to the AF, the service information that can be accepted by the PCF (e.g. the acceptable bandwidth). In the absence of other policy control mechanisms outside the scope of PCC, it is recommended that the PCF include this information in the response.

In this Release, the PCF supports only the interaction with a single AF for each AF session.

The Authorization of QoS shall be based on complete service information unless the PCF is required to perform the authorization of QoS based on preliminary service information. The PCF shall after receiving the complete service information, update the affected PCC rules accordingly.

At reception of the service information from the AF if configured through policy and taking into account information defined in TS 26.114 [31], the PCF determines the Maximum Packet Loss Rate for UL and DL based on the service information and sends it to SMF along with the PCC rule.

NOTE 2: Based on local configuration, the PCF sets the Maximum Packet Loss Rate (UL, DL) corresponding to either the most robust codec configuration (e.g. codec, mode, redundancy) or the least robust codec configuration of the negotiated set in each direction.

NOTE 3: Details for setting the Maximum Packet Loss Rate are specified by SA4.

The PCF supports usage monitoring control as described in clause 6.2.1.7.

The PCF supports sponsored data connectivity for a service as described in clause 6.2.1.8.

The PCF uses the information relating to subscriber spending available in the CHF as input for policy decisions related to e.g. QoS control, gating or charging conditions. Details for policy decisions based on spending limits are described in clause 6.1.3.17.

The PCF uses one or more pieces of information defined in the clause 6.2.1.2 as input for the selection of traffic steering policies used to control the steering of the subscriber's traffic as described in clause 6.1.3.14.

The PCF reports PDU Session events, e.g. Access Type, RAT Type (if applicable), Access Network Information, PLMN identifier where the UE is located, as described in clause 6.1.3.18.

The subscription and reporting of events when the target for reporting is an Internal Group Identifier or any UE accessing a combination of (DNN, S-NSSAI), is described in clause 5.2.5.7 of TS 23.502 [3]. The events that can be reported by the PCF are described in clause 6.1.3.18.

The subscription and reporting of events targeting an individual UE IP address (IPv4 address or IPv6 prefix) and optionally the DN information are described below. The events that can be reported by the PCF are described in clause 6.1.3.18.

The PCF shall ensure that the sum of the packet filters used by all PCC rules which trigger the generation of signalled QoS rules does not exceed the number of supported packet filters for signalled QoS rules indicated by the UE for the PDU Session, if this information is provided by the SMF (as defined in clause 6.2.1.2).

For EPC IWK, when PCF receives from the SMF of the report on UE resumed from suspend state, the PCF may provision PCC Rules to the SMF to trigger an IP-CAN Session modification procedure.

The PCF may provide the IP index as the PDU Session related policy to the SMF for IP address/Prefix allocation at SM Policy Association Establishment. If PCF receives from the SMF an allocated IP address/Prefix for the PDU Session, it shall not include IP Index into the PDU Session related policy.

On receiving the DN Authorization Profile Index provided by the SMF at the establishment or modification of the SM Policy Association for a PDU Session, the PCF takes the DN Authorization Profile Index as input for a policy decision and then obtains the list of PCC Rules (as defined in clause 6.3) and/or PDU Session related policy (as defined in clause 6.4) and provides them to the SMF as part of the Session Management Policy Control Data for enforcement.

On receiving the Session-AMBR provided by the SMF at the establishment or modification of the SM Policy Association for a PDU Session under the conditions defined in clause 5.6.6 of TS 23.501 [2], the PCF provides the Authorized Session-AMBR as part of the PDU Session policy control information defined in clause 6.4.

The PCF provides DNAI(s) in the PCC rule(s) to the SMF, taking into account the AF request and the Local routing indication from the PDU Session policy control subscription information.

When the PCF detects that all PCC rules related to an AF session are removed, or the PCF detects that the SM Policy Association is terminated, the PCF shall request the AF to terminate the AF session. If the SMF indicated that the PCC rules were removed or that the SM Policy Association is terminated due to PS to CS handover, the PCF shall indicate PS to CS handover as cause within the request to terminate the AF session.

NOTE 4: For 5G-SRVCC (i.e. SRVCC from NG-RAN to UTRAN) as specified in TS 23.216 [25]), the SM Policy Association is terminated by the SMF. For SRVCC (i.e. SRVCC from E-UTRAN to GERAN/UTRAN) as specified in TS 23.216 [25], the SMF indicates that PCC rules are removed.

6.2.1.1.2 Non-session management related functionality

The PCF provides the following non-session management related functionality:

- Access and mobility related policy control (as described in clause 6.1.2.1);
- UE policy information control (as described in clause 6.1.2.2);
- Negotiation for future BDT (as described in clause 6.1.2.4).

6.2.1.2 Input for PCC decisions

The PCF shall accept input for PCC decision-making from the SMF, the AMF, the CHF, the NWDAF if present, the UDR and if the AF is involved, from the AF, as well as the PCF may use its own predefined information. These different nodes should provide as much information as possible to the PCF. At the same time, the information below describes examples of the information provided. Depending on the particular scenario all the information may not be available or is already provided to the PCF.

The AMF may provide the following information:

- SUPI;

- PEI of the UE;
- Location of the subscriber;
- Service Area Restrictions;
- RFSP Index;
- RAT Type;
- GPSI;
- Access Type;
- Serving Network identifier (PLMN ID or PLMN ID and NID, see clause 5.34 of TS 23.501 [2]);
- Allowed NSSAI;
- UE time zone;
- Subscribed UE-AMBR;
- Mapping Of Allowed NSSAI;
- S-NSSAI for the PDU Session;
- Requested DNN.

NOTE 1: The Access Type and RAT Type parameters should allow extension to include new types of accesses.

The UE may provide the following information:

- OSId;
- List of PSIs;
- Indication of UE support for ANDSP.

The SMF may provide the following information:

- SUPI;
- PEI of the UE;
- IPv4 address of the UE;
- IPv6 network prefix assigned to the UE;
- Default 5QI and default ARP;
- Request type (initial, modification, etc.);
- Type of PDU Session (IPv4, IPv6, IPv4v6, Ethernet, Unstructured);
- Access Type;
- RAT Type;
- GPSI;
- Internal-Group Identifier;
- Location of the subscriber;
- S-NSSAI;
- DNN;
- Serving Network identifier (PLMN ID or PLMN ID and NID, see clause 5.34 of TS 23.501 [2]);

- Application identifier;
- Allocated application instance identifier;
- Detected service data flow descriptions;
- UE support of reflective QoS (as defined in clause 5.7.5.1 of TS 23.501 [2]);
- Number of supported packet filters for signalled QoS rules for the PDU Session (indicated by the UE as defined in clause 5.7.1.4 of TS 23.501 [2]);
- 3GPP PS Data Off status;
- DN Authorization Profile Index (see clause 5.6.6 of TS 23.501 [2]);
- DN authorized Session AMBR (see clause 5.6.6 of TS 23.501 [2]).

The UDR may provide the information for a subscriber connecting to a specific DNN and S-NSSAI, as described in the clause 6.2.1.3.

The UDR may provide the following policy information related to an ASP:

- The ASP identifier;
- A transfer policy together with a Background Data Transfer Reference ID, the volume of data to be transferred per UE, the expected amount of UEs.

NOTE 2: The information related with AF influence on traffic routing may be provided by UDR when the UDR serving the NEF is deployed and stores the application request.

The UDR may provide the service specific information as defined in clause 4.15.6.7 of TS 23.502 [3].

The AF, if involved, may provide the following application session related information directly or via NEF, e.g. based on SIP and SDP:

- Subscriber Identifier;
- IP address of the UE;
- Media Type;
- Media Format, e.g. media format sub-field of the media announcement and all other parameter information (a= lines) associated with the media format;
- Bandwidth;
- Sponsored data connectivity information;
- Flow description, e.g. source and destination IP address and port numbers and the protocol;
- AF application identifier;
- DNN and possibly S-NSSAI;
- AF Communication Service Identifier (e.g. IMS Communication Service Identifier), UE provided via AF;
- AF Application Event Identifier;
- AF Record Information;
- Flow status (for gating decision);
- Priority indicator, which may be used by the PCF to guarantee service for an application session of a higher relative priority;

NOTE 3: The AF Priority information represents session/application priority and is separate from the MPS 5GS Priority indicator.

- Emergency indicator;
- Application service provider;
- DNAI;
- Information about the N6 traffic routing requirements;
- GPSI;
- Internal-Group Identifier;
- Temporal validity condition;
- Spatial validity condition;
- AF subscription for early and/or late notifications about UP management events;
- AF transaction identifier;
- TSN QoS information as described in clause 6.1.3.23;
- QoS information to be monitored;
- Reporting frequency.

The AF may provide the following BDT related information via NEF:

- Background Data Transfer Reference ID;
- BDT Policy;
- Volume per UE;
- Number of UEs;
- Desired time window;
- Network Area Information.

The CHF, if involved, may provide the following information for a subscriber:

- Policy counter status for each relevant policy counter.

The NWDAF, if involved, may provide analytics information as described in clause 6.1.1.3.

In addition, the predefined information in the PCF may contain additional rules based on charging policies in the network, whether the subscriber is in its home network or roaming, depending on the QoS Flow attributes.

The 5QIs (see clause 5.7.4 of TS 23.501 [2]) in the PCC rule is derived by the PCF from AF or UDR interaction if available. The input can be SDP information or other available application information, in line with operator policy.

The Allocation and Retention Priority in the PCC Rule is derived by the PCF from AF or UDR interaction if available, in line with operator policy.

6.2.1.3 Policy control subscription information management

The PCF may request subscription information at PDU Session establishment and during the UE Policy Association Establishment procedure.

The PCF may receive notifications on changes in the subscription information. Upon reception of a notification, the PCF shall make the policy control decisions necessary to accommodate the change in the subscription and shall update the SMF and/or the AMF if needed.

NOTE 1: How the PCF provisions/retrieves information related with policy control subscription data is defined in TS 23.501 [2].

The policy control subscription profile information provided by the UDR during the UE Policy Association Establishment procedure using Nudr service for Data Set "Policy Data" and Data Subset "UE context policy control data" is described in Table 6.2-1:

Table 6.2-1: UE context policy control subscription information

Information name	Description	Category
Subscriber categories	List of category identifiers associated with the subscriber	Optional
Tracing Requirements	Tracing requirements as defined in TS 32.421 [18]	Optional
PEI	The Permanent Equipment Identifier of the UE.	Optional
OSId	Identifies the operating system supported by UE.	Optional
Indication of UE support for ANDSP	Indicates the UE support for ANDSP.	Optional
S-NSSAI subscription information	Contains the list of subscribed S-NSSAIs, its associated subscribed DNNs. For each DNN, it includes the Allowed PDU Session types, the Allowed SSC modes and the ATSSS information (NOTE).	Optional
NOTE: ATSSS information is defined in TS 23.502 [3] Table 5.2.3.3.1-1 and Indicates whether MA PDU Session establishment is allowed.		

NOTE 2: S-NSSAI subscription information can be part of UE context policy control subscription information and Session Management Subscription data/Slice Selection Subscription data. UDR implementation and the provisioning system are responsible for keeping the consistency of this information when both Data Sets are stored in the same UDR. The provisioning system is responsible for keeping the consistency of this information when both Data Sets are stored in different UDRs.

The policy control subscription profile information provided by the UDR at PDU Session establishment, using Nudr service for Data Set "Policy Data" and Data Subset "PDU Session policy control data" is described in Table 6.2-2.

Table 6.2-2: PDU Session policy control subscription information

Information name	Description	Category
Allowed services	List of subscriber's allowed service identifiers	Optional
Subscriber categories	List of category identifiers associated with the subscriber	Optional
Subscribed GBR	Maximum aggregate bitrate that can be provided across all GBR QoS Flows for the DNN and S-NSSAI.	Optional
ADC support	Indicates whether application detection and control can be enabled for a subscriber	Optional
Subscriber spending limits control	Indicates whether the PCF must enforce policies based on subscriber spending limits	Optional
IP index information	Information that identifies the IP Address allocation method during PDU Session establishment	Optional
Background Data Transfer Reference ID(s)	Reference ID(s) for Background Data Transfer Policies that apply to the UE.	Optional
Local routing indication	Indication on whether AF influence on traffic routing is allowed or not allowed	Optional
Charging related information	This part defines the charging related information in the policy control subscription profile	
Default charging method	Default charging method for the PDU Session (online / offline)	Optional
CHF address	The address of the Charging Function and optionally the associated CHF instance ID and CHF set ID (see clause 6.3.1.0 of TS 23.501 [2])	Optional
Usage monitoring related information	This part includes a list of usage monitoring profiles associated with the subscriber. Each usage monitoring profile is logically associated with a particular operator offer, and includes the following elements	
Monitoring key	An identifier to a usage monitoring control instance that includes one or more PCC rules	Conditional (NOTE 1)
Usage monitoring level	Indicates the scope of the usage monitoring instance (PDU Session level or per Service)	Optional
Start date	Start date and time when the usage monitoring profile applies	Optional
End date	End date and time when the usage monitoring profile applies	Optional
Volume limit	Maximum allowed traffic volume	Optional
Time limit	Maximum allowed resource time usage	Optional
Reset period	Time period to reset the remaining allowed consumed usage for periodic usage monitoring control (postpaid subscriptions)	Optional
MPS subscription data	This part defines the MPS subscription information in the policy control subscription profile	
MPS priority	Indicates subscription to MPS priority service; priority applies to all traffic on the PDU Session	Conditional (NOTE 1)
IMS signalling priority	Indicates subscription to IMS signalling priority service; priority only applies to IMS signalling traffic	Conditional (NOTE 1)
MPS priority level	Relative priority level for multimedia priority services	Conditional (NOTE 1)
MCS priority	Indicates subscription to MCS priority service; priority applies to all traffic on the PDU Session	Conditional (NOTE 1)
MCS priority level	Relative priority level for MCS services	Conditional (NOTE 1)
NOTE 1: The information is mandatory if the specific part is included in the subscription information (e.g. the monitoring key is mandatory if the usage monitoring information part is included)		

Table 6.2-3: Remaining allowed usage subscription information

Information name	Description	Category
Remaining allowed usage related information	*This part includes a list of Remaining allowed usage associated with the subscriber.*	
Monitoring key	An identifier to a usage monitoring control included one or more PCC rules	Conditional (NOTE 1)
Usage monitoring level	Iindicates the scope of the usage monitoring (PDU Session level or service level)	Optional
Volume usage	Remaining allowed traffic volume	Optional
Time usage	Remaining allowed resource time usage	Optional
NOTE 1: The information is mandatory if the specific part is included in the subscription information (e.g. the monitoring key is mandatory if the usage monitoring information part is included)		

The *Allowed services* may comprise any number of service identifiers allowed for the subscriber in the PDU Session. The PCF maps those service identifiers into PCC rules according to local configuration and operator policies.

The *Subscriber category* may comprise any number of identifiers associated with the subscriber (e.g. gold, silver, etc.). Each identifier associates operator defined policies to the subscriber that belong to that category.

The *Usage monitoring related information* may comprise any number of usage monitoring control instances associated with the subscriber. In each usage monitoring control instance is mandatory to include the *Monitoring key*. The *Reset period* only applies to usage monitoring control instances that periodically reset the allowed usage (e.g. daily, monthly, etc.). If the Reset period is not specified, the usage monitoring control instance ends when the allowed data is consumed or when the *End date* is reached. The usage monitoring related information is used by the PCF instead of the respective information for the subscriber category.

The policy subscription profile may be extended with operator-specific information. Operator-specific extensions may be added both to any specific part of the policy control subscription information (e.g. to the subscriber category part), or as a new optional information block.

Handling of operator specific policy data by the PCF is out of scope of this specification in this release.

The policy control subscription profile information provided by the UDR during the UE Policy Association Establishment procedure using Nudr service for Data Set "Policy Data" and Data Subset "Policy Set Entry" is described in Table 6.2-4.

Table 6.2-4: Policy Set Entry

Information name	Description	Category
Policy Set Entry	List of PSIs and content for each PSI. Content may be Access Network Discovery & Selection Policy Information or UE Route Selection Policy information or both.	Optional

6.2.1.4 V-PCF

The V-PCF is a functional element that encompasses policy control decision functionalities in the VPLMN.

For session management related policy control, the V-PCF only includes functionality for local breakout roaming scenario based on roaming agreements.

For UE policy control, the V-PCF receives the UE policy from the H-PCF and forwards it to the UE via the AMF. The V-PCF can send additional UE policy information (i.e. ANDSP policies) to the UE which is different from the one from H-PCF.

For Access and mobility related policy control, the V-PCF generates the values for RFSP Index, UE-AMBR, Service Area Restriction and SMF selection management.

6.2.1.5 H-PCF

The H-PCF is a functional element that encompasses policy control decision functionalities in the HPLMN.

For session management related policy control, the H-PCF only includes functionality for home routed roaming scenario and provides the same functionality as the PCF in the non-roaming case.

For UE policy control, H-PCF generates the UE policy based on subscription data and transfers the UE policy to the UE via the AMF, or via the V-PCF in the roaming case.

6.2.1.6 Application specific policy information management

The application specific information used for policy control includes:

- Negotiation of BDT information stored in the UDR as Data Set "Policy Data" and Data Subset "Background Data Transfer data": It contains an ASP identifier, Non-IP information or IP 3-tuple to identify the Application server, a transfer policy together with the Background Data Transfer Reference ID, the volume of data to be transferred per UE, the expected amount of UEs and optionally, the subscription to notifications when the BDT policy needs to renegotiated;

- Sponsored data connectivity profile information stored in the UDR as Data Set "Policy Data" and Data Subset "Sponsored data connectivity profile data": It contains a list of ASP identifiers and their applications per sponsor identity;

- Application Function request information for multiple UEs (per group of UEs or all UEs) stored in the UDR as Data Set "Application Data" and Data Subset "AF request information for multiple UEs".

The application specific policy information may be requested/updated by the PCF per AF request.

The management of Application Function request information for multiple UEs is defined in clause 6.3.7.2 of TS 23.501 [2], the management of policies for the negotiation of BDT is defined in clause 6.1.2.4 of this specification and the provision and usage of sponsored data connectivity profile is defined in clause 6.2.1.1 of this specification.

6.2.1.7 Usage monitoring

The PCF supports usage monitoring control for a PDU Session or per Monitoring Key. Usage is defined as either volume or time of user plane traffic.

The PCF may receive usage monitoring related information per DNN and S-NSSAI combination and UE from the UDR, i.e. the overall amount of allowed resources (based either on traffic volume and/or traffic time) that are to be monitored for the PDU Sessions of a user, together with the corresponding remaining allowed usage related information. In addition, usage monitoring related information for Monitoring key(s) per DNN and S-NSSAI combination and UE may also be received from the UDR, together with the corresponding remaining allowed usage related information. For the purpose of usage monitoring per access type, the PCF receives an individual Monitoring key per access type from UDR. Details about the usage monitoring related information and the remaining allowed usage related information provided by the UDR are described in clause 6.2.1.3.

For the purpose of usage monitoring control the PCF shall request the Usage report trigger and provide the necessary usage threshold(s), either volume threshold, time threshold, or both volume threshold and time threshold, upon which the SMF shall report to the PCF. The PCF shall decide if and when to activate usage monitoring to the SMF.

The PCF may provide a Monitoring time to the SMF for the Monitoring keys(s) and optionally specify a subsequent threshold value for the usage after the Monitoring time.

If the SMF reports usage before the Monitoring time is reached, the Monitoring time is not retained by the SMF. Therefore, the PCF may again provide a Monitoring time and optionally the subsequent threshold value for the usage after the Monitoring time in the response.

It shall be possible for the PCF to request a usage report from the SMF.

NOTE 1: The PCF ensures that the number of requests/following policy decisions provided to the SMF do not cause excessive signalling load by e.g. assigning the same time for the report only for a preconfigured number of PDU Sessions.

Once the PCF receives a usage report from the SMF the PCF shall deduct the value of the usage report from the remaining allowed usage for that DNN and S-NSSAI combination and UE (if usage per PDU Session is reported). If usage is reported from the SMF, the PCF shall deduct the value of the usage report from the remaining allowed usage

for individual Monitoring key(s) for that DNN and S-NSSAI combination and UE (if usage for one or several Monitoring keys is reported).

NOTE 2: The PCF maintains usage thresholds for each Monitoring key and PDU Session that is active for a certain DNN and S-NSSAI combination and UE. Updating the remaining allowed usage after the SMF reporting, minimizes the risk of exceeding the usage allowance.

If the remaining allowed usage reaches a value of zero (or below zero), the PCF may apply other policy decisions and interact with the SMF accordingly.

If the SMF reports usage for a certain Monitoring key and if monitoring shall continue for that Monitoring key then the PCF shall provide new threshold value(s) in the response to the SMF respectively. If Monitoring time and subsequent threshold value are used then the PCF provides them to the SMF as well.

The PCF may provide a new volume threshold and/or a new time threshold to the SMF, the new threshold values overrides the existing threshold values in the SMF.

If monitoring shall no longer continue for that Monitoring key, then the PCF shall not provide a new threshold in the response to the SMF.

If the last PDU Session of a user for a DNN and S-NSSAI combination is terminated, the PCF shall store the remaining allowed usage, i.e. the information about the remaining overall amount of resources, in the UDR.

If the End date of the usage monitoring related information (see clause 6.2.1.3 for details) is reached, the PCF shall reset the remaining allowed usage to the value(s) indicated in the usage monitoring related information and shall then interact with the SMF to undo any previously applied policy decisions related to remaining allowed usage of zero (or below zero).

6.2.1.8 Sponsored data connectivity

The PCF may authorise an application service provider to request specific PCC decisions (e.g. authorisation to request sponsored IP flows, authorisation to request QoS resources) based on sponsored data connectivity profile from the UDR. For sponsored data connectivity, the PCF may receive a usage threshold from the AF. If the AF specifies a usage threshold, the PCF shall use the Sponsor Identity to construct a Monitoring key for monitoring the volume, time, or both volume and time of user plane traffic, and invoke usage monitoring on the SMF. The PCF shall notify the AF when the SMF reports that a usage threshold for the Monitoring key is reached provided that the AF requests to be notified for this event, as described in clause 6.1.3.18. If the usage threshold is reached, the AF may terminate the AF session or provide a new usage threshold to the PCF. Alternatively, the AF may allow the session to continue without specifying a usage threshold. If the AF decides to allow the session to continue without specifying a usage threshold, then monitoring in the SMF shall be discontinued for that monitoring key by the PCF, unless there are other reasons for continuing the monitoring.

If the H-PCF detects that the UE is in a home-routed roaming scenario when sponsored data connectivity is requested by an AF, it may allow the sponsored data connectivity in the service authorization request, reject the service authorization request, or initiate the AF session termination based on home operator policy.

NOTE: Sponsored data connectivity is not supported in the roaming with local breakout scenario in this Release.

If the AF revokes the service information and the AF has notified previously a usage threshold to the PCF, the PCF shall report the usage up to the time of the revocation of service authorization.

If the PDU Session terminates and the AF has specified a usage threshold then the PCF shall notify the AF of the accumulated usage (i.e. either volume, or time, or both volume and time) of user plane traffic since the last usage report.

6.2.2 Session Management Function (SMF)

6.2.2.1 General

The SMF is responsible for the enforcement of the policy decisions related to service data flow detection, authorized QoS, charging, gating, traffic usage reporting, packet routing and forwarding and traffic steering. The SMF controls the policy and charging enforcement which includes the binding of service data flows to QoS Flows (as described in clause 6.1.3.2.4) as well as the interaction with the CHF. The SMF interacts with the UPF(s), the RAN and the UE to achieve the appropriate treatment of the user plane traffic.

The SMF control of the UPF(s) is described in TS 23.501 [2] as well as the interaction principles between SMF and RAN and between SMF and UE. The procedures for the interaction between SMF and UPF, SMF and RAN as well as SMF and UE are described in TS 23.502 [3].

The SMF is enforcing the Policy Control as indicated by the PCF in two different ways:

- Gate enforcement. The SMF shall instruct the UPF to allow a service data flow, which is subject to policy control, to pass through the UPF if and only if the corresponding gate is open;
- QoS enforcement:
  - 5QI corresponding with 5G QoS Characteristics. The SMF shall be able to convert a 5QI value to 5G QoS Characteristics values.
  - PCC rule QoS enforcement. The SMF shall instruct the UPF to enforce the authorized QoS of a service data flow according to the active PCC rule (e.g. to enforce DSCP marking).
  - QoS Flow QoS enforcement. The SMF controls the QoS that is provided to a combined set of service data flows. The policy enforcement function ensures that the resources which can be used by an authorized set of service data flows are within the "authorized resources" specified by the PCF. The authorized QoS provides an upper bound on the resources that can be reserved (GFBR) or allocated (MFBR) for the QoS Flow. During QoS Flow QoS enforcement, if packet filters are provided to the UE, the SMF shall provide packet filters with the same content as that in the SDF template filters received from the PCF.

The SMF is enforcing the charging control in the following way:

- For a service data flow (defined by an active PCC rule) that is subject to charging control, the SMF shall allow the service data flow to pass through the UPF if and only if there is a corresponding active PCC rule with and, for online charging, the CHF has authorized credit for the charging key. The SMF may let a service data flow pass through the UPF during the course of the credit re-authorization procedure.

For a service data flow (defined by an active PCC rule) that is subject to both Policy Control and Charging Control, the SMF shall allow the service data flow to pass through the UPF if and only if the right conditions from both policy control and charging control happen. i.e. the corresponding gate is open and in the case of online charging the CHF has authorized credit for its charging key.

For a service data flow (defined by an active PCC rule) that is subject to policy control only and not charging control, the SMF shall allow the service data flow to pass through the UPF if and only if the conditions for policy control are met.

A SMF may be served by one or more PCF nodes. The SMF shall contact the appropriate PCF as described in clause 6.3.7.1 of TS 23.501 [2].

The operator may configure an indicator in UDM which is delivered to the SMF within the Charging Characteristics and used by the SMF to not establish the SM Policy Association during the PDU Session establishment procedure.

NOTE 1: The decision to not establish the SM Policy Association applies for the life time of the PDU Session.

NOTE 2: The indicator in the UDM is operator specific, therefore its value is understood within the HPLMN and can be used in both non-roaming or home routed roaming cases.

The SMF shall, on request from the PCF, modify a PCC rule, using the equivalent SMF behaviour as the removal of the old and the activation of the new (modified) PCC rule. The SMF shall modify a PCC rule as an atomic operation. The SMF shall not modify a predefined PCC rule on request from the PCF.

The SMF should support predefined PCC rules.

The SMF shall gather and report QoS Flow usage information according to clause 6.1.3.3. The SMF may have a pre-configured Default charging method. Upon the initial interaction with the PCF, the SMF shall provide pre-configured Default charging method if available.

At PDU Session establishment the SMF shall initiate the SM Policy Association Establishment procedure. If no PCC rule was activated for the PDU Session, the SMF shall reject the PDU Session establishment.

If there is no PCC rule active for a successfully established PDU Session at any later point in time, e.g. through a PCF initiated SM Policy Association Modification, the SMF shall initiate a PDU Session termination procedure. If the PCF terminates the SM Policy Association, the SMF shall initiate a PDU Session termination procedure.

If there is no PCC rule active for a successfully established QoS Flow at any later point in time, e.g. through a PCF triggered SM Policy Association Modification, the SMF shall initiate a PDU Session Modification procedure an terminate the QoS Flow.

If the PDU Session is modified, e.g. by changing the characteristics for an QoS Flow, the SMF shall first use the Policy Control Request Trigger to determine whether to request the PCC rules for the modified PDU Session from the PCF; afterwards, the SMF shall use the re-authorisation triggers, if available, in order to determine whether to require re-authorisation for the PCC rules that were either unaffected or modified. If the SMF receives an unsolicited update of the PCC rules from the PCF, the PCC rules shall be activated, modified or removed as indicated by the PCF.

The SMF shall inform the PCF about the outcome of a PCC rule operation. If a QoS Flow cannot be established or modified to satisfy the QoS Flow binding, then the SMF shall reject the activation of a PCC rule. If the SMF is requested to notify the PCF about a successful resource allocation (see clause 6.1.3.5) and the currently fulfilled QoS of an established or modified QoS Flow matches an Alternative QoS Profile (as described in clause 5.7.2.4.3 of TS 23.501 [2]), the SMF shall also provide to the PCF the reference to the Alternative QoS parameter set corresponding to the Alternative QoS Profile referenced by the RAN.

The SMF shall inform the PCF about any removal of a PCC rule, that the PCF has activated, that occurs without explicit instruction from the PCF.

When QoS Flow resources are released, i.e. at SM Policy Association termination or SMF-initiated SM Policy Association modification notifying that PCC Rules are removed, the SMF shall also provide, if available, the reason why resources are released, i.e. RAN/NAS Release Cause.

NOTE 3: In the case of a rejection of a PCC rule activation the PCF may e.g. modify the attempted PCC rule, de-activate or modify other PCC rules and retry activation or abort the activation attempt and, if applicable, inform the AF that transmission resources are not available.

The SMF forwards the Maximum Packet Loss Rate for UL and DL, if received from PCF for the PCC rule bound to a 5QI=1 QoS Flow. In the case multiple PCC Rules share one 5QI=1 QoS Flow and the SMF received multiple Maximum Packet Loss Rates, the SMF chooses the lowest value per direction related to these PCC rules.

When the PCF provides updated PCC rules for the PDU Session to the SMF, and the PCC rules were not enforced due to that the UE is in suspend state, e.g. due to SRVCC to GERAN without DTM support as specified in clause 6.2.2.1 in the TS 23.216 [25] or CSFB to UTRAN without PS Handover as specified in clause 6.5 in the TS 23.272 [26], the SMF shall indicate to the PCF that the PCC Rules were not enforced with the reason that the UE is in suspend state. Upon reception of the failure indication, the PCF may subscribe to UE resumed from suspend state event trigger.

NOTE 4: This above description applies in the case of EPC interworking.

6.2.2.2 Service data flow detection

The Service Data Flow detection uses the service data flow template included in a PCC Rule provide by the PCF. The service data flow template defines the data for the service data flow detection as a set of service data flow filters or an application identifier referring to an application detection filter. The SMF maps the service data flow template in the PCC Rule into the detection information in a Packet Detection Rules to the UPF as described in TS 23.501 [2].

The application detection filters provided to the SMF may be extended with the PFDs provided by the NEF (PFDF). How the SMF uses the service data flow detection capabilities in the UPF is described in clause 5.8.2 of TS 23.501 [2].

For IP PDU Session type and Ethernet PDU Session type, the service data flow filters that may apply for traffic on a PDU Session are defined in clause 5.7.6 of TS 23.501 [2]. The following specifics apply:

- Each service data flow template may contain any number of service data flow filters;
- Each service data flow filter is applicable uplink, downlink or both uplink and downlink;

NOTE 1: Service data flow filters that apply in both uplink and downlink should be used whenever possible.

- Each service data flow filter may contain information about whether the explicit signalling of the corresponding traffic mapping information to the UE is required.

NOTE 2: This information enables e.g. the generation/removal of traffic mapping information for the UE as well as the usage of PCC rules with specific service data flow filters on the QoS Flow associated with the default QoS rule without the need to generate traffic mapping information.

6.2.2.3 Measurement

The SMF shall ensure that the UPF supports data volume, duration, combined volume/duration and event based measurement for charging. The Measurement method indicates what measurement type is applicable to the PCC rule.

NOTE 1: Event based charging is only applicable to predefined PCC rules and PCC rules using an application detection filter (i.e. with an application identifier).

The SMF shall ensure that the UPF measurement measures all the user plane traffic, except traffic that PCC causes to be discarded.

The SMF shall ensure that the UPF maintains a measurement per QoS Flow, and Charging Key combination.

If Service identifier level reporting is mandated in a PCC rule, the SMF shall ensure that the UPF maintains a measurement for that Charging Key and Service Identifier combination, for the QoS Flow.

NOTE 2: In addition, the SMF may instruct the UPF to maintain QoS Flow level measurement if required by the operator.

For usage monitoring, the SMF shall ensure that the UPF supports volume and time measurement for a PDU Session and maintains a measurement for each PDU Session for which the PCF has requested the Usage report trigger and provided threshold values on a PDU Session level. The SMF shall ensure that the UPF is able to support volume and time measurements simultaneously for a given PDU Session.

The SMF shall ensure that the UPF supports volume and time measurement per Monitoring key and maintain a measurement for each Monitoring key if the PCF has requested the Usage report trigger and provided threshold values on Monitoring key level. The SMF shall ensure that the UPF is able to support volume and time measurements simultaneously for a given Monitoring Key.

The SMF shall ensure that the UPF supports simultaneous volume and time measurement for usage monitoring on PDU Session level and Monitoring key level for the same PDU Session.

Volume and time measurements for usage monitoring purposes on PDU Session level and on Monitoring key level shall be performed independently of each other. If the PCC rule is associated with an indication of exclusion from session level monitoring, the SMF shall ensure that the UPF does not consider the corresponding service data flow for the volume and time measurement on PDU Session level.

If the Usage report reached Policy Control Request Trigger is set and a volume or a time threshold is reached, the SMF shall report this event to the PCF. The SMF shall continue to perform volume or time measurement after the threshold is reached and before a new threshold is provided by the PCF. At PDU Session termination or if the conditions defined in clause 6.4 for continued monitoring are no longer met, or if the PCF explicitly requests a usage report, the SMF shall inform the PCF about the resources that have been consumed by the user since the last usage report for the affected Monitoring keys, including the resources consumed before and after the Monitoring time was reached, if provided according to clause 6.2.1.1.

If combined volume and time measurements are requested by the PCF, then the reporting shall be done for both together. For example, if the volume threshold is reached, the consumed time shall be reported as well and, in order to continue combined volume and time measurements, the PCF shall provide a new time threshold along with a new volume threshold. The SMF shall continue to instruct the UPF to perform volume and time measurement after the threshold is reached and before a new threshold is provided by the PCF. If new threshold is provided only for time or volume, then the measurements shall continue only for that provided type and the SMF shall ensure that the accumulated usage for the non provided type is discarded by the UPF.

When the PCF requests to report usage, the SMF shall report the accumulated usage to the PCF according to the provided usage threshold, i.e. the SMF reports accumulated volume when the volume threshold was provided by the PCF, accumulated time when the time threshold was provided by the PCF and both accumulated volume and accumulated time when volume threshold and time threshold were provided by the PCF.

If the Usage thresholds for a Monitoring key are not provided to the SMF in the acknowledgement of a PDU Session modification where its usage was reported, then the usage monitoring shall not continue in the SMF for that Monitoring key.

When the Monitoring time occurs, the accumulated volume and/or time usage shall be recorded by the UPF and reported to the SMF, and:

- If the subsequent usage threshold value is provided, the usage threshold shall be reset to this value by the SMF.
- Otherwise, the usage threshold shall be set by the SMF to the remaining value of the threshold previously sent by the PCF (i.e. excluding the accumulated usage).

The first usage report after the Monitoring Time was reached shall indicate the usage up to the Monitoring time and usage after the Monitoring time.

In order to support time based usage monitoring, the PCF may optionally indicate to the SMF, along with other usage monitoring information provided, the Inactivity Detection Time. This value represents the time interval after which the time measurement shall stop for the Monitoring key, if no packets are received belonging to the corresponding Monitoring Key during that time period. Time measurement shall resume on receipt of a further packet belonging to the Monitoring key.

Time measurement for a Monitoring key shall also be stopped when time based usage monitoring is disabled, if this happens before the Inactivity Detection Time is reached.

If an Inactivity Detection Time value of zero is provided, or if no Inactivity Detection Time is present within the usage monitoring information provided by the PCF, the time measurement shall be performed continuously from the point at which it was started until time based usage monitoring is disabled.

The SMF instructs the UPF to provide usage reports to the SMF as described in TS 23.501, clause 5.8.2.6.

6.2.2.4 QoS control

The SMF receives the authorized QoS for a service data flow in the PCC rule. The SMF derives the QoS parameters for a QoS Flow (other than the QoS Flow associated with the default QoS rule) based on the PCC rule information of the PCC rule(s) bound to this QoS Flow:

- The SMF shall set the QoS Flow parameters 5QI and ARP to the values of the corresponding PCC rule parameters.
- For the QoS Flow parameters QNC, Priority Level, Averaging Window and Maximum Data Burst Volume, the SMF shall use the corresponding PCC rule parameters if they are available in the PCC rule.
- For GBR QoS Flows, the SMF should set the GFBR to the sum of the GBRs of all PCC rules that are active and bound to that QoS Flow and the MFBR to the sum of the MBRs of all PCC rules that are active and bound to that GBR QoS Flow. If a set of PCC Rules is subject to resource sharing as specified in clause 6.1.3.13 the SMF should use, for each applicable direction, the highest GBR from the set of PCC Rules sharing resources as input for calculating the GFBR and may use, for each applicable direction, the highest MBR from the set of PCC Rules as input for calculating the MFBR.
- For GBR QoS Flows, the SMF shall set the QoS Flow parameter Maximum Packet Loss Rate for UL and DL if the corresponding PCC rule parameters are available in the PCC rule. In the case multiple PCC Rules are bound to the QoS Flow and the SMF received multiple Maximum Packet Loss Rates, the SMF chooses the lowest value per direction in all these PCC rules.
- If the PCC rule contains a non-standardized 5QI, the SMF shall also provide the corresponding 5G QoS characteristics parameters (as received in the PDU Session related information Explicitly signalled QoS Characteristics) for the QoS Flow.
- If the PCC rule contains Alternative QoS Parameter Sets, the SMF shall provide their attributes as Alternative QoS Profile(s) (see clause 5.7.1.2a of TS 23.501 [2]) in the same prioritized order (in which they occur in the PCC rule) in addition to the QoS parameters for the QoS Flow.

The SMF shall set the QoS parameters of the QoS Flow associated with the default QoS rule to:

- the PCC rule parameters contained in the PCC rule that is bound to this QoS Flow (in the way it is described above) if the PCC rule attribute Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters is present; or otherwise

- the Authorized default 5QI/ARP received in the PDU Session related information. If the Authorized default 5QI contains a non-standardized 5QI, the SMF shall also provide the corresponding 5G QoS characteristics parameters (as received in the PDU Session related information Explicitly signalled QoS Characteristics) for the QoS Flow associated with the default QoS rule.

The SMF receives the Authorized Session-AMBR in the PDU Session related information. The SMF ensures that the Authorized Session-AMBR for a PDU Session is enforced for bandwidth policing at the UPF(s) as described in clause 5.7.1 of TS 23.501 [2].

The SMF generates QoS rule(s) as described in TS 23.501 [2]. For a PDU Session of unstructured type, only one PCC Rule allowing all packets is to be activated in the SMF and only the QoS Flow associated with the default QoS rule exists as described in clause 5.7.1 of TS 23.501 [2].

6.2.2.5 Application detection

The SMF shall instruct the UPF to detect the Start and Stop of the application traffic for the PCC rules used for application detection (i.e. with application identifier) that the PCF has activated at the SMF.

If the PCF has subscribed to the event and notification is not muted for the specific PCC Rule, the SMF shall also instruct the UPF to report the Start/Stop of application, as described in the TS 23.501 [2].

When receiving the application detection report from UPF, the SMF shall forward the application identifier, the start/stop indication and, when service data flow descriptions were deduced, the application instance identifier(s) and the service data flow description(s), to the PCF.

NOTE: The PCF can make policy decision when receiving the application detection report.

6.2.2.6 Traffic steering

The SMF shall support traffic steering control as defined in Clause 6.1.3.14.

The SMF may be configured with the traffic steering policy IDs related to the mechanism enabling traffic steering to the N6-LAN, DN and/or DNAIs associated with N6 traffic routing requirements.

Upon receiving a PCC rule which contains the traffic steering control information, the SMF shall provide the information to the UPF for the enforcement. The traffic steering control information in the PCC rule may include a set of DNAI(s) and for each DNAI a traffic steering policy ID and/or N6 traffic routing information dynamically provided by the AF.

Based on the received traffic steering policy ID(s), the UPF may remove or insert VLAN tags on N6 interface for downlink and uplink frames, respectively. The details of the scenario is defined in clause 5.6.10.2 of TS 23.501 [2].

NOTE: The UPF can, for example, perform marking packets in order to indicate a certain type of traffic to the DN side of the N6 reference point which enables those packets to be steered in the DN. As another example the UPF can forward, i.e. offload, traffic identified by the traffic descriptor to a local tunnel.

6.2.2.7 Access Traffic Steering, Switching and Splitting

The SMF may support functionality for traffic steering, switching and splitting within a MA PDU Session, as described in TS 23.501 [2].

Upon receiving a PCC rule which contains the MA PDU Session Control information, the SMF shall instruct the UPF accordingly and shall also create and provide applicable ATSSS rules to the UE (the details for both SMF actions are described in TS 23.501 [2]).

6.2.3 Application Function (AF)

The Application Function (AF) is an element offering applications that require dynamic policy and/or charging control over the user plane behaviour and/or an element requesting non-session based network capability exposure. The AF

shall communicate with the PCF to transfer dynamic session information, required for PCF decisions as well as to receive access network specific information and notifications about events related to the PDU Session or the QoS Flow transferring the application traffic. One example of an AF is the P-CSCF of the IM CN subsystem.

An AF may communicate with multiple PCFs. The mechanism for an AF to select the PCF associated to a PDU Session based on the UE address is described in clause 6.1.1.2.

AF may contact the PCF via the NEF for network capability exposure as defined in clause 4.3.6.

The AF may receive an indication that the service information is not accepted by the PCF together with service information that the PCF would accept. In that case, the AF rejects the service establishment towards the UE. If possible, the AF forwards the service information to the UE that the PCF would accept.

For certain events related to policy control, the AF shall be able to give instructions to the PCF to act on its own, i.e. based on the service information currently available as described in clause 6.1.3.6.

NOTE 1: The QoS authorization based on incomplete service information is required for e.g. IMS session setup scenarios with available resources on originating side and a need for resource reservation on terminating side.

The AF may request the PCF to report events related to the PDU Session or the QoS Flow transferring the application traffic as defined in clause 6.1.3.18. The AF may use the access network specific information and notifications about events in the AF session signalling or to adjust the event reporting related to the PDU Session or the QoS Flow transferring the application traffic.

The AF may contact the PCF via the NEF to request a time window and related conditions for future BDT. Details of the AF behaviour to support future BDT are defined in clause 6.1.2.4.

To support sponsored data connectivity the AF may provide the PCF with the sponsored data connectivity information, including optionally a usage threshold, as specified in clause 6.2.1.1. The AF may request the PCF to report events related to sponsored data connectivity.

NOTE 2: Annex D describes the scenario for sponsored data connectivity.

The AF may receive a request to terminate an AF session. The PCF may include an indication that the transmission resources are lost due to PS to CS handover.

NOTE 3: The AF action upon reception of the indication that the transmission resources are lost due to PS to CS handover is application specific. The IMS uses the indication to prevent a termination of an ongoing session as specified in TS 24.229 [29] and TS 24.237 [30].

6.2.4 Unified Data Repository (UDR)

The Unified Data Repository (UDR) is defined in TS 23.501 [2].

6.2.5 Charging Function (CHF)

The Charging Function is specified in TS 32.240 [8].

6.2.6 Void

6.2.7 Network Exposure Function (NEF)

The Network Exposure Function (NEF) is defined in TS 23.501 [2] and additionally supports the following policy related functionalities:

- Service specific policy and charging control;
- Management of packet flow descriptions;
- Sponsor data connectivity including usage monitoring (as defined in clause 6.2.1.1);

- Negotiations for future BDT.

6.2.8 Access and Mobility Management Function (AMF)

The Access and Mobility Management Function (AMF) is defined in TS 23.501 [2] and additionally supports the following policy related functionalities:

- Enforcement of access and mobility related policies received from the PCF;
- Transfers of UE policy information received from the PCF to the UE via N1 interface;
- Reporting of events to the PCF that the PCF has subscribed to.

6.2.9 Network Data Analytics Function (NWDAF)

The Network Data Analytics Function (NWDAF) is defined in TS 23.288 [24].

6.3 Policy and charging control rule

6.3.1 General

The Policy and charging control rule (PCC rule) comprises the information that is required to enable the user plane detection of, the policy control and proper charging for a service data flow. The packets detected by applying the service data flow template of a PCC rule form a service data flow.

Two different types of PCC rules exist: Dynamic rules and predefined rules. The dynamic PCC rules are provisioned by the PCF to the SMF, while the predefined PCC rules are configured into the SMF, as described in TS 23.501 [2], and only referenced by the PCF.

NOTE 1: The procedure for provisioning predefined PCC rules is out of scope for this specification.

The operator defines the PCC rules.

Table 6.3.1 lists the information contained in a PCC rule, including the information name, the description and whether the PCF may modify this information in a dynamic PCC rule which is active in the SMF. The Category field indicates if a certain piece of information is mandatory or not for the construction of a PCC rule, i.e. if it is possible to construct a PCC rule without it.

The differences with table 6.3 in TS 23.203 [4] are shown, either "none" means that the IE applies in 5GS or "removed" meaning that the IE does not apply in 5GS, this is due to the lack of support in the 5GS for this feature or "modified" meaning that the IE applies with some modifications defined in the IE.

Table 6.3.1: The PCC rule information in 5GC

Information name	Description	Category	PCF permitted to modify for a dynamic PCC rule in the SMF	Differences compared with table 6.3. in TS 23.203 [4]
Rule identifier	Uniquely identifies the PCC rule, within a PDU Session. It is used between PCF and SMF for referencing PCC rules.	Mandatory	No	None
Service data flow detection	*This part defines the method for detecting packets belonging to a service data flow.*			
Precedence	Determines the order, in which the service data flow templates are applied at service data flow detection, enforcement and charging. (NOTE 1).	Conditional (NOTE 2)	Yes	None
Service data flow template	For IP PDU traffic: Either a list of service data flow filters or an application identifier that references the corresponding application detection filter for the detection of the service data flow. For Ethernet PDU traffic: Combination of traffic patterns of the Ethernet PDU traffic. It is defined in clause 5.7.6.3 of TS 23.501 [2].	Mandatory (NOTE 3)	Conditional (NOTE 4)	Modified (packet filters for Ethernet PDU traffic added)
Mute for notification	Defines whether application's start or stop notification is to be muted.	Conditional (NOTE 5)	No	None
Charging	*This part defines identities and instructions for charging and accounting that is required for an access point where flow based charging is configured*			
Charging key (NOTE 22)	The charging system (CHF) uses the charging key to determine the tariff to apply to the service data flow.		Yes	None
Service identifier	The identity of the service or service component the service data flow in a rule relates to.		Yes	None
Sponsor Identifier	An identifier, provided from the AF which identifies the Sponsor, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional (NOTE 6)	Yes	None
Application Service Provider Identifier	An identifier, provided from the AF which identifies the Application Service Provider, used for sponsored flows to correlate measurements from different users for accounting purposes.	Conditional (NOTE 6)	Yes	None
Charging method	Indicates the required charging method for the PCC rule. Values: online or offline or neither.	Conditional (NOTE 7)	No	None
Service Data flow handling while requesting credit	Indicates whether the service data flow is allowed to start while the SMF is waiting for the response to the credit request. Only applicable for charging method online. Values: blocking or non-blocking		No	New

Information name	Description	Category	PCF permitted to modify for a dynamic PCC rule in the SMF	Differences compared with table 6.3. in TS 23.203 [4]
Measurement method	Indicates whether the service data flow data volume, duration, combined volume/duration or event shall be measured. This is applicable to reporting, if the charging method is online or offline. Note: Event based charging is only applicable to predefined PCC rules and PCC rules used for application detection filter (i.e. with an application identifier).		Yes	None
Application Function Record Information	An identifier, provided from the AF, correlating the measurement for the Charging key/Service identifier values in this PCC rule with application level reports.		No	None
Service Identifier Level Reporting	Indicates that separate usage reports shall be generated for this Service Identifier. Values: mandated or not required		Yes	None
Policy control	*This part defines how to apply policy control for the service data flow.*			
Gate status	The gate status indicates whether the service data flow, detected by the service data flow template, may pass (Gate is open) or shall be discarded (Gate is closed).		Yes	None
5G QoS Identifier (5QI)	The 5QI authorized for the service data flow.	Conditional (NOTE 10)	Yes	Modified (corresponds to QCI in TS 23.203 [4])
QoS Notification Control (QNC)	Indicates whether notifications are requested from 3GPP RAN when the GFBR can no longer (or can again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow.	Conditional (NOTE 15)	Yes	Added
Reflective QoS Control	Indicates to apply reflective QoS for the SDF.		Yes	Added
UL-maximum bitrate	The uplink maximum bitrate authorized for the service data flow		Yes	None
DL-maximum bitrate	The downlink maximum bitrate authorized for the service data flow		Yes	None
UL-guaranteed bitrate	The uplink guaranteed bitrate authorized for the service data flow		Yes	None
DL-guaranteed bitrate	The downlink guaranteed bitrate authorized for the service data flow		Yes	None
UL sharing indication	Indicates resource sharing in uplink direction with service data flows having the same value in their PCC rule		No	None
DL sharing indication	Indicates resource sharing in downlink direction with service data flows having the same value in their PCC rule		No	None
Redirect	Redirect state of the service data flow (enabled/disabled)	Conditional (NOTE 8)	Yes	None
Redirect Destination	Controlled Address to which the service data flow is redirected when redirect is enabled	Conditional (NOTE 9)	Yes	None
ARP	The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability	Conditional (NOTE 10)	Yes	None

Information name	Description	Category	PCF permitted to modify for a dynamic PCC rule in the SMF	Differences compared with table 6.3. in TS 23.203 [4]
Bind to QoS Flow associated with the default QoS rule	Indicates that the dynamic PCC rule shall always have its binding with the QoS Flow associated with the default QoS rule (NOTE 11).		Yes	Modified (corresponds to bind to the default bearer in TS 23.203 [4])
Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters	Indicates that the dynamic PCC rule shall always have its binding with the QoS Flow associated with the default QoS rule. It also indicates that the that the QoS related attributes of the PCC rule shall be applied to derive the QoS parameters of the QoS Flow associated with the default QoS rule instead of the PDU Session related parameters Authorized default 5QI/ARP.	Conditional (NOTE 17)	Yes	Added
PS to CS session continuity	Indicates whether the service data flow is a candidate for vSRVCC.			Removed
Priority Level	Indicates a priority in scheduling resources among QoS Flows (NOTE 14).		Yes	Added
Averaging Window	Represents the duration over which the guaranteed and maximum bitrate shall be calculated (NOTE 14).		Yes	Added
Maximum Data Burst Volume	Denotes the largest amount of data that is required to be transferred within a period of 5G-AN PDB (NOTE 14).		Yes	Added
Disable UE notifications at changes related to Alternative QoS Profiles	Indicates to disable QoS Flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation. The fulfilled situation is either the QoS profile or an Alternative QoS Profile.	Conditional (NOTE 25)	Yes	Added
Access Network Information Reporting	*This part describes access network information to be reported for the PCC rule when the corresponding QoS Flow is established, modified or terminated.*			
User Location Report	The serving cell of the UE is to be reported. When the corresponding QoS Flow is deactivated, and if available, information on when the UE was last known to be in that location is also to be reported.		Yes	None
UE Timezone Report	The time zone of the UE is to be reported.		Yes	None
Usage Monitoring Control	*This part describes identities required for Usage Monitoring Control.*			None
Monitoring key (NOTE 23)	The PCF uses the monitoring key to group services that share a common allowed usage.		Yes	None
Indication of exclusion from session level monitoring	Indicates that the service data flow shall be excluded from PDU Session usage monitoring		Yes	None
N6-LAN Traffic Steering Enforcement Control (NOTE 18)	*This part describes information required for N6-LAN Traffic Steering.*			

Information name	Description	Category	PCF permitted to modify for a dynamic PCC rule in the SMF	Differences compared with table 6.3. in TS 23.203 [4]
Traffic steering policy identifier(s)	Reference to a pre-configured traffic steering policy at the SMF (NOTE 12).		Yes	None
AF influenced Traffic Steering Enforcement Control (NOTE 18)	*This part describes information required for AF influenced Traffic Steering.*			
Data Network Access Identifier	Identifier(s) of the target Data Network Access (DNAI). It is defined in clause 5.6.7 of TS 23.501 [2].		Yes	Added
Per DNAI: Traffic steering policy identifier	Reference to a pre-configured traffic steering policy at the SMF (NOTE 19).		Yes	Added
Per DNAI: N6 traffic routing information	Describes the information necessary for traffic steering to the DNAI. It is described in clause 5.6.7 of TS 23.501 [2] (NOTE 19).		Yes	Added
Information on AF subscription to UP change events	Indicates whether notifications in the case of change of UP path are requested and optionally indicates whether acknowledgment to the notifications shall be expected (as defined in clause 5.6.7 of TS 23.501 [2]).		Yes	Added
Indication of UE IP address preservation	Indicates UE IP address should be preserved. It is defined in clause 5.6.7 of TS 23.501 [2].		Yes	Added
Indication of traffic correlation	Indicates that the target PDU Sessions should be correlated via a common DNAI in the user plane. It is described in clause 5.6.7 of TS 23.501 [2].		Yes	Added
NBIFOM related control Information	*This part describes PCC rule information related with NBIFOM*			
Allowed Access Type	The access to be used for traffic identified by the PCC rule			Removed
RAN support information	*This part defines information supporting the RAN for e.g. handover threshold decision.*			
UL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the uplink direction for the service data flow. It is defined in clause 5.7.2.8 of TS 23.501 [2].	Conditional (NOTE 13)	Yes	None
DL Maximum Packet Loss Rate	The maximum rate for lost packets that can be tolerated in the downlink direction for the service data flow. It is defined in clause 5.7.2.8 of TS 23.501 [2].	Conditional (NOTE 13)	Yes	None
MA PDU Session Control (NOTE 20)	*This part defines information supporting control of MA PDU Sessions*		Yes	New
Application descriptors	identifies the application traffic to apply the Steering Functionality and the Steering mode. It is described in clause 5.32.8 of TS 23.501 [2].	Conditional (NOTE 27)	Yes	New
Steering Functionality	Indicates the applicable traffic steering functionality.	Conditional (NOTE 21)	Yes	New
Steering mode	Indicates the rule for distributing traffic between accesses together with associated parameters (if any).	Conditional (NOTE 21)	Yes	New

Information name	Description	Category	PCF permitted to modify for a dynamic PCC rule in the SMF	Differences compared with table 6.3. in TS 23.203 [4]
Charging key for Non-3GPP access (NOTE 22)	Indicates the Charging key used for charging packets carried via Non-3GPP access for a MA PDU Session.		Yes	New
Monitoring key for Non-3GPP access (NOTE 23)	Indicates the Monitoring key used to monitor usage of the packets carried via Non-3GPP access for a MA PDU Session.		Yes	New
QoS Monitoring for URLLC	*This part describes PCC rule information related with QoS Monitoring for URLLC.*			
QoS parameter(s) to be measured	UL packet delay, DL packet delay or round trip packet delay.		Yes	Added
Reporting frequency	Defines the frequency for the reporting, such as event triggered, periodic.		Yes	Added
Target of reporting	Defines the target of the QoS Monitoring reports, it can be either the PCF or the AF, decided by the PCF.		Yes	Added
Alternative QoS Parameter Sets (NOTE 24) (NOTE 26)	*This part defines Alternative QoS Parameter Sets for the service data flow.*			
Packet Delay Budget	The Packet Delay Budget in this Alternative QoS Parameter Set.		Yes	Added
Packet Error Rate	The Packet Error Rate in this Alternative QoS Parameter Set.		Yes	Added
UL-guaranteed bitrate	The uplink guaranteed bitrate in this Alternative QoS Parameter Set.		Yes	Added
DL-guaranteed bitrate	The downlink guaranteed bitrate in this Alternative QoS Parameter Set.		Yes	Added
TSC Assistance Container	*This part defines parameters provided by TSN AF. Following are the parameters:* - *Burst Arrival Time - Indicates the burst arrival time in reference to TSN GM and ingress port.* - *Periodicity The time period (in reference to TSN GM) between start of two bursts.* - *Flow Direction: Direction of the flow.*		No	Added
Downlink Data Notification Control	*This part describes information required for controlling the sending of Downlink data delivery status event and DDN Failure event notifications as specified in clause 4.15.3 of TS 23.502 [3].*			
Notification control for DDD status	Indicates that notifications of downlink data delivery status are required and the requested type of such notifications.		Yes	Added
Notification Control for DDN Failure	Indicates that notifications of DDN Failure are required.		Yes	Added

Information name	Description	Category	PCF permitted to modify for a dynamic PCC rule in the SMF	Differences compared with table 6.3. in TS 23.203 [4]
NOTE 1: For PCC rules based on an application detection filter, the precedence is only relevant for the enforcement, i.e. when multiple PCC rules overlap, only the enforcement, reporting of application starts and stops, monitoring, and charging actions of the PCC rule with the highest precedence shall be applied. NOTE 2: The Precedence is mandatory for PCC rules with SDF template containing SDF filter(s). For dynamic PCC rules with SDF template containing an application identifier, the precedence is either preconfigured in SMF or provided in the PCC rule from PCF. NOTE 3: Either service data flow filter(s) or application identifier shall be defined per each rule. NOTE 4: YES, if the service data flow template consists of a set of service data flow filters. NO if the service data flow template consists of an application identifier NOTE 5: Optional and applicable only if application identifier exists within the rule. NOTE 6: Applicable to sponsored data connectivity. NOTE 7: Mandatory if there is no default charging method for the PDU Session. NOTE 8: Optional and applicable only if application identifier exists within the rule. NOTE 9: If Redirect is enabled. NOTE 10: Mandatory when Bind to QoS Flow associated with the default QoS rule is not present. NOTE 11: The presence of this attribute causes the 5QI/ARP/QNC/Priority Level/Averaging Window/Maximum Data Burst Volume of the rule to be ignored for the QoS Flow binding. NOTE 12: The Traffic steering policy identifier can be different for uplink and downlink direction. If two Traffic steering policy identifiers are provided, then one is for uplink direction, while the other one is for downlink direction. NOTE 13: Optional and applicable only for voice service data flow in this release. NOTE 14: Optional and applicable only when a value different from the standardized value for this 5QI in Table 5.7.4-1 TS 23.501 [2] is required. NOTE 15: Optional and applicable only for GBR service data flow. NOTE 16: Usage of the charging information in described in TS 32.255 [21]. NOTE 17: Only one PCC rule can contain this attribute and this PCC rule shall not contain the attribute Bind to QoS Flow associated with the default QoS rule. NOTE 18: Only one of the two shall be present in a PCC rule. NOTE 19: Per DNAI, a Traffic steering policy identifier and/or N6 traffic routing information can be provided. If the pre-configured traffic steering policy (that is referenced by the Traffic steering policy identifier) contains information that is overlapping with the N6 traffic routing information, the N6 traffic routing information shall take precedence. NOTE 20: Only applicable to a PCC Rules provided to a MA PDU Session. NOTE 21: Mandatory when MA PDU Session Control information is provided. NOTE 22: When a Charging key for Non-3GPP access is provided, the parameters in the Charging Section (other than the Charging key) apply to both accesses and the Charging key (in the Charging Section) shall be used for charging packets carried via the 3GPP access. NOTE 23: When a Monitoring key for Non-3GPP access is provided, the Monitoring key (in the Usage Monitoring Control Section) shall be used to monitor usage of the packets carried via the 3GPP access. NOTE 24: Optional and applicable only for GBR service data flow with QoS Notification Control enabled. NOTE 25: Optional and applicable only for GBR service data flow for which Alternative QoS Parameter Set(s) are provided. NOTE 26: One or more Alternative QoS Parameter Sets can be provided in a prioritized order starting with the Alternative QoS Parameter Set that has the highest priority. NOTE 27: Mandatory in MA PDU Session Control information only when there is application identifier in the service data flow template.				

The Rule identifier shall be unique for a PCC rule within a PDU Session. A dynamically provided PCC rule that has the same Rule identifier value as a predefined PCC rule shall replace the predefined rule within the same PDU Session.

The Precedence defines in what order the activated PCC rules within the same PDU Session shall be applied at the UPF for service data flow detection. When a dynamic PCC rule and a predefined PCC rule have the same precedence, the dynamic PCC rule takes precedence.

NOTE 2: The operator shall ensure that overlap between the predefined PCC rules can be resolved based on precedence of each predefined PCC rule in the SMF. The PCF shall ensure that overlap between the dynamically allocated PCC rules can be resolved based on precedence of each dynamically allocated PCC rule.

For downlink packets all the service data flow templates, activated for the PDU Session shall be applied for service data flow detection and for the mapping to the correct QoS Flow. For uplink packets the service data flow templates activated on their QoS Flow shall be applied for service data flow detection (further details are provided in clause 6.2.2.2).

The *Service data flow template* may comprise any number of *Service data flow filters* or an *application identifier* as is defined in table 6.3.1.

NOTE 3: Predefined PCC rules may include service data flow templates, which support extended capabilities, including enhanced capabilities to identify events associated with application protocols.

A Service data flow filter contains information for matching user plane packets for IP PDU traffic or Ethernet PDU traffic. All Service data flow filters of a Service data flow template shall be of the same type, i.e. either Packet Filters for IP or Ethernet PDU traffic (defined in clause 5.7.6 of TS 23.501 [2]). The Service data flow template information within an activated PCC rule is applied by the SMF to instruct the UPF to identify the packets belonging to a particular service data flow.

For the IP PDU Session type only, the Service data flow template may consist of an application identifier that references an application detection filter that is used for matching user plane packets. The application identifier is also identifying the application, for which the rule applies. The same application identifier value can occur in a dynamic PCC rule and one or multiple predefined PCC rules. If so, the PCF shall ensure that there is at most one PCC rule active per application identifier value at any time.

The *Mute for notification* defines whether notification to the PCF of application's starts or stops shall be muted. Absence of this parameter means that start/stop notifications shall be sent.

The *Charging key* is the reference to the tariff for the service data flow. Any number of PCC Rules may share the same charging key value. The Charging key values for each service shall be operator configurable.

NOTE 4: Assigning the same Charging key for several service data flows implies that the charging does not require the credit management to be handled separately.

The *Service identifier* identifies the service. PCC Rules may share the same service identifier value. The service identifier provides the most detailed identification, specified for flow-based charging, of a service data flow.

NOTE 5: The PCC rule service identifier need not have any relationship to service identifiers used on the AF level, i.e. is an operator policy option.

The *Sponsor Identifier* indicates the (3rd) party organization willing to pay for the operator's charge for connectivity required to deliver a service to the end user.

The *Application Service Provider Identifier* indicates the (3rd) party organization delivering a service to the end user.

The *Charging method* indicates whether online charging or offline charging is required, or the service data flow is not subject to any end user charging. If the charging method identifies that the service data flow is not subject to any end user charging, a Charging key shall not be included in the PCC rule for that service data flow, along with other charging related parameters. If the charging method is omitted the SMF shall apply the default charging method provided within the PDU Session related policy information (see clause 6.4). The Charging method is mandatory if there is no default charging method for the PDU Session.

NOTE 6: With converged charging architecture for 5GC, online charging method also includes usage reporting from the SMF to the CHF. Hence, setting the charging method to online will also result in usage reports and thus allow for offline charging being performed by the CHF.

The *Service Data Flow handling while requesting credit* indicates either "blocking" if a credit for the Charging Key needs to be granted as a condition for the PCC Rule to be active or "non-blocking" if a credit for the Charging Key has been requested as a condition for the PCC Rule to be active.

The *Measurement method* indicates what measurements apply to charging for a PCC rule.

The *Service Identifier Level Reporting* indicates whether the SMF shall generate reports per Service Identifier. The SMF shall accumulate the measurements from all PCC rules with the same combination of Charging key/Service Identifier values in a single report.

The *Application Function Record Information* identifies an instance of service usage. A subsequently generated usage report (i.e. CDR), generated as a result of the PCC rule by the SMF, may include the Application Function Record Information, if available. The Application Function Record Information may contain the AF Charging Identifier and/or the Flow identifiers. If exclusive charging information related to the Application function record information is required, the PCF shall provide a service identifier, not used by any other PCC rule of the PDU Session at this point in time, for the AF session.

NOTE 7: For example, the PCF may be configured to maintain a range of service identifier values for each service which require exclusive per instance charging information. Whenever a separate counting or credit management for an AF session is required, the PCF shall select a value, which is not used at this point in time, within that range. The uniqueness of the service identifier in the SMF ensures a separate accounting/credit management while the AF record information identifies the instance of the service.

The *Gate* indicates whether the SMF shall instruct the UPF to let a packet identified by the PCC rule pass through (gate is open) to discard the packet (gate is closed).

NOTE 8: A packet, matching a PCC Rule with an open gate, may be discarded due to credit management reasons.

The *5G QoS Identifier*, 5QI, represents the QoS parameters for the service data flow. The 5G QoS identifier is scalar and accommodates the need for differentiating QoS in both 3GPP and non-3GPP access type.

The bitrates indicate the authorized bitrates at the IP packet level of the SDF, i.e. the bitrates of the IP packets before any access specific compression or encapsulation.

The *UL maximum-bitrate* indicates the authorized maximum bitrate for the uplink component of the service data flow.

The *DL maximum-bitrate* indicates the authorized maximum bitrate for the downlink component of the service data flow.

The *UL guaranteed-bitrate* indicates the authorized guaranteed bitrate for the uplink component of the service data flow.

The *DL guaranteed-bitrate* indicates the authorized guaranteed bitrate for the downlink component of the service data flow.

The 'Maximum bitrate' is used for enforcement of the maximum bit rate that the SDF may consume, while the 'Guaranteed bitrate' is used by the SMF to determine resource allocation demands.

The *UL sharing indication* indicates that resource sharing in uplink direction for service data flows with the same value in their PCC rule shall be applied by the SMF as described in clause 6.2.2.4.

The *DL sharing indication* indicates that resource sharing in downlink direction for service data flows with the same value in their PCC rule shall be applied by the SMF as described in clause 6.2.2.4.

The *Allocation and Retention Priority* indicates the allocation, retention and priority of the service data flow. The ARP contains information about the priority level, the pre-emption capability and the pre-emption vulnerability. The Allocation and Retention Priority resolves conflicts of demands for network resources.

The *Priority Level* is signalled together with the 5QI to the (R)AN and UPF, only when a value different from the standardized value in the QoS characteristics Table 5.7.4-1 in TS 23.501 [2] is required.

The *Averaging Window* is signalled together with the 5QI to the (R)AN and UPF, only when a value different from the standardized value in the QoS characteristics Table 5.7.4-1 in TS 23.501 [2] is required.

The *Maximum Data Burst Volume* is signalled together with the 5QI to the (R)AN, only when a value different from the standardized value in the QoS characteristics Table 5.7.4-1 in TS 23.501 [2] is required.

The *Bind to QoS Flow associated with the default QoS rule* indicates that the SDF shall be bound to the QoS Flow associated with the default QoS rule. The presence of this parameter attribute causes the 5QI/ARP of the rule to be ignored by the SMF during the QoS Flow binding.

The *Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters* indicates that the SDF shall be bound to the QoS Flow associated with the default QoS rule and that the QoS related attributes of the PCC rule shall be applied by the SMF to derive the QoS parameters of the QoS Flow associated with the default QoS rule instead of the PDU Session related information Authorized default 5QI/ARP.

NOTE 9: The Bind to QoS Flow associated with the default QoS rule and apply PCC rule parameters Indication has to be used whenever the PDU Session related information Authorized default 5QI/ARP (as described in clause 6.3.1) cannot be directly used as the QoS parameters of the QoS Flow associated with the default QoS rule, for example when a GBR 5QI is used or the 5QI priority level has to be changed.

The *QoS Notification Control*, QNC, indicates whether notifications are requested from the access network (i.e. 3GPP RAN) when the GFBR can no longer (or can again) be guaranteed for a QoS Flow during the lifetime of the QoS Flow.

If it is set and the GFBR can no longer (or can again) be guaranteed, the access network (i.e. 3GPP RAN) sends a notification towards the SMF, which then notifies the PCF.

The *Disable UE notifications at changes related to Alternative QoS Profiles* parameter indicates to disable QoS Flow parameters signalling to the UE when the SMF is notified by the NG-RAN of changes in the fulfilled QoS situation. The fulfilled situation is either the QoS profile or an Alternative QoS Profile.

The *Reflective QoS Control* indicates to apply reflective QoS for the service data flow. The indication is used to control the RQI marking in the DL packets of the service data flow and may trigger the sending of the RQA parameter for the QoS Flow the service data flow is bound to. Reflective QoS is defined in clause 5.7.5 of TS 23.501 [2].

NOTE 10: While the UE applies a standardized value for the precedence of all UE derived QoS rules, PCC rules require different precedence values and PCF configuration has to ensure that there is a large enough value range for the precedence of PCC rules corresponding to UE derived QoS rules. To avoid that the precedence of network provided QoS rules need to be changed when Reflective QoS is activated and filters are overlapping, the PCF will take the standardized value for the precedence of UE derived QoS rules into account when setting the precedence value of PCC rules subject to Reflective QoS.

The *Reflective QoS Control* parameter shall not be used for the PCC rule with match-all SDF template. If PCC rule with match-all SDF template is present, the *Reflective QoS Control* parameter shall not be used for PCC rules which contain the *Bind to QoS Flow of the default QoS rule* parameter, either.

The *N6-LAN Traffic Steering Enforcement Control* contains *Traffic steering policy identifier(s)* for steering traffic onto N6-LAN to the appropriate N6 service functions deployed by the operator.

The access network information reporting parameters (*User Location Report*, *UE Timezone Report*) instruct the SMF about what information to forward to the PCF when the PCC rule is activated, modified or removed.

The *Monitoring Key* is the reference to a resource threshold. Any number of PCC Rules may share the same monitoring key value. The monitoring key values for each service shall be operator configurable.

The *Indication of exclusion from session level monitoring* indicates that the service data flow shall be excluded from the PDU Session usage monitoring.

The *AF influenced Traffic Steering Enforcement Control* contains:

- *a set of DNAI(s)* (i.e. a reference to the DNAI(s) the SMF needs to consider for UPF selection/reselection), an optional Indication of traffic correlation and, per DNAI, a corresponding Traffic steering policy identifier (i.e. a reference to a pre-configured traffic steering policy at the SMF), and/or a corresponding N6 traffic routing information (when the N6 traffic routing information is provided explicitly as part of the AF influence request, as described in clause 5.6.7 of TS 23.501 [2]), or;

- an AF subscription to UP change events parameter which contains subscription information defined in clause 5.2.8.3 of TS 23.502 [3] for the change of UP path Event Id i.e. an Indication of early and/or late notification and information on where to provide the corresponding notifications (Notification Target Address + Notification Correlation ID as specified in clause 4.15.1 of TS 23.502 [3]) and optionally an indication of "AF acknowledgment to be expected" to the corresponding notifications as described in clause 5.6.7 of TS 23.501 [2].

The *Traffic Steering Enforcement Control* may contain Indication of UE IP address preservation. The SMF takes this indication into account when determining whether to reselect PSA UPF, as specified in clause 5.6.7 of TS 23.501 [2].

The *Redirect* indicates whether the uplink part of the service data flow should be redirected to a controlled address.

The *Redirect Destination* indicates the target redirect address when *Redirect* is enabled.

The *UL Maximum Packet Loss Rate* indicates the maximum rate for lost packets that can be tolerated in the uplink direction.

The *DL Maximum Packet Loss Rate* indicates the maximum rate for lost packets that can be tolerated in the downlink direction.

The *Application descriptors* provides one or several instances of the OSId and OSAppId combination. It is used by the UE to identify the application traffic corresponding to the application identifier to apply the Steering Functionality and the Steering mode.

The *Steering Functionality* indicates the method for how traffic matching the SDF template is sent over the MA PDU Session. The method ATSSS_LL indicates that the traffic matching the SDF template is sent over the MA PDU Session without additional tunnelling, e.g. with IP flow switching. The method MPTCP indicates that the traffic matching the SDF template is sent over the MA PDU Session using MPTCP.

The *Steering mode* indicates the rule for distributing traffic between accesses, together with the associated parameters. The PCF may indicate separate values for up-link and down-link directions. The available steering modes are defined in TS 23.501 [2].

The *Charging key for Non-3GPP access* indicates the Charging key that shall be used for charging the detected service data flow traffic carried via Non-3GPP access. The other charging related parameters apply for both accesses.

The *Monitoring key for Non-3GPP access* indicates the Monitoring key that shall be used for monitoring the usage of the detected service data flow traffic carried via Non-3GPP access.

The *QoS parameter(s) to be measured* indicates the UL packet delay, DL packet delay or round trip packet delay between the UE and the UPF is to be monitored when the QoS Monitoring for URLLC is enabled for the service data flow.

The *Reporting frequency* indicates the frequency for the reporting, such as event triggered, periodic. The following applies:

- If the *Reporting frequency* indicates "periodic", the *reporting period* shall also be included in the PCC rule.

- The *reporting period* shall also be used for reporting measurement failure in any of the *Reporting frequency* modes "periodic" or " event triggered ": if no measurement result is available in the UPF within the *reporting period*, the UPF shall report to the SMF and the SMF shall report to the PCF or to the AF indicating a measurement failure.

- If the *Reporting frequency* indicates "event triggered", the *reporting period*, *Reporting threshold(s)* and the *minimum waiting time* shall also be included in the PCC rule. The *Reporting threshold(s)* indicates the measurement threshold for each of the included *QoS parameter(s)* to be measured, i.e. the UL packet delay, DL packet delay or round trip packet delay. When *Reporting threshold(s)* is exceeded, the UPF shall report to the SMF and the SMF shall report to the PCF or to the AF. If more than one value is received at one given point of time for UL packet delay, DL packet delay or round trip packet delay respectively, the SMF reports the minimum and maximum packet delays to the PCF or the AF. The SMF sends the first report when the *Reporting threshold* is exceeded and the minimum waiting time is applied for the subsequent report (if the threshold is exceeded after the waiting time).

The *Target of reporting* indicates the target for the QoS Monitoring reports sent as notifications. It can be either the PCF or the AF (the NEF may be on the path between SMF and AF). The PCF shall include Notification Target Address + Notification Correlation ID as specified in clause 4.15.1 of TS 23.502 [3].

The *Alternative QoS Parameter Set(s)* define alternative set(s) of QoS parameters for the service data flow. Every set consists of a PER, a PDB, as well as an UL and a DL guaranteed bitrate QoS parameter.

The TSC Assistance Container contains the following parameters:

- The Burst Arrival Time is sent to the SMF to indicate burst arrival time at the ingress port of 5GS for a given flow direction (DS-TT for UL, NW-TT for DL). It is used by the SMF to determine TSCAI burst arrival time as defined in clause 5.27.2 of TS 23.501 [2] to assist transmission of deterministic flows on Uu.

  The Periodicity is sent to the SMF to indicate the time between bursts. It is used by the SMF to forward to RAN as part of TSCAI in order to assist transmission of deterministic flows on Uu.

- The Flow direction is sent to SMF to indicate the direction of the flow (UL or DL).

The *Downlink Data Notification Control* applies to the control of subscription to Downlink Data Delivery status event notifications and DDN Failure event notifications as specified in clause 4.15.3 of TS 23.502 [3]. The following parameters are included:

- The *Notification control for DDD status* applies as described in clause 4.15.3.2.8 of TS 23.502 [3] and contains the following parameters:

  - indication that notifications of Downlink Data Delivery status are required; and

  - the requested type of such notifications (notifications about downlink packets being buffered, and/or discarded).

- The *Notification Control for DDN Failure* applies as described in clause 4.15.3.2.9 of TS 23.502 [3] and contains the following parameters:

  - indication that notifications of DDN Failure are required.

NOTE 11: Downlink Data Notification Control information is provided to assist the SMF in the generation/update of N4 information. The PCF will not be notified about the Downlink data delivery status events or the DDN Failure events.

6.3.2 Policy and charging control rule operations

Policy and Charging Rule operations consist of activation, modification and de-activation of PCC rules. The PCF may activate, modify and deactivate a PCC rule at any time. However, the modification is applicable to dynamic PCC rules only.

Activation of a dynamic PCC rule provides the PCC rule information to the SMF. Activation of a predefined PCC rule provides an identifier of the relevant PCC rule to the SMF.

Each PCC rule shall be installed for a single QoS Flow only (for further details about predefined PCC rules see below).

An active PCC rule means that:

- the service data flow template shall be used for service data flow detection;
- the service data flow template shall be used for mapping of downlink packets to the QoS Flow determined by the QoS Flow binding;
- the service data flow template shall be used for service data flow detection of uplink packets on the PDU Session determined by the QoS Flow binding;
- usage data for the service data flow shall be recorded;
- policies associated with the PCC rule, if any, shall be invoked;
- for service data flow detection with an application detection filter, the start or the stop of the application traffic is reported to the PCF, if applicable and requested by the PCF. In that case, the notification for start may include service data flow filters, (if possible to provide) and the application instance identifier associated with the service data flow filters.
- Either one of the conditions below:
  - a credit has been granted for the service data flow. Applicable when the Charging method is set to "online" and the Service Data Flow handling while requesting credit is set to "blocking"; or
  - a credit has been requested for the service data flow. Applicable when the Charging method is set to "online" and the Service Data Flow handling while requesting credit is set to "non-blocking".

A predefined PCC rule is known at least, within the scope of one PDU Session.

NOTE 1: The same predefined PCC rule can be activated for multiple QoS Flows in multiple PDU Sessions.

A predefined PCC rule is bound to one and only one QoS Flow per PDU Session. For a predefined PCC rule whose service data flow cannot be fully reflected for the uplink direction in terms of traffic mapping information sent to the UE, the SMF may request the UPF to apply the uplink service data flow detection at additional QoS Flows with non-GBR 5QI of the same PDU Session. The deactivation of such a predefined PCC rule ceases its service data flow detection for the whole PDU Session.

The PCF may, at any time, deactivate an active PCC rule in the SMF. At QoS Flow termination all active PCC rules on that QoS Flow are deactivated without explicit instructions from the PCF to do so.

Policy and charging control rule operations can be also performed in a deferred mode. A PCC rule may have either a single deferred activation time, or a single deferred deactivation time or both.

A PCC rule with only a deferred activation time shall be inactive until that time. A PCC rule with only a deferred deactivation time shall be active until that time. When the rule activation time occurs prior to the rule deactivation time, the rule is inactive until the activation and remains active until the deactivation time occurs. When the rule deactivation time occurs prior to the rule activation time, the rule is initially active until the deactivation time, then remains inactive until the activation time, and then becomes active again. An inactive PCC rule, that has not been activated yet, is still considered to be installed, and may be removed by the PCF. When modifying a dynamic PCC rule by setting, modifying or clearing its deferred activation and/or deactivation time or by changing any other attribute of a PCC rule having a deferred activation and/or deactivation time, the PCF shall provide all attributes of that PCC rule, including attributes that have not changed.

NOTE 2: In this case, the PCF omission of an attribute that has a prior value will erase that attribute from the rule.

Deferred activation and deactivation of PCC rules can only be used for PCC rules that belong to the QoS Flow associated with the default QoS rule that allows all UL packets.

Deferred modification of PCC rules shall not be applied for changes of the QoS or service data flow filter information of PCC rules.

NOTE 3: This limitation prevents dependencies on the signalling of changed traffic mapping information towards the UE.

6.4 PDU Session related policy information

The purpose of the PDU Session related policy information is to provide policy and charging control related information that is applicable to a single Monitoring key or the whole PDU Session respectively. The PCF may provide PDU Session related policy information to the SMF together with PCC rules or separately.

Table 6.4-1 includes the PDU Session related policy information.

The differences with table 6.4 and table 6.6 in TS 23.203 [4] are shown, either "none" means that the IE applies in 5GS or "removed" meaning that the IE does not apply in 5GS, this is due to the lack of support in the 5GS for this feature or "modified" meaning that the IE applies with some modifications defined in the IE.

Table 6.4-1: PDU Session related policy information

Attribute	Description	PCF permitted to modify for dynamically provided information	Scope	Differences compared with table 6.4. and 6.6 in TS 23.203 [4]
Charging information	Defines the containing CHF address and optionally the associated CHF instance ID and CHF set ID.	No	PDU Session	None
Default charging method	Defines the default charging method for the PDU Session.	No	PDU Session	None
PDU Session with offline charging only	Indicates that the "online" charging method is never used for PCC rules in the PDU Session.	No	PDU Session	Added
Policy control request trigger	Defines the event(s) that shall cause a re-request of PCC rules for the PDU Session.	Yes	PDU Session	Explicitly subscribed by invoking Npcf_SMPolicyControl service operation
Authorized QoS per bearer (UE-initiated IP-CAN bearer activation/modification)	Defines the authorised QoS for the IP-CAN bearer (QCI, GBR, MBR).	Yes	IP-CAN bearer	Removed
Authorized MBR per QCI (network initiated IP-CAN bearer activation/modification)	Defines the authorised MBR per QCI.	Yes	IP-CAN session	Removed
Revalidation time limit	Defines the time period within which the SMF shall perform a PCC rules request.	Yes	PDU Session	None
PRA Identifier(s)	Defines the Presence Reporting Area(s) to monitor for the UE with respect to entering/leaving	Yes	PDU Session	None but only applicable to PCF
List(s) of Presence Reporting Area elements (NOTE 14)	Defines the elements of the Presence Reporting Area(s)	Yes	PDU Session	None but only applicable to PCF
Default NBIFOM access	The access to be used for all traffic that does not match any existing Routing Rule	Yes (only at the addition of an access to the IP-CAN session)	IP-CAN session	Removed
IP Index (NOTE 11)	Provided to SMF to assist in determining the IP Address allocation method (e.g. which IP pool to assign from) when a PDU Session requires an IP address – as defined in clause 5.8.2.2.1 of TS 23.501 [2].	No	PDU Session	Added
Redundant PDU Session	Indicates whether the PDU Session is a redundant PDU Session	No	PDU Session	New
Explicitly signalled QoS Characteristics (NOTE 1)	Defines a dynamically assigned 5QI value (from the non-standardized value range) and the associated 5G QoS characteristics as defined in clause 5.7.3 of TS 23.501 [2].	No	PDU Session	Added
Reflective QoS Timer	Defines the lifetime of a UE derived QoS rule belonging to the PDU Session.	No	PDU Session	Added
Authorized Session-AMBR (NOTE 2) (NOTE 3)	Defines the Aggregate Maximum Bit Rate for the Non-GBR QoS Flows of the PDU Session.	Yes	PDU Session	Modified

Attribute	Description	PCF permitted to modify for dynamically provided information	Scope	Differences compared with table 6.4. and 6.6 in TS 23.203 [4]
Authorized default 5QI/ARP (NOTE 3) (NOTE 10)	Defines the default 5QI and ARP of the QoS Flow associated with the default QoS rule.	Yes	PDU Session	Modified
Time Condition (NOTE 4)	Defines the time at which the corresponding Subsequent Authorized Session-AMBR or Subsequent Authorized default 5QI/ARP shall be applied.	No (NOTE 5)	PDU Session	Modified
Subsequent Authorized Session-AMBR (NOTE 4) (NOTE 2)	Defines the Aggregate Maximum Bit Rate for the Non-GBR QoS Flows of the PDU Session when the Time Condition is reached.	No (NOTE 5)	PDU Session	Modified
Subsequent Authorized default 5QI/ARP (NOTE 4) (NOTE 10)	Defines the default 5QI and ARP when the Time Condition is reached.	No (NOTE 5)	PDU Session	Modified
Usage Monitoring Control related information (NOTE 12) (NOTE 13)	Defines the information that is required to enable user plane monitoring of resources for individual applications/services, groups of applications/services, for a PDU Session.			
Monitoring key	The PCF uses the monitoring key to group services that share a common allowed usage.	No	PDU Session (NOTE 12)	None
Volume threshold (NOTE 7)	Defines the traffic volume value after which the SMF shall report usage to the PCF for this monitoring key.	Yes	Monitoring key	None
Time threshold (NOTE 7)	Defines the resource time usage after which the SMF shall report usage to the PCF.	Yes	Monitoring key	None
Monitoring time	Defines the time at which the SMF shall reapply the Volume and/or Time Threshold.	No (NOTE 6)	Monitoring Key	None
Subsequent Volume threshold (NOTE 9)	Defines the traffic volume value after which the SMF shall report usage to the PCF for this Monitoring key for the period after the Monitoring time.	No (NOTE 6)	Monitoring Key	None
Subsequent Time threshold (NOTE 9)	Defines resource time usage after which the SMF shall report usage to the PCF for this Monitoring key for the period after the Monitoring time.	No (NOTE 6)	Monitoring Key	None
Inactivity Detection Time (NOTE 8)	Defines the period of time after which the time measurement shall stop, if no packets are received.	Yes	Monitoring Key	None
Ethernet port management related				
Port number	Port number for which Port Management Information Container is provided.	Yes	PDU Session	New
Port Management Information Container	Includes Ethernet port management information	Yes	PDU Session	New
Bridge Management Information Container	Includes Bridge management information	Yes		New

Attribute	Description	PCF permitted to modify for dynamically provided information	Scope	Differences compared with table 6.4. and 6.6 in TS 23.203 [4]
NOTE 1: Multiple Non-standardized QoS Characteristics can be provided by the PCF. Operator configuration is assumed to ensure that the non-standardized 5QI to QoS characteristic relation is unique within the PLMN. NOTE 2: The Authorized Session-AMBR and the Subsequent Authorized Session-AMBR may be provided together with a list of Access Types possibly complemented by RAT types. NOTE 3: There is always an unconditional value for the Authorized Session-AMBR and Authorized default 5QI/ARP available at the SMF. The initial value is received as Subscribed Session-AMBR/Subscribed default 5QI/ARP, and the PCF can overwrite it with these parameters. NOTE 4: The Time Condition and Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP are used together. The PCF may provide up to four instances of them. When multiple instances are provided, the values of the associated Time Condition have to be different. NOTE 5: The PCF may replace all instances that have been provided previously with a new instruction. A previously provided Time Condition and Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP pair cannot be individually modified. NOTE 6: The PCF may replace all instances that have been provided previously with a new instruction. A previously provided Volume threshold/Time threshold and Monitoring Time pair cannot be individually modified. NOTE 7: This attribute is also used by the SMF, e.g. during PDU Session termination, to inform the PCF about the resources that have been consumed by the UE. NOTE 8: This attribute is applicable in presence of Time threshold only. NOTE 9: This attribute is applicable in presence of Monitoring Time only. NOTE 10: The Authorized default 5QI and the Subsequent Authorized default 5QI shall be of Non-GBR Resource Type. NOTE 11: This attribute is applicable only when no IP address/Prefix for the PDU Session is received from the SMF. NOTE 12: A Monitoring Key can either be used to monitor the traffic of a PDU Session, the traffic of a PDU Session per access (for a MA PDU Session) or the traffic of specific SDF(s) in the PCC Rule(s) that share the same Monitoring Key. NOTE 13: For a MA PDU Session, the PDU Session level Usage Monitoring shall be possible per access (i.e. 3GPP and/or Non-3GPP) and irrespective of the access. NOTE 14: The list of PRA elements shall be a short list of elements.				

Upon the initial interaction with the SMF, the PCF may provide the following attributes to the SMF:

The *Charging information* contains addresses of the CHF that manages charging for the PDU Session and optionally the associated CHF instance ID and CHF set ID (see clause 6.3.1.0 of TS 23.501 [2]). If received, the SMF shall apply it as defined in clause 6.3.11 of TS 23.501 [2].

The *Default charging method* indicates what charging method shall be used in the PDU Session for every PCC rule where the charging method identifier is omitted, including predefined PCC rules that are activated by the SMF. If received by the SMF, it supersedes the *Default charging method* in the charging characteristics profile.

The *PDU Session with offline charging only* can be assigned to a PDU Session by the PCF to indicate that the online charging method is never set for any of the PCC Rules activated during the lifetime of the PDU Session nor provided as Default charging method.

NOTE 1: If this parameter is provided by the PCF or configured in the SMF charging characteristics the SMF can use the Nchf_OfflineOnlyCharging service instead of the Nchf_ConvergedCharging service for a PDU Session as defined in TS 32.255 [21].

The *IP Index* indicates the IP Address/Prefix allocation method which is used by the SMF for IP Address/Prefix allocation during PDU Session Establishment procedure as defined in clause 5.8.2.2.1 of TS 23.501 [2].

Upon every interaction with the SMF, the PCF may provide the following attributes to the SMF:

The *Revalidation time limit* defines the time period within which the SMF shall trigger a request for PCC rules for an established PDU Session.

The *Reflective QoS Timer* defines the lifetime of a UE derived QoS rule belonging to the PDU Session. It is used in the UE as defined in clause 5.7.5.3 of TS 23.501 [2].

NOTE 2: The Reflective QoS Timer that is sent to the UE has to be in alignment with the corresponding timer configured in the UPF (defined in clause 5.7.5.3 of TS 23.501 [2]).

The *Authorized Session-AMBR* defines the UL/DL Aggregate Maximum Bit Rate for the Non-GBR QoS Flows of the PDU Session, which is enforced in the UPF as defined in clause 5.7.1 of TS 23.501 [2]. The PCF may provide the *Authorized Session-AMBR* in every interaction with the SMF. When the SMF receives it from the PDU Session policy, it is provided to the UPF over N4 interface for the enforcement.

The *Authorized default 5QI/ARP* defines the 5QI and ARP values of the QoS Flow associated with the default QoS rule as described in clause 6.2.2.4. The SMF applies the *Authorized default 5QI/ARP* also for the QoS Flow binding as described in clause 6.1.3.2.4.

The *Time Condition* and *Subsequent Authorized Session-AMBR / Subsequent Authorized default 5QI/ARP* are used together and up to four instances with different values of the *Time Condition* parameter may be provided by the PCF. *Time Condition* indicates that the associated *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* is only applied when the time defined by this attribute is met. When the SMF receives a *Time Condition* and *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* pair, it stores it locally. The SMF shall discard any previously received *Subsequent Authorized Session-AMBR* / *Subsequent Authorized default 5QI/ARP* instances on explicit instruction as well as whenever the PCF provides a new instruction for one or more *Subsequent Authorized Session-AMBR* / *Subsequent Authorized default 5QI/ARP*. When the time defined by the *Time Condition* parameter is reached, the SMF shall apply (or instruct the UPF to apply) *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP*.

NOTE 3: In order to reduce the risk for signalling overload, the PCF should avoid simultaneous provisioning of the *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* for many UEs (e.g. by spreading over time).

NOTE 4: In order to provide further *Subsequent Authorized Session-AMBR/ Subsequent Authorized default 5QI/ARP* in a timely fashion the PCF can use its own clock to issue the desired changes or use the Revalidation time limit parameter to trigger an SMF request for a policy decision.

NOTE 5: For services that depend on specific Session-AMBR and/or default 5QI/ARP (e.g. MPS session) the PCF is responsible to ensure that no *Subsequent Authorized Session-AMBR* or *Subsequent Authorized default 5QI/ARP* interfere with the service, e.g. by removing the *Subsequent Authorized Session-AMBR* or *Subsequent Authorized default 5QI/ARP* before the respective change time is reached.

The *Monitoring Key* is the reference to a resource threshold. Any number of PCC Rules may share the same monitoring key value. The monitoring key values for each service shall be operator configurable.

It shall also be possible for an operator to use the *Monitoring Key* parameter to indicate usage monitoring on an PDU Session level or, in the case of an MA PDU Session, to indicate usage monitoring on PDU Session level for the 3GPP access and/or the Non-3GPP access.

Usage monitoring on PDU Session level is active when a PDU Session is active when a *Monitoring Key* for the PDU Session and a corresponding volume and/or time threshold value have been provided to the SMF. Usage monitoring on Monitoring key level is active when a volume and/or time threshold has been provided for a *Monitoring Key* to the SMF and there is at least one PCC rule active for the PDU Session that is associated with that *Monitoring Key*.

The *Volume threshold* indicates the overall user traffic volume value after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Time threshold* indicates the overall resource time usage after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Monitoring time* indicates the time at which the SMF shall store the accumulated usage information.

The *Subsequent Volume threshold* indicates the overall user traffic volume value measured after Monitoring time, after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Subsequent Time threshold* indicates the overall resource time usage measured after Monitoring time, after which the SMF shall report the Usage threshold reached trigger to the PCF.

The *Inactivity Detection Time* indicates the period of time after which the time measurement shall stop, if no packets are received during that time period.

The *Port Management Information Container* carries Ethernet port management information for an Ethernet port located in DS-TT or NW-TT. The port for which the container is provided is identified by the port number.

The *Bridge Management Information Container* carries Bridge management information for a 5GS Bridge.

6.5 Access and mobility related policy information

To enable the enforcement in the 5GC system of the access and mobility policy decisions made by the PCF for the control of the service area restrictions and RFSP Index, the 5GC system may provide the Access and mobility related policy control information from the PCF to the AMF.

Table 6.5-1 lists the AMF access and mobility related policy information.

Table 6.5-1: Access and mobility related policy control information

Information name	Description	Category	PCF permitted to modify in a UE context in the AMF	Scope
UE-AMBR	This defines the UE-AMBR value that applies for a UE	Conditional (NOTE 5)	Yes	UE context
Service Area Restrictions	*This part defines the service area restrictions*			
List of allowed TAIs.	List of allowed TAIs (NOTE 3) (NOTE 4).	Conditional (NOTE 1)	Yes	UE context
List of non-allowed TAIs.	List of non-allowed TAIs (NOTE 3).	Conditional (NOTE 1)	Yes	UE context
Maximum number of allowed TAIs	The maximum number of allowed TAIs. (NOTE 4)	Conditional (NOTE 1)	Yes	UE context
RFSP Index	*This part defines the RFSP index*			
RFSP Index	Defines the RFSP Index that applies for a UE	Conditional (NOTE 2)	Yes	UE context
SMF selection management	This part defines the SMF selection management instructions			
DNN replacement of unsupported DNNs	Defines if a UE requested unsupported DNN is requested for replacement by PCF	Conditional (NOTE 6)	Yes	UE context
List of S-NSSAIs	Defines the list of S-NSSAIs containing DNN candidates for replacement by PCF	Conditional (NOTE 6) (NOTE 7)	Yes	UE context
Per S-NSSAI: List of DNNs	Defines UE requested DNN candidates for replacement by PCF	Conditional (NOTE 6)	Yes	UE context

NOTE 1: If service area restrictions is enabled.
NOTE 2: If RFSP index is enabled.
NOTE 3: Either the list of allowed TAIs or the list of non-allowed TAIs are provided by the PCF.
NOTE 4: Both the maximum number of allowed TAIs and the list of allowed TAIs may be sent by PCF.
NOTE 5: If UE-AMBR is enabled.
NOTE 6: If SMF selection management by PCF is enabled.
NOTE 7: The List of S-NSSAIs contains S-NSSAIs, valid in the serving network, of the Allowed NSSAI.

The *list of allowed TAIs* indicates the TAIs where the UE is allowed to be registered, see clause 5.3.4 of TS 23.501 [2] for the description on how AMF uses this information.

The *list of non-allowed TAIs* indicates the TAIs where the UE is not allowed to be registered, see clause 5.3.4 of TS 23.501 [2] for the description on how AMF uses this information.

The *Maximum number of allowed TAs* indicates the maximum number of allowed Tracking Areas, the list of TAI is defined in the AMF and not explicitly provided by the PCF.

The *RFSP Index* defines the RFSP Index for radio resource management functionality.

The *UE-AMBR* limits the aggregated bit rate across all Non-GBR QoS Flows of a UE in the serving network.

The *DNN replacement of unsupported DNNs* indicates that the AMF shall contact the PCF for replacement of an unsupported DNN requested by the UE.

The *List of S-NSSAIs* defines the S-NSSAIs, valid in the serving network, of the Allowed NSSAI that contain DNN candidates for replacement by PCF.

The *List of DNNs* defines the DNN candidates for which the AMF shall contact the PCF for replacement if such a DNN is requested by a UE.

6.6 UE policy information

6.6.1 Access Network Discovery & Selection Policy Information

6.6.1.1 General

The Access Network Discovery & Selection policy is an optional policy that may be provided to UE by the network.

In this release of the specification, the Access Network Discovery & Selection policy shall contain only rules that aid the UE in selecting a WLAN access network. Rules for selecting other types of non-3GPP access networks are not specified.

The WLAN access network selected by the UE with the use of Access Network Discovery & Selection policy may be used for direct traffic offload (i.e. sending traffic to the WLAN outside of a PDU Session) and for registering to 5GC using the non-3GPP access network selection information.

If the UE supports non-3GPP access to 5GC, it shall support ANDSP.

The procedure for WLAN access network selection is defined in clause 6.6.1.3, the procedure for N3IWF selection is defined in clause 6.3.6.1 of TS 23.501 [2].

The Access Network Discovery & Selection policy shall contain one or more WLAN Selection Policy (WLANSP) rules defined in clause 4.8.2.1.6 of TS 23.402 [9].

The Access Network Discovery & Selection policy may contain information to select ePDG or N3IWF by the UE as specified in TS 23.501 [2]

Table 6.6.1-1: Access Network Discovery & Selection Policy

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
WLANSP rules	1 or more WLANSP rules as specified in 4.8.2.1.6 of TS 23.402 [9]	Mandatory	Yes	UE context
ePDG identifier configuration	The UE uses this information to select ePDG as defined in clause 6.3.6.1 of TS 23.501 [2]	Optional	Yes	UE context
N3IWF identifier configuration	The UE uses this information to select N3IWF as defined in clause 6.3.6.1 of TS 23.501 [2]	Optional	Yes	UE context
Non-3GPP access node (N3AN) selection information	The UE uses this information to select ePDG or N3IWF as defined in clause 6.3.6.1 of TS 23.501 [2]	Optional	Yes	UE context

6.6.1.2 UE selecting a WLANSP rule

The UE may be provisioned with multiple valid WLANSP rules (by the HPLMN and by the VPLMN when the UE is roaming). A WLANSP rule is valid if it meets the validity conditions included in the WLANSP rule (if provided).

When the UE is in the home the UE uses the valid WLANSP rules from the home PLMN to select an available WLAN. When the UE is roaming and the UE has valid rules from both HPLMN and VPLMN the UE gives priority to the valid WLANSP rules from the VPLMN.

6.6.1.3 UE procedure for selecting a WLAN access based on WLANSP rules

The UE shall apply the procedure in this clause when the UE is provisioned with WLANSP rules and:

a) when the UE initiates untrusted non-3GPP access to 5GC and attempts to select a WLAN access network; or

b) when the UE initiates trusted non-3GPP access to 5GC by executing the Access Network Selection Procedure specified in clause 6.3.12.2 of TS 23.501 [2] and attempts to select a WLAN access network.

When the UE has valid 3GPP subscription credentials (i.e. a valid USIM) and WLANSP rules, the UE shall perform WLAN selection based on these rules, the applicable User Preferences On Non-3GPP Access Selection and the corresponding procedures specified in this document. User Preferences On Non-3GPP Access Selection take precedence over the WLANSP rules.

The UE determines the most preferred WLAN access network using WLANSP rules when a WLAN access network cannot be selected based on User Preferences On Non-3GPP Access Selection (e.g. when there are no User Preferences On Non-3GPP Access Selection or when there is no user-preferred WLAN access network available).

The UE constructs a prioritized list of the available WLANs by discovering the available WLANs and comparing their attributes / capabilities against the groups of selection criteria in the valid WLANSP rule(s). When there are multiple valid WLANSP rules the UE evaluates the valid WLANSP rules in priority order. The UE evaluates first if an available WLAN access meets the criteria of the highest priority valid WLANSP rule. The UE then evaluates if an available WLAN access meets the selection criteria of the next priority valid WLANSP rule.

Within a valid WLANSP rule, the WLAN(s) that match the group of selection criteria with the highest priority are considered as the most preferred WLANs, the WLAN(s) that match the group of selection criteria with the second highest priority are considered as the second most preferred WLANs, etc.

When a group of selection criteria includes the HomeNetwork attribute and is set, then the UE (a) shall create a list of available WLANs that directly interwork with the home operator (as specified in clause 4.8.2.1.6 of TS 23.402 [9]) and (b) shall apply the group of selection criteria to all the WLANs in this list. Otherwise, when the HomeNetwork attribute is not set or is not present, the UE shall apply the group of selection criteria to all available WLANs. The UE may need to perform ANQP procedures (as specified in the HS2.0 Rel-2 specification [ref]) or other procedures in order to discover the attributes / capabilities of the available WLANs.

When the UE is roaming the UE may have valid WLANSP rules from both the VPLMN and the HPLMN. In such a case the UE gives priority to the valid WLANSP rules from the VPLMN. The UE constructs a prioritised list of the available WLANs when the available WLAN accesses meet the selection criteria of the valid rules from the VPLMN and the valid rules from the HPLMN. The prioritised WLAN accesses based on the WLANSP rules from the HPLMN will have lower priority from the prioritised list of WLAN access based on the WLANSP rules of the VPLMN.

6.6.2 UE Route Selection Policy information

6.6.2.1 Structure Description

The UE Route Selection Policy (URSP) includes a prioritized list of URSP rules.

Table 6.6.2.1-1: UE Route Selection Policy

Information name	Description	Category	PCF permitted to modify in a URSP	Scope
URSP rules	1 or more URSP rules as specified in table 6.6.2.1-2	Mandatory	Yes	UE context

The structure of the URSP rules is described in Table 6.6.2.1-2 and Table 6.6.2.1-3.

Table 6.6.2.1-2: UE Route Selection Policy Rule

Information name	Description	Category	PCF permitted to modify in a UE context	Scope
Rule Precedence	Determines the order the URSP rule is enforced in the UE.	Mandatory (NOTE 1)	Yes	UE context
Traffic descriptor	*This part defines the Traffic descriptor components for the URSP rule.*	Mandatory (NOTE 3)		
Application descriptors	It consists of OSId and OSAppId(s). (NOTE 2)	Optional	Yes	UE context
IP descriptors (NOTE 5)	Destination IP 3 tuple(s) (IP address or IPv6 network prefix, port number, protocol ID of the protocol above IP).	Optional	Yes	UE context
Domain descriptors	Destination FQDN(s) or a regular expression as a domain name matching criteria.	Optional	Yes	UE context
Non-IP descriptors (NOTE 5)	Descriptor(s) for destination information of non-IP traffic	Optional	Yes	UE context
DNN	This is matched against the DNN information provided by the application.	Optional	Yes	UE context
Connection Capabilities	This is matched against the information provided by a UE application when it requests a network connection with certain capabilities. (NOTE 4)	Optional	Yes	UE context
List of Route Selection Descriptors	A list of Route Selection Descriptors. The components of a Route Selection Descriptor are described in table 6.6.2.1-3.	Mandatory		

NOTE 1: Rules in a URSP shall have different precedence values.
NOTE 2: The information is used to identify the Application(s) that is(are) running on the UE's OS. The OSId does not include an OS version number. The OSAppId does not include a version number for the application.
NOTE 3: At least one of the Traffic descriptor components shall be present.
NOTE 4: The format and some values of Connection Capabilities, e.g. "ims", "mms", "internet", etc., are defined in TS 24.526 [19]. More than one connection capabilities value can be provided.
NOTE 5: A URSP rule cannot contain the combination of the Traffic descriptor components IP descriptors and Non-IP descriptors.

Table 6.6.2.1-3: Route Selection Descriptor

Information name	Description	Category	PCF permitted to modify in URSP	Scope
Route Selection Descriptor Precedence	Determines the order in which the Route Selection Descriptors are to be applied.	Mandatory (NOTE 1)	Yes	UE context
Route selection components	*This part defines the route selection components*	Mandatory (NOTE 2)		
SSC Mode Selection	One single value of SSC mode. (NOTE 5)	Optional	Yes	UE context
Network Slice Selection	Either a single value or a list of values of S-NSSAI(s).	Optional (NOTE 3)	Yes	UE context
DNN Selection	Either a single value or a list of values of DNN(s).	Optional	Yes	UE context
PDU Session Type Selection	One single value of PDU Session Type	Conditional (NOTE 8)	Yes	UE context
Non-Seamless Offload indication	Indicates if the traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session.	Optional (NOTE 4)	Yes	UE context
Access Type preference	Indicates the preferred Access Type (3GPP or non-3GPP or Multi-Access) when the UE establishes a PDU Session for the matching application.	Optional	Yes	UE context
Route Selection Validation Criteria (NOTE 6)	*This part defines the Route Validation Criteria components*	Optional		
Time Window	The time window when the matching traffic is allowed. The RSD is not considered to be valid if the current time is not in the time window.	Optional	Yes	UE context
Location Criteria	The UE location where the matching traffic is allowed. The RSD rule is not considered to be valid if the UE location does not match the location criteria.	Optional	Yes	UE context

NOTE 1: Every Route Selection Descriptor in the list shall have a different precedence value.
NOTE 2: At least one of the route selection components shall be present.
NOTE 3: When the Subscription Information contains only one S-NSSAI in UDR, the PCF needs not provision the UE with S-NSSAI in the Network Slice Selection information. The "match all" URSP rule has one S-NSSAI at most.
NOTE 4: If this indication is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.
NOTE 5: The SSC Mode 3 shall only be used when the PDU Session Type is IP.
NOTE 6: The Route Selection Descriptor is not considered valid unless all the provided Validation Criteria are met.
NOTE 7: In this Release of specification, inclusion of the Validation Criteria in Roaming scenarios is not considered.
NOTE 8: This component shall be present when the Route Selection Component does not include the "Non-Seamless Offload indication".

Each URSP rule contains a Traffic descriptor (containing one or more components described in Table 6.6.2.1-2) that determines when the rule is applicable. A URSP rule is determined to be applicable when every component in the Traffic descriptor matches the corresponding information from the application. A URSP rule is determined not to be applicable when for any given component in the Traffic descriptor:

- No corresponding information from the application is available; or
- The corresponding information from the application does not match any of the values in the Traffic descriptor component.

NOTE 1: It is recommended to avoid listing more than two components in the Traffic descriptor of a URSP rule.

If a URSP rule is provided that contains a Traffic descriptor with two or more components, it is recommended to also provide URSP rule(s) with lower precedence and a Traffic descriptor with less components, in order to increase the likelihood of URSP rule matching for a particular application.

Each URSP rule contains a list of Route Selection Descriptors containing one or multiple Route Selection Descriptors each having a different Route Selection Descriptor Precedence value. A Route Selection Descriptor contains one or more of the following components:

- Session and Service Continuity (SSC) Mode: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting the included SSC Mode.

- Network Slice Selection: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting any of the included S-NSSAIs, see clause 5.15.4 in TS 23.501 [2]. It includes one or more S-NSSAI(s).

- DNN Selection: Indicates that the traffic of the matching application shall be routed via a PDU Session supporting any of the included DNNs. It includes one or more DNN(s). When DNN is used in Traffic descriptor, corresponding Route Selection Descriptor of the rule shall not include DNN Selection component.

- PDU Session Type Selection: Indicates that the traffic of matching application shall be routed via a PDU Session supporting the included PDU Session Type. The possible PDU Session Types are defined in clause 5.6.10 in TS 23.501 [2].

- Non-Seamless Offload indication: Indicates that traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session when the rule is applied. If this component is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.

- Access Type Preference: If the UE needs to establish a PDU Session when the rule is applied, this indicates the Access Type (3GPP or non-3GPP or multi-access) on which the PDU Session should be established. The type "Multi-Access" indicates that the PDU Session should be established as a MA PDU Session, using both 3GPP access and non-3GPP access.

- Time Window: The Route Selection Descriptor is not be considered valid unless the UE is in the time window.

- Location Criteria: The Route Selection Descriptor is not be considered valid unless the UE's location matches the Location Criteria.

NOTE 2: The structure of the URSP does not define how the PCF splits the URSP when URSP cannot be delivered to the UE in a single NAS message.

NOTE 3: It is expected that UE applications will not be able to change or override the PDU Session parameters in the URSP rules. A UE application can express preferences when it requests a network connection (e.g. certain Connection Capabilities), which can be mapped into specific PDU Session parameters by the URSP rules.

NOTE 4: When one Route Selection Descriptor in a URSP rule contains a Time Window or Location Criteria, all Route Selection Descriptors in the URSP rule must contain a Time Window or Location Criteria.

In the case of network rejection of the PDU Session Establishment Request, the UE may trigger a new PDU Session establishment based on the rejection cause and the URSP policy.

When the PCF provisions URSP rules to the UE, one URSP rule with a "match all" Traffic descriptor may be included.

NOTE 5: When URSP rules containing NSSP are available to the UE and the URSP rule with the "match all" Traffic descriptor is not part of them, a UE application that has no matching URSP rule and no UE Local Configuration cannot request a network connection.

The URSP rule with the "match all" Traffic descriptor is used to route the traffic of applications which do not match any other URSP rules and shall therefore be evaluated as the last URSP rule, i.e. with lowest priority. There shall be only one Route Selection Descriptor in this URSP rule. The Route Selection Descriptor in this URSP rule includes at most one value for each Route Selection Component.

NOTE 6: How to set the URSP rule with the "match all" Traffic descriptor as the URSP rule with lowest priority is defined in TS 24.526 [19].

6.6.2.2 Configuration and Provision of URSP

The UE may be provisioned with URSP rules by PCF of the HPLMN. When the UE is roaming, the PCF in the HPLMN may update the URSP rule in the UE. For URSP rules, the UE shall support the provisioning from the PCF in the HPLMN, as specified in TS 24.501 [22]. In addition, the UE may be also pre-configured with URSP rules (e.g. by the operator).

Only the URSP rules provisioned by the PCF is used by the UE, if both URSP rules provisioned by the PCF and pre-configured URSP rules are present. If no URSP rule is provisioned by the PCF, and the UE has pre-configured rules configured in both the USIM and ME, then only the pre-configured URSP rules configured in the USIM is used.

6.6.2.3 UE procedure for associating applications to PDU Sessions based on URSP

For every newly detected application the UE evaluates the URSP rules in the order of Rule Precedence and determines if the application is matching the Traffic descriptor of any URSP rule.

When a URSP rule is determined to be applicable for a given application (see clause 6.6.2.1), the UE shall select a Route Selection Descriptor within this URSP rule in the order of the Route Selection Descriptor Precedence.

When a valid Route Selection Descriptor is found, the UE determines if there is an existing PDU Session that matches all components in the selected Route Selection Descriptor. The UE compares the components of the selected Route Selection Descriptor with the existing PDU Session(s) as follows:

- For a component which only contains one value (e.g. SSC mode), the value of the PDU Session has to be identical to the value specified in the Route Selection Descriptor.
- For a component which contains a list of values (e.g. Network Slice Selection), the value of the PDU Session has to be identical to one of the values specified in the Route Selection Descriptor.
- When some component(s) is not present in the Route Selection Descriptor, a PDU Session is considered matching only if it was established without including the missing component(s) in the PDU Session Establishment Request.
- When the Route Selection Descriptor includes a Time Window or a Location Criteria, the PDU Session is considered matching only if the PDU Session is associated with an RSD that has the same Time Window or a Location Criteria Validity Conditions.

When a matching PDU Session exists the UE associates the application to the existing PDU Session, i.e. route the traffic of the detected application on this PDU Session.

If the UE determines that there is more than one existing PDU Session which matches (e.g. the selected Route Selection Descriptor only specifies the Network Slice Selection, while there are multiple existing PDU Sessions matching the Network Slice Selection with different DNNs), it is up to UE implementation to select one of them to use.

NOTE 1: When more than one PDU Sessions of SSC mode 3 to the same DNN and S-NSSAI exist due to PDU Session anchor change procedure as described in clause 4.3.5.2 of TS 23.502 [3], the UE can take the PDU Session Address Lifetime value into account when selecting the PDU Session.

If none of the existing PDU Sessions matches, the UE tries to establish a new PDU Session using the values specified by the selected Route Selection Descriptor. If the PDU Session Establishment Request is accepted, the UE associates the application to this new PDU Session. If the PDU Session Establishment Request is rejected, based on the rejection cause, the UE selects another combination of values in the currently selected Route Selection Descriptor if any other value for the rejected component in the same Route Selection Description can be used. Otherwise, the UE selects the next Route Selection Descriptor, which contains a combination of component value which is not rejected by network, in the order of the Route Selection Descriptor Precedence, if any. If the UE fails to establish a PDU Session with any of the Route Selection Descriptors, it tries other URSP rules in the order of Rule Precedence with matching Traffic descriptors, except the URSP rule with the "match-all" Traffic descriptor, if any. The UE shall not use the UE Local Configuration in this case.

The UE receives the updated URSP rules and (re-)evaluates their validities in a timely manner when certain conditions are met, for example:

- the URSP is updated by the PCF;

- the UE moves from EPC to 5GC;
- change of Allowed NSSAI or Configured NSSAI;
- change of LADN DNN availability;
- UE registers over 3GPP or non-3GPP access;
- UE establishes connection to a WLAN access.

Details of the conditions are defined by TS 24.526 [19].

NOTE 2: When providing the updated URSP rules to the UE with a new DNN, the PCF can set the SMF selection management trigger in the AMF to contact the PCF at PDU Session establishment (as specified in clause 6.1.2.5) if the old DNN is requested by the UE.

The Route Selection Descriptor of a URSP rule shall be only considered valid if all of the following conditions are fulfilled:

- If any S-NSSAI(s) is present, the S-NSSAI(s) is in the Allowed NSSAI for the non-roaming case and in the mapping of the Allowed NSSAI to HPLMN S-NSSAI(s) for the roaming case.
- If any DNN is present and the DNN is an LADN DNN, the UE is in the area of availability of this LADN.
- If Access Type preference is present and set to Multi-Access, the UE supports ATSSS.
- If a Time Window is present and the time matches what is indicated in the Time Window.
- If a Location Criteria is present and the UE location matches what is indicated in the Location Criteria.

If a matching URSP rule has no valid RSD, the UE tries other URSP rules in the order of Rule Precedence with matching Traffic descriptors, except the URSP rule with "match-all" Traffic descriptor. The UE shall not use the UE Local Configuration in this case.

When URSP rules are updated or their validity according to the conditions above change, the association of existing applications to PDU Sessions may need to be re-evaluated. The UE may also re-evaluate the application to PDU Session association due to the following reasons:

- periodic re-evaluation based on UE implementation;
- an existing PDU Session that is used for routing traffic of an application based on a URSP rule is released;
- The expiration of Time Window in Route Selection Validation Criteria, i.e. the expiration of Time Window, or UE's location no longer matches the Location Criteria.

NOTE 3: It is up to UE implementation to avoid frequent re-evaluation due to location change.

If the re-evaluation leads to a change of the application to PDU Session association, e.g. the application is to be associated with another PDU Session or a new PDU Session needs to be established, the UE may enforce such changes in a timely manner based on implementation, e.g. immediately or when UE enters CM-IDLE state.

If the selected Route Selection Descriptor contains a Non-Seamless Offload indication and the UE has established a connection to a WLAN access, the UE routes the traffic matching the Traffic descriptor of the URSP rule via the WLAN access outside of a PDU Session.

6.6.3 V2X Policy information

The V2X Policy information (V2XP) is defined in TS 23.287 [28].

Annex A (informative): URSP rules example

As an example, the URSP rules provisioned in the UE may include the following rules:

Table A-1: Example of URSP rules

Example URSP rules		Comments
Rule Precedence =1 Traffic Descriptor: Application descriptor=App1	Route Selection Descriptor Precedence=1 Network Slice Selection: S-NSSAI-a SSC Mode Selection: SSC Mode 3 DNN Selection: internet Access Type preference: 3GPP access	This URSP rule associates the traffic of application "App1" with S-NSSAI-a, SSC Mode 3, 3GPP access and the "internet" DNN. It enforces the following routing policy: The traffic of App1 should be transferred on a PDU Session supporting S-NSSAI-a, SSC Mode 3 and DNN=internet over 3GPP access. If this PDU Session is not established, the UE shall attempt to establish a PDU Session with S-NSSAI-a, SSC Mode 3 and the "internet" DNN over 3GPP access.
Rule Precedence =2 Traffic Descriptor: Application descriptor=App2	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-a Access Type preference: Non-3GPP access	This URSP rule associates the traffic of application "App2" with S-NSSAI-a and Non-3GPP access. It enforces the following routing policy: The traffic of application App2 should be transferred on. a PDU Session supporting S-NSSAI-a using a Non-3GPP access. If this PDU Session is not established, the UE shall attempt to establish a PDU Session with S-NSSAI-a over Access Type=non-3GPP access. If the PDU Session cannot be established, the traffic of App2 shall be directly offloaded to WLAN, if the UE is connected to a WLAN with SSID-a (based on the 2nd RSD)
	Route Selection Descriptor Precedence =2 Non-seamless Offload indication: Permitted (WLAN SSID-a)	
Rule Precedence =3 Traffic Descriptor: DNN=DNN_1	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-a Access Type preference: Non-3GPP access	This URSP rule associates the traffic of applications that are configured to use DNN_1 with DNN_1, S-NSSAI-a over Non-3GPP access. It enforces the following routing policy: The traffic of application(s) that are configured to use DNN_1 should be transferred on a PDU Session supporting S-NSSAI-a over Non-3GPP access. If this PDU Session is not established, the UE shall attempt to establish the PDU Session with S-NSSAI-a over Non-3GPP access.
Rule Precedence =4 Traffic Descriptor: Application descriptor=App1 Connection Capabilities="internet", "supl"	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-a DNN Selection: DNN_1 Access Type preference: Non-3GPP access	This URSP rule associates the application "App1" and the Connection Capabilities "internet" and "supl" with DNN_1, S-NSSAI-a over Non-3GPP access. It enforces the following routing policy: When the "App1" requests a network connection with Connection Capability "internet" or "supl", the UE establishes (if not already established) a PDU Session with DNN_1 and S-NSSAI-a over Non-3GPP access. After that, the UE routes the traffic of "App1" over this PDU Session.
Rule Precedence =5 Traffic Descriptor: Application descriptor=App3 Connection Capabilities="ims"	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-c DNN Selection: DNN_1 Access Type preference: Multi-Access	This URSP rule associates the application "App3" and the Connection Capability "ims" with DNN_1, S-NSSAI-c and multi-access connectivity. It enforces the following routing policy: When the "App3" requests a network connection with Connection Capability "ims", the UE establishes (if not already established) a MA PDU Session with DNN_1 and S-NSSAI-c. After that, the UE routes the traffic of "App3" over this MA PDU Session by using the received ATSSS rules.

Rule Precedence =6 Traffic Descriptor: Application descriptor=App1	Route Selection Descriptor Precedence =1 DNN Selection: DNN_1 Network Slice Selection: S-NSSAI-a Access Type preference: Multi Access	This URSP rule associates App 1 with DNN_1, S-NSSAI-a with Multi Access connectivity. It enforces the following routing policy: The traffic of Application 1 should be transferred on a PDU Session supporting S-NSSAI-a and DNN_1 according to the received ATSSS rules. After that the UE routes the traffic of any other application according to the ATSSS rule with match all packet filters if available.
Rule Precedence = lowest priority Traffic Descriptor: *	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-b SSC Mode Selection: SSC Mode 3 DNN Selection: internet	This URSP rule associates all traffic not matching any prior rule a PDU Session with S-NSSAI-b, SSC Mode 3 and the "internet" DNN. It enforces the following routing policy: All traffic not matching any prior rule should be transferred on a PDU Session supporting S-NSSAI-b, SSC Mode 3 and DNN=internet with no access network preference.

Annex B (informative): Deployment option to support of BSF and DRA coexistence due to network migration

During the network migration, DRA and BSF may coexist in operator's network. The DRA can be a consumer of Nbsf services and the BSF can provide binding functionality for different subscribers. When the AF using Rx, such as P-CSCF, sends Rx request to the DRA, if the DRA has no binding information for the subscriber, based on configuration or via NRF, it selects the BSF. Then the DRA can query the BSF by invoking Nbsf_Management discovery service operation, to get the relevant PCF address, based on which the DRA routes the Rx request to the selected PCF.

NOTE: The DRA decides to select a BSF based on user IP address range.

Annex C (Normative): Support for Application Functions supporting Rx interface

To allow the 5G system to interwork with AFs related to existing services, e.g. IMS based services as described in TS 23.228 [5], Mission Critical Push To Talk services as described in TS 23.179 [6], the PCF shall support the corresponding IMS procedures defined in the main body of this TS via Rx interface. This facilitates the migration from EPC to 5GC without requiring these AFs to upgrade to support the Npcf_PolicyAuthorization services in Rel-16.

Figure C-1: Interworking between 5G Policy framework and AFs supporting Rx interface

Session Binding applies for PDU Sessions of IP type only.

The functionality described for Multimedia Priority Services (clause 6.1.3.11) and Mission Critical service (clause 6.1.3.19) applies via Rx interface.

In order to support IMS Emergency services over Rx interface, in addition to the functional description in clause 6.1.3.10, the following applies: The PCF shall provide the IMEI and the subscriber identifiers (IMSI, MSISDN) (if available), received from the SMF at PDU Session establishment, if so requested by the P-CSCF. The PCF derives the IMEI from the PEI, the IMSI from the SUPI and the MSISDN from the GPSI.

NOTE 1: TS 23.501 [2] defines both 5G identifiers, SUPI, PEI and GPSI and then how they are allocated to allow interworking with functional entities not supporting 5G identifies such as P-CSCF.

Any AF using Rx, such as P-CSCF, the BSF determines the selected PCF address according to the information included in the incoming Rx requests and the information stored at the BSF. The BSF is able to proxy or redirect Rx requests targeting an IP address of a UE to the selected PCF.

The following event reporting is supported over Rx interface:

Table C-1: Events relevant for reporting from the PCF

Event	Description	Availability for Rx Session
PLMN Identifier Notification	The PLMN identifier where the UE is currently located.	Yes
Change of Access Type	The Access Type and, if applicable, the RAT Type of the PDU Session has changed.	Yes
EPS fallback	EPS fallback is initiated	Yes
Signalling path status	The status of the resources related to the signalling traffic of the AF session.	Yes
Access Network Charging Correlation Information	The Access Network Charging Correlation Information of the resources allocated for the AF session.	Yes
Access Network Information Notification	The user location and/or timezone when the PDU Session has changed in relation to the AF session.	Yes
Reporting Usage for Sponsored Data Connectivity	The usage threshold provided by the AF has been reached; or the AF session is terminated.	Yes
Resource allocation status	The status of the resources related to the AF session (established/released).	Yes
QoS targets can no longer (or can again) be fulfilled	The QoS targets can no longer (or can again) be fulfilled by the network for (a part of) the AF session.	No
Out of credit	Credit is no longer available.	Yes

Annex D (informative): PCC usage for sponsored data connectivity

D.1 General

With sponsored data connectivity, the Sponsor has a business relationship with the operator and the Sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.

A possible deployment configuration for sponsored data connectivity in the non-roaming case is illustrated in Figure D.1-1.

NOTE 1: Sponsored data connectivity is not supported in the roaming with visited access scenario in this Release.

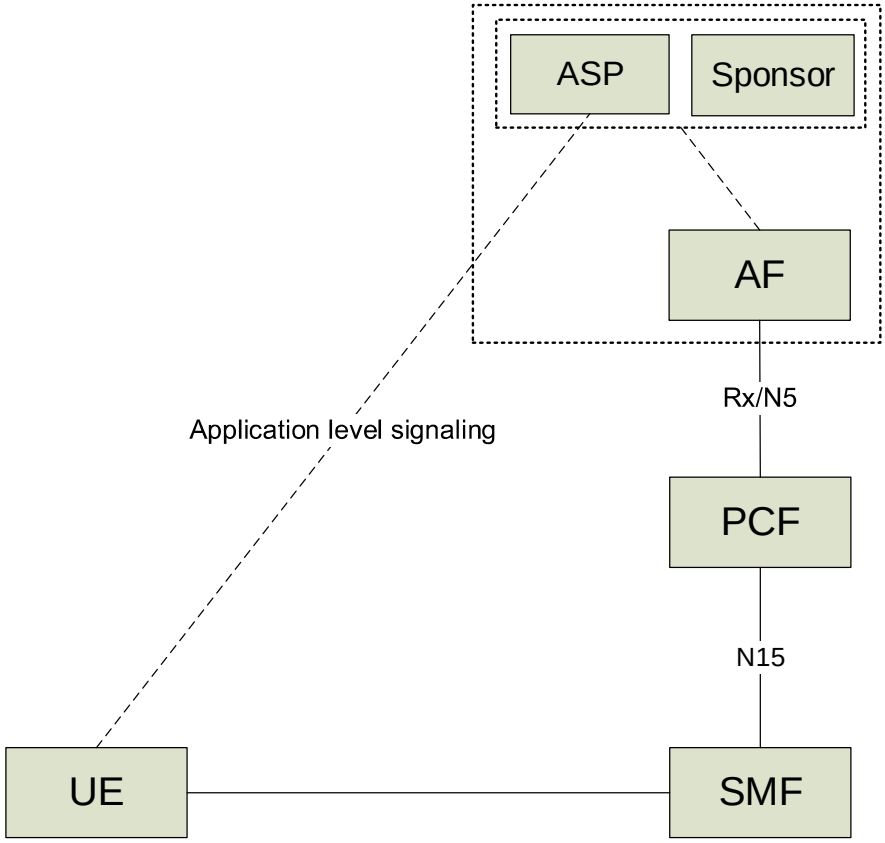

Figure D.1-1: Deployment for sponsored data connectivity

The relationship between the AF and Sponsor and between the Sponsor and ASP is out of scope of this specification. A single AF can serve multiple ASPs and multiple sponsors.

NOTE 2: An ASP can also be a sponsor.

The sponsor may choose to supply the PCF (via the AF) with the usage thresholds that it expects the SMF to enforce. Alternatively, the Sponsor can allow the ASP to enforce such control over the sponsored data connectivity.

The information required for the detection of sponsored HTTP traffic (i.e. server host name) can be verified with the corresponding server IP address/prefix of the IP packets by the SMF. The SMF uses implementation specific logic to perform this verification.

D.2 Reporting for sponsored data connectivity

There are two deployment scenarios for usage reporting for sponsored data connectivity. The Sponsor Identifier and Application Service Provider Identifier are provided for sponsored services to the PCF from the AF over the Rx/N5 interface.

In the first scenario the PCF assigns a service specific Charging Key for a sponsored IP flow. The Charging key is used by the SMF to generate separate accounting records for offline charging and and/or usage data records for online charging for the sponsored flows. Correlation of accounting records and usage data records from multiple users per sponsor and/or application service provider is then performed using the charging key.

In a second scenario the Sponsor Identifier and Application Service Provider Identity is included in PCC rules from the PCF to the SMF as defined in clause 6.3.1. For this scenario the same Charging Key may be used both for IP flows that are sponsored and for flows that are not sponsored. Accounting records generated by the SMF for offline charging include the Sponsor Identity and the Application Service Provider Identity. Correlation of accounting records from multiple users per sponsor and/or application service provider can then be based on Sponsor Identity and Application Service Provider Identity instead of the Charging Key. Usage reporting for online charging including Sponsor Identity and Application Service Provider Identity has not been specified in this release of the specification. PCC rules that include a Sponsor Identity and an Application Service Provider Identity should include a Charging Method that indicates offline charging.

Annex E (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-12	SP-78	SP-170933	-	-	-	MCC Editorial update for presentation to TSG SA#78 for approval	1.0.0
2017-12	SP-78	-	-	-	-	MCC Editorial update after TSG SA#78 Approval	15.0.0
2018-03	SP-79	SP-180107	0001	-	F	Clarification on PCF interaction	15.1.0
2018-03	SP-79	SP-180092	0002	3	F	Remove EN related with Session binding	15.1.0
2018-03	SP-79	SP-180107	0003	1	F	Correction for background data transfer for TS 23.503	15.1.0
2018-03	SP-79	SP-180093	0004	-	F	Correction on Notification control for GBR QoS flow	15.1.0
2018-03	SP-79	SP-180093	0005	1	F	Addition of Reflective QoS Timer in PDU session related policy information	15.1.0
2018-03	SP-79	SP-180107	0006	2	F	Removal of editor's notes and addition of references to empty sections	15.1.0
2018-03	SP-79	SP-180107	0007	1	F	Influence of additional non-standardized QoS parameters on QoS Flow Binding	15.1.0
2018-03	SP-79	SP-180107	0008	1	F	Description of components in URSP	15.1.0
2018-03	SP-79	SP-180107	0010	1	F	QoS rule generation	15.1.0
2018-03	SP-79	SP-180093	0011	2	F	UE policies granularity and UE assistance for policy evaluation	15.1.0
2018-03	SP-79	SP-180091	0012	1	F	Resource reservation for services sharing priority	15.1.0
2018-03	SP-79	SP-180093	0013	2	F	Add Nchf service in service base representation architecture	15.1.0
2018-03	SP-79	SP-180107	0014	-	F	Traffic mapping information that disallows UL packets	15.1.0
2018-03	SP-79	SP-180091	0016	1	F	Moving NWDAF to 23.501	15.1.0
2018-03	SP-79	SP-180107	0017	3	F	Default URSP Rule	15.1.0
2018-03	SP-79	SP-180107	0018	2	F	UE selects a PDU Session based on URSP	15.1.0
2018-03	SP-79	SP-180107	0020	2	F	Clarification on the handling of event triggers	15.1.0
2018-03	SP-79	SP-180107	0021	3	F	Update of UDR policy related subscription	15.1.0
2018-03	SP-79	SP-180107	0022	1	F	Remove EN related with EPC IWK	15.1.0
2018-03	SP-79	SP-180107	0023	-	F	Remove some ENs	15.1.0
2018-03	SP-79	SP-180107	0024	3	F	AF subscription to AMF and SMF events and events reporting	15.1.0
2018-03	SP-79	SP-180107	0025	1	F	Corrections to description of session management related policy enforcement	15.1.0
2018-03	SP-79	SP-180095	0028	2	B	Supporting 3GPP PS Data Off in 5GS	15.1.0
2018-03	SP-79	SP-180107	0031	2	F	Session Binding Mechanism for non-IP PDU Session	15.1.0
2018-03	SP-79	SP-180107	0032	2	F	Clarification on enforcement of Application Detection Control	15.1.0
2018-03	SP-79	SP-180092	0033	2	F	Resolve the Editor's Note on Presence Reporting Area	15.1.0
2018-03	SP-79	SP-180107	0034	2	F	Update of event trigger section	15.1.0
2018-03	SP-79	SP-180107	0035	5	F	Clarification on AF using legacy Rx binding with relevant PCF	15.1.0
2018-03	SP-79	SP-180125	0036	1	B	Addition of PDU Session type IPv4v6	15.1.0
2018-06	SP-80	SP-180478	0019	7	B	Additional PDU Session Type in Route Selection Descriptor	15.2.0
2018-06	SP-80	SP-180483	0037	1	F	Correction to URSP and UE preferences for NSSP and SSCMSP	15.2.0
2018-06	SP-80	SP-180481	0043	7	F	Clarification on using PSI	15.2.0
2018-06	SP-80	SP-180481	0044	7	F	Clarification on UE policy configuration	15.2.0
2018-06	SP-80	SP-180483	0046	1	F	Correction on Policy Control Request Triggers	15.2.0
2018-06	SP-80	SP-180480	0049	2	F	Clarification on match all URSP rule	15.2.0
2018-06	SP-80	SP-180480	0050	2	F	Clarification on policy provision in roaming case	15.2.0
2018-06	SP-80	SP-180478	0051	2	F	Alignment with the definition of PCF-AMF and PCF-SMF interfaces	15.2.0
2018-06	SP-80	SP-180482	0053	1	F	Cleanups on the support of session binding for Ethernet PDU session Type	15.2.0
2018-06	SP-80	SP-180486	0054	2	F	NEF and UDR in LBO architecture for AF influence on traffic routing	15.2.0
2018-06	SP-80	SP-180486	0055	5	F	Network slicing information for binding the AF request to the relevant PCF	15.2.0
2018-06	SP-80	SP-180489	0058	4	F	Support use of DNN for URSP traffic descriptor	15.2.0
2018-06	SP-80	SP-180490	0060	1	F	TS23.503 Clarification on Access and mobility related policy	15.2.0
2018-06	SP-80	SP-180490	0061	2	F	TS23.503 Clarification on BSF	15.2.0
2018-06	SP-80	SP-180490	0062	2	F	TS23.503 ePDG/N3IWF selection information	15.2.0
2018-06	SP-80	SP-180483	0063	2	F	Correction to the UE Policy Section 6.1.2.2.1	15.2.0
2018-06	SP-80	SP-180489	0064	-	F	The interaction between PCF and AF	15.2.0
2018-06	SP-80	SP-180484	0067	-	F	Corrections to PFD management descriptions	15.2.0
2018-06	SP-80	SP-180487	0068	1	F	Protocol criteria for domain name matching	15.2.0
2018-06	SP-80	SP-180484	0071	3	F	Delivery of UE policies	15.2.0
2018-06	SP-80	SP-180485	0073	2	F	How to differentiate the PSIs in different PLMNs	15.2.0
2018-06	SP-80	SP-180477	0079	-	D	Corrected the name of a PCF service operation in clause 6.1.2.2.2	15.2.0
2018-06	SP-80	SP-180485	0081	2	F	Handling of Configured NSSAIs in Roaming Scenarios - 23.503	15.2.0
2018-06	SP-80	SP-180478	0082	2	F	Alignement for policy control application specific information	15.2.0
2018-06	SP-80	SP-180490	0084	2	F	Update for usage monitoring support	15.2.0
2018-06	SP-80	SP-180490	0085	2	F	Update for sponsored data connectivity support	15.2.0
2018-06	SP-80	SP-180487	0087	5	F	Provisioning of ANDSP via signalling	15.2.0
2018-06	SP-80	SP-180483	0088	4	F	Provisioning of ANDSP via signalling	15.2.0
2018-06	SP-80	SP-180487	0089	2	F	QoS flow binding for URLLC services	15.2.0
2018-06	SP-80	SP-180487	0093	1	F	Removal of editor's notes	15.2.0
2018-09	SP-81	SP-180723	0097	1	F	PDU Session selection	15.3.0
2018-09	SP-81	SP-180723	0098	1	F	UE Policy Delivery in case of UE not reachable	15.3.0

2018-09	SP-81	SP-180724	0099	3	B	Support of tracing in 5GS signalling: PCF related data	15.3.0
2018-09	SP-81	SP-180723	0103	3	F	Number of packet filters supported by UE	15.3.0
2018-09	SP-81	SP-180723	0107	3	F	Policy Control Request triggers for updating the AM Policy Association	15.3.0
2018-09	SP-81	SP-180723	0108	2	F	N28 session termination	15.3.0
2018-09	SP-81	SP-180723	0109	2	F	URSP updates and Application to PDU session association re-evaluation	15.3.0
2018-09	SP-81	SP-180723	0111	3	F	Clarification on initial UE policy provisioning	15.3.0
2018-09	SP-81	SP-180723	0112	3	F	Notification Control applicability	15.3.0
2018-09	SP-81	SP-180723	0117	-	F	Change OCS to CHF in TS23.503	15.3.0
2018-09	SP-81	SP-180723	0119	4	F	Clarification of URSP update trigger	15.3.0
2018-09	SP-81	SP-180723	0121	3	F	BDT: clarification on network area information and ASP identifier	15.3.0
2018-09	SP-81	SP-180723	0123	1	F	Correction on UE policy delivery	15.3.0
2018-09	SP-81	SP-180723	0125	3	F	Corrections to URSP rules	15.3.0
2018-09	SP-81	SP-180723	0128	-	F	Clarification on Application identifier	15.3.0
2018-09	SP-81	SP-180723	0129	3	F	Alignment with 23502 for SBI friendly UE policy distribution	15.3.0
2018-09	SP-81	SP-180723	0131	2	F	Corrections to AF influence (5.6.7) based on CT WG3 LS on AF influence on traffic routing	15.3.0
2018-09	SP-81	SP-180723	0132	2	F	Application detection report when the PFDs are removed	15.3.0
2018-09	SP-81	SP-180723	0133	3	F	Correction on PRA	15.3.0
2018-09	SP-81	SP-180723	0135	-	F	Reference to TS 24.526	15.3.0
2018-09	SP-81	SP-180723	0138	1	F	Storage of UE Policy in VPLMN	15.3.0
2018-09	SP-81	SP-180723	0139	1	F	Binding information storage	15.3.0
2018-09	SP-81	SP-180723	0141	1	F	Update of input parameters for PCC decisions	15.3.0
2018-12	SP-82	SP-181086	0146	2	F	Clarification on UE policy distribution	15.4.0
2018-12	SP-82	SP-181084	0149	4	F	Bulk subscription to events provided by PCF	15.4.0
2018-12	SP-82	SP-181090	0150	4	F	Selection of the CHF for charging and spending limit control for the PDU session	15.4.0
2018-12	SP-82	SP-181089	0151	4	F	Extending Charging Control Data in a PCC Rule	15.4.0
2018-12	SP-82	SP-181091	0152	5	F	UE policy service update	15.4.0
2018-12	SP-82	SP-181084	0153	-	F	Alignment with 23.501 for N36	15.4.0
2018-12	SP-82	SP-181090	0154	2	F	Removing Subscribed GBR from PDU Session policy control subscription information	15.4.0
2018-12	SP-82	SP-181084	0158	5	F	AF subscribed events	15.4.0
2018-12	SP-82	SP-181218	0159	10	F	Correction on SSCMSP	15.4.0
2018-12	SP-82	SP-181086	0160	1	F	Control of QoS parameters for default QoS Flow	15.4.0
2018-12	SP-82	SP-181086	0161	-	F	Consistent usage of Policy Control Request Trigger GFBR of QoS Flow cannot be guaranteed	15.4.0
2018-12	SP-82	SP-181087	0162	5	F	Correction for URSP rule parameter traffic descriptor	15.4.0
2018-12	SP-82	SP-181087	0163	2	F	Clarification on URSP rule and UE local configuration association	15.4.0
2018-12	SP-82	SP-181087	0164	11	F	Clarification on user preference and URSP	15.4.0
2018-12	SP-82	SP-181088	0165	6	F	Efficient delivery of UE Policies	15.4.0
2018-12	SP-82	SP-181085	0166	1	F	Clarification on inclusion of list of PSIs in Initial Registration	15.4.0
2018-12	SP-82	SP-181087	0167	4	F	Correction to traffic steering control	15.4.0
2018-12	SP-82	SP-181091	0171	2	F	Updates to SMF Policy Control Request Triggers	15.4.0
2018-12	SP-82	SP-181089	0172	2	F	Location change triggers	15.4.0
2018-12	SP-82	SP-181085	0177	1	F	Clarification of the OSId and OSAppId	15.4.0
2018-12	SP-82	SP-181085	0178	2	F	Clarification of IP descriptors in URSP	15.4.0
2018-12	SP-82	SP-181089	0181	1	F	OSID storage	15.4.0
2018-12	SP-82	SP-181085	0182	2	F	Clarification on packet filter handling	15.4.0
2018-12	SP-82	SP-181090	0183	1	F	Subscriber IP index provisioning	15.4.0
2019-03	SP-83	SP-190160	0180	7	F	Indication of ANDSP (non-3GPP) support	15.5.0
2019-03	SP-83	SP-190160	0188	1	F	Correction to traffic steering control	15.5.0
2019-03	SP-83	SP-190160	0190	-	F	SEPPs in roaming architecture	15.5.0
2019-03	SP-83	SP-190160	0191	2	F	PSI list corrections	15.5.0
2019-03	SP-83	SP-190160	0193	-	F	PSI list corrections	15.5.0
2019-03	SP-83	SP-190160	0194	2	F	PSI list corrections	15.5.0
2019-03	SP-83	SP-190160	0196	2	F	Packet filters to the UE	15.5.0
2019-03	SP-83	SP-190160	0197	1	F	Alignment on UE policy delivery trigger	15.5.0
2019-03	SP-83	SP-190160	0198	1	F	UE Policy related corrections	15.5.0
2019-03	SP-83	SP-190160	0201	3	F	Clarification on URSP rule validation check	15.5.0
2019-03	SP-83	SP-190160	0202	6	F	Policy Control using DN authorization profile index	15.5.0
2019-03	SP-83	SP-190160	0203	1	F	Clarification on condition of including UE Policy Container in RR message	15.5.0
2019-03	SP-83	SP-190160	0204	3	F	Clarification for UE policy distribution	15.5.0
2019-03	SP-83	SP-190160	0207	2	F	PCC support for MCS	15.5.0
2019-03	SP-83	SP-190160	0210	2	F	Clarification on associating applications to PDU Sessions	15.5.0
2019-03	SP-83	SP-190160	0212	-	F	Corrections on routing rule	15.5.0
2019-03	SP-83	SP-190160	0221		F	Change OCS to CHF in TS 23.503	15.5.0
2019-03	SP-83	SP-190160	0222	1	F	Clarification on when PCF allocates a PSI	15.5.0
2019-03	SP-83	SP-190173	0185	4	B	PCC support for traffic switching, steering and splitting	**16.0.0**
2019-03	SP-83	SP-190173	0187	3	B	Support of ATSSS rules and URSP rules for MA-PDU Sessions	**16.0.0**
2019-03	SP-83	SP-190169	0199	4	B	N6-based traffic routing for 5G-LAN type of services	**16.0.0**

2019-03	SP-83	SP-190172	0205	2	B	Update of TS 23.503 for Rel.16 BDT Notification	**16.0.0**
2019-03	SP-83	SP-190172	0206	2	B	Use of analytics for background data transfer	**16.0.0**
2019-03	SP-83	SP-190173	0208	2	B	Support for Multi-Access PDU Session in URSP and PDU session selection	**16.0.0**
2019-03	SP-83	SP-190171	0209	-	B	Update 23.503 to support solution 13 in 23.725	**16.0.0**
2019-03	SP-83	SP-190236	0219	4	F	Replacing references to TS 23.203 with text in clauses 6.3 and 6.4	**16.0.0**
2019-03	SP-83	SP-190175	0220	2	F	Terminology alignments and editorial corrections	**16.0.0**
2019-03	SP-83	SP-190172	0224	1	C	Aligning specification with eNA TS 23.288	**16.0.0**
2019-06	SP-84	SP-190427	0215	4	F	Replacing references to TS 23.203 with context in clause 6.1.3.5	**16.1.0**
2019-06	SP-84	SP-190427	0217	4	F	Replacing references to TS 23.203 with text in clause 6.2.2	**16.1.0**
2019-06	SP-84	SP-190430	0228	1	F	Removal of Editor's note related to N6 routing	**16.1.0**
2019-06	SP-84	SP-190414	0229	-	F	QoS Flow for which the deferred activation/deactivation of PCC rule can only be used	**16.1.0**
2019-06	SP-84	SP-190414	0230	3	F	Replacing references to TS 23.203 with text for clause 6.1.3.9	**16.1.0**
2019-06	SP-84	SP-190402	0232	2	A	Alignment with stage 3 on multiple values for a PFD attribute	**16.1.0**
2019-06	SP-84	SP-190414	0235	1	C	Charging requirements and functional description	**16.1.0**
2019-06	SP-84	SP-190415	0236	2	B	Access and mobility related policy information for 5G-RG	**16.1.0**
2019-06	SP-84	SP-190415	0237	1	B	Session binding information in wireline access	**16.1.0**
2019-06	SP-84	SP-190419	0238	5	B	Support for IMS functionality using Npcf services	**16.1.0**
2019-06	SP-84	SP-190427	0240	2	F	Clarification for the association between application and PDU session	**16.1.0**
2019-06	SP-84	SP-190398	0242	6	B	Adding Support for Delivering Background Data Transfer Polices to the UE	**16.1.0**
2019-06	SP-84	SP-190412	0243	2	C	Explicit indication of AF response to be expected for runtime coordination with AF	**16.1.0**
2019-06	SP-84	SP-190420	0246	2	B	Input for PCC decision from NWDAF	**16.1.0**
2019-06	SP-84	SP-190402	0250	1	A	Clarify on the condition of setting PDU Session Type in URSP	**16.1.0**
2019-06	SP-84	SP-190402	0252	1	A	Clarification the condition of URSP rule validity on S-NSSAI for roaming case	**16.1.0**
2019-06	SP-84	SP-190414	0255	3	F	Replace the reference to 23.203 to the clause in 23.503 in 6.2.7	**16.1.0**
2019-06	SP-84	SP-190420	0256	-	B	Removal of Editor's note for BDT warning notification and define send for notification in TS23.503	**16.1.0**
2019-06	SP-84	SP-190402	0261	2	A	Alignment with 23501 on Policy Control Request Triggers relevant for SMF	**16.1.0**
2019-06	SP-84	SP-190402	0263	2	C	23.503-23203 endorsement	**16.1.0**
2019-06	SP-84	SP-190427	0264	2	C	Serving network policy control	**16.1.0**
2019-06	SP-84	SP-190414	0265	2	B	23.503 part of PCF selection for PDU sessions with same DNN and S-NSSAI	**16.1.0**
2019-06	SP-84	SP-190406	0267	-	C	PCC support for MCS Priority Levels	**16.1.0**
2019-06	SP-84	SP-190414	0269	2	F	Replace the TS 23.203 reference with the texts for PCF description in 6.2.1.1	**16.1.0**
2019-06	SP-84	SP-190431	0271	2	B	PDU session management for Background Data Transfer	**16.1.0**
2019-06	SP-84	SP-190402	0273	2	A	PCR trigger on serving node change	**16.1.0**
2019-06	SP-84	SP-190427	0274	1	F	Replacing references to TS 23.203 with text for clauses 4.3.4, 5 and 6	**16.1.0**
2019-06	SP-84	SP-190427	0275	1	F	Replacing references to TS 23.203 with text for general policy control features	**16.1.0**
2019-06	SP-84	SP-190427	0276	1	F	Replacing references to TS 23.203 with text in Annex X	**16.1.0**
2019-06	SP-84	SP-190427	0277	-	F	Replacing references to TS 23.203 with text in scope and abbreviation	**16.1.0**
2019-06	SP-84	SP-190427	0278	1	F	Replacing references to TS 23.203 with text in definitions section	**16.1.0**
2019-06	SP-84	SP-190402	0282	2	A	Adding the input from AF via NEF for PCC decisions	**16.1.0**
2019-06	SP-84	SP-190423	0285	2	C	New UE Policy Control Request Trigger for V2X	**16.1.0**
2019-09	SP-85	SP-190608	0227	7	B	QoS Monitoring to assist URLLC Service	16.2.0
2019-09	SP-85	SP-190621	0258	7	C	DNN replacement	16.2.0
2019-09	SP-85	SP-190610	0279	2	F	Update of policy framework extensions for ATSSS	16.2.0
2019-09	SP-85	SP-190618	0288	2	C	Introducing support for Ethernet port management	16.2.0
2019-09	SP-85	SP-190601	0292	1	A	Clarifications on Location change reporting to PCF	16.2.0
2019-09	SP-85	SP-190621	0295	-	F	Add missing NOTE number for PDU Session Type in RSD table	16.2.0
2019-09	SP-85	SP-190622	0297	1	F	Clarification of the use of URSP validation criteria	16.2.0
2019-09	SP-85	SP-190601	0299	-	A	Correction on the architecture	16.2.0
2019-09	SP-85	SP-190621	0300	1	F	Missing description on AF request trigger	16.2.0
2019-09	SP-85	SP-190619	0303	2	F	xBDT negotiation and BDT policy retrieval	16.2.0
2019-09	SP-85	SP-190622	0304	2	F	Alignment with SA5 on the support of offline only charging	16.2.0
2019-09	SP-85	SP-190615	0305	3	B	QoS Handling for V2X Communication Over Uu Reference Point	16.2.0
2019-09	SP-85	SP-190618	0308	3	B	TSN Support in TS 23.503	16.2.0
2019-09	SP-85	SP-190618	0309	1	F	Adding NID as input for policy decisions	16.2.0
2019-09	SP-85	SP-190618	0310	4	B	Update to Policy Framework for TSC	16.2.0
2019-09	SP-85	SP-190608	0313	1	B	QoS Monitoring parameter(s) sent to the AF	16.2.0
2019-09	SP-85	SP-190621	0315	1	F	Clarification on applicability of UE policy to PLMNs	16.2.0
2019-12	SP-86	SP-191080	0290	5	F	BDT renegotiation upon expected network performance change	16.3.0
2019-12	SP-86	SP-191089	0316	-	F	MBR of Non-GBR type 5QI	16.3.0
2019-12	SP-86	SP-191073	0320	3	C	Correction on Policy Control information to support QoS Monitoring	16.3.0
2019-12	SP-86	SP-191093	0321	6	F	DNN and slicing for xBDT	16.3.0
2019-12	SP-86	SP-191075	0322	1	F	AMF change notification	16.3.0

2019-12	SP-86	SP-191092	0325	3	F	QoS mapping for uplink TSC communication	16.3.0
2019-12	SP-86	SP-191064	0326	7	F	Correction of PCF discovery via BSF to consider eSBA binding principles	16.3.0
2019-12	SP-86	SP-191089	0327	1	F	Correction on PCC description	16.3.0
2019-12	SP-86	SP-191089	0329	3	F	23.503:PCF provides local traffic routing policy to SMF based on AF request	16.3.0
2019-12	SP-86	SP-191080	0330	1	F	Corrections for analytics	16.3.0
2019-12	SP-86	SP-191084	0331	2	F	Corrections to handling of Alternative QoS Profiles	16.3.0
2019-12	SP-86	SP-191077	0334	7	F	Selection of the preferred access type for non-MPTCP traffic in a MA PDU session	16.3.0
2019-12	SP-86	SP-191092	0336	1	F	Implement traffic correlation indicaiton of AF influence	16.3.0
2019-12	SP-86	SP-191089	0339	1	F	Aligning TS 23.503 with the CHEM feature of SA4	16.3.0
2019-12	SP-86	SP-191072	0342	6	F	SR-VCC with PS to CS handover indication	16.3.0
2019-12	SP-86	SP-191089	0348	3	F	Clarification for pre-configured URSP	16.3.0
2019-12	SP-86	SP-191075	0349	2	A	Addition of Reallocation Of Credit missing Policy Control Request Trigger	16.3.0
2019-12	SP-86	SP-191089	0354	2	F	List of NSSAIs parameter update in DNN Replacement triggers	16.3.0
2019-12	SP-86	SP-191089	0362	3	F	Clarification on Policy Control Request Triggers	16.3.0
2019-12	SP-86	SP-191075	0368	1	A	Location Change related triggers	16.3.0
2019-12	SP-86	SP-191075	0375	2	F	Clarifications on policy control related interface and functionality for MCS support	16.3.0
2019-12	SP-86	SP-191071	0376	-	F	Correction of CHF discovery to consider eSBA binding principles	16.3.0
2020-03	SP-87E	SP-200077	0344	5	F	TSN parameters	16.4.0
2020-03	SP-87E	SP-200060	0352	3	A	Location Change (Serving CN node), alignment with stage 3	16.4.0
2020-03	SP-87E	SP-200069	0361	2	F	Clarification on Access type for ATSSS	16.4.0
2020-03	SP-87E	SP-200077	372	3	F	MDBV mapping and configuration for TSC QoS Flow	16.4.0
2020-03	SP-87E	SP-200080	0381	1	F	Domain descriptors in URSP	16.4.0
2020-03	SP-87E	SP-200080	0382	1	F	SRVCC with PS to CS handover	16.4.0
2020-03	SP-87E	SP-200080	0384	2	F	Reporting event of EPS FB initiated	16.4.0
2020-03	SP-87E	SP-200065	0385	3	F	Correction of PCF discovery via BSF to consider eSBA binding principles - AF/NEF/SCP re-selection functionality (23.503)	16.4.0
2020-03	SP-87E	SP-200067	0388	1	F	Alignement on the packet delay measurement failure for the QoS monitoring support	16.4.0
2020-03	SP-87E	SP-200070	0389	2	F	Clarification of the BDT policy re-negotiation descriptions	16.4.0
2020-03	SP-87E	SP-200080	0390	3	F	Correction on the binding mechanism	16.4.0
2020-03	SP-87E	SP-200080	0391	-	F	Corrections for authorized QoS description	16.4.0
2020-03	SP-87E	SP-200080	0392	-	F	Correction about the DN Information	16.4.0
2020-03	SP-87E	SP-200077	0394	5	F	QoS flow binding for TSN streams with same periodicity	16.4.0
2020-03	SP-87E	SP-200080	0397	4	F	Clarification on support of UE policies by the UE	16.4.0
2020-03	SP-87E	SP-200070	0398	2	F	Correction on policy decision based on UE related analytics	16.4.0
2020-03	SP-87E	SP-200080	0400	4	F	Replace the reference to 23.203 to the clause in 23.503 in 4.3.6	16.4.0
2020-03	SP-87E	SP-200080	0401	4	F	Replace the reference to 23.203 to the clause in 23.503 in 6.2.3	16.4.0
2020-03	SP-87E	SP-200070	0408	1	F	Policy decisions based on Analytics	16.4.0
2020-03	SP-87E	SP-200080	0417	1	F	Correction on QoS Flow Binding for QoS Flow Behaviour	16.4.0
2020-03	SP-87E	SP-200080	0419	1	F	Corrections for event reporting from the PCF	16.4.0
2020-03	SP-87E	SP-200069	0420	1	F	Correction on QoS Flow Binding about ATSSS	16.4.0
2020-03	SP-87E	SP-200080	0423	1	F	Policy update on DNN replacement	16.4.0
2020-03	SP-87E	SP-200069	0424	1	F	Clarification on PS Data Off	16.4.0
2020-03	SP-87E	SP-200067	0429	1	F	UE notification due to Alternative QoS Profile	16.4.0
2020-04	SP-87E	SP-200077	0344	5	F	TSN parameters (MCC re-implementation of missing parts of the CR)	16.4.1
2020-07	SP-88E	SP-200425	0416	2	F	Correction on QoS Flow Binding for CN PDB	16.5.0
2020-07	SP-88E	SP-200422	0431	1	F	PCC control for DDD status and availability after DDN failure events	16.5.0
2020-07	SP-88E	SP-200439	0433	1	F	Clarification of SDF generation	16.5.0
2020-07	SP-88E	SP-200551	0434	1	F	Reallocation of credit reporting to the AF	16.5.0
2020-07	SP-88E	SP-200428	0435	1	F	Providing OSid and OSAppId in the MA PDU Session Control Information	16.5.0
2020-07	SP-88E	SP-200439	0436	-	F	QoS parameter mapping for TSN	16.5.0
2020-07	SP-88E	SP-200552	0438	-	F	Completion of description in general PCF clause	16.5.0
2020-07	SP-88E	SP-200439	0441	1	F	QoS container vs. TSCAI input container	16.5.0
2020-07	SP-88E	SP-200428	0442	1	F	Clarification on Access Type Preferrence in RSD of URSP rule	16.5.0
2020-07	SP-88E	SP-200551	0443	-	F	Correct the wrong placement of UE-AMBR	16.5.0
2020-07	SP-88E	SP-200434	0444	-	F	Correction on V2X Policy related description	16.5.0
2020-07	SP-88E	SP-200551	0447	1	F	The clarification for PDU session establishment based on URSP rule	16.5.0
2020-07	SP-88E	SP-200431	0448	1	F	Clarifications on policy decisions based on network analytics	16.5.0
2020-07	SP-88E	SP-200434	0449	1	F	Correction on QoS Flow Binding for general SMF behaviour and Alternative QoS Parameter Sets	16.5.0
2020-07	SP-88E	SP-200594	0451	2	F	URSP info provision for xBDT	16.5.0
2020-07	SP-88E	SP-200552	0452	1	F	PCC handling for MPTCP and ATSSS-LL with any Steering Mode	16.5.0
2020-07	SP-88E	SP-200428	0453	1	F	PS data off for MA PDU session when PCC is not deployed	16.5.0
2020-07	SP-88E	SP-200428	0454	-	F	Corrections for MA PDU session capabilities	16.5.0
2020-07	SP-88E	SP-200439	0455	1	F	Adding TSN AF decides the TSN Qos container	16.5.0
2020-07	SP-88E	SP-200551	0456	1	F	Use of DNN replacement when updating URSP rules	16.5.0

2020-07	SP-88E	SP-200424	0458	1	F	Routing binding indication generated by AF	16.5.0
2020-07	SP-88E	SP-200551	0459	1	F	Update to Reporting and Credit management	16.5.0
2020-07	SP-88E	SP-200439	0461	2	F	Correction to session binding for TSN	16.5.0
2020-07	SP-88E	SP-200439	0464	2	F	Updating Session Binding rule	16.5.0
2020-07	SP-88E	SP-200552	0465	1	F	Clarification on the of online charging and offline charging indication on N7 interface	16.5.0
2020-07	SP-88E	SP-200551	0466	-	F	Clarification of PCF behaviour to honor UE provided maximum packet filter support	16.5.0
2020-07	SP-88E	SP-200439	0468	-	F	Clarification of ETH Filters	16.5.0
2020-08	SP-88E	SP-200425	0472	-	F	Replacement of noted CR0472R1 with CR0472: Update about Alternative QoS Profile	16.5.1
2020-09	SP-89E	SP-200688	0475	-	F	Supplement for TSN QoS information	16.6.0
2020-09	SP-89E	SP-200688	0477	1	F	Clarification of the delay parameter for TSN QoS	16.6.0
2020-09	SP-89E	SP-200682	0478	1	F	QoS Flow establishment based on AQP	16.6.0
2020-09	SP-89E	SP-200679	0479	1	F	Alignment of BDT policy negotiation description with the procedures in TS 23.502	16.6.0
2020-09	SP-89E	SP-200679	0480	1	F	Re-ordering of interactions in the BDT policy re-negotiation description	16.6.0
2020-09	SP-89E	SP-200688	0482	1	F	Clarification on BSF behaviour for TSN service	16.6.0
2020-09	SP-89E	SP-200688	0484	1	F	Adding BMIC information to TSN part.	16.6.0
2020-09	SP-89E	SP-200682	0486	1	F	V2X Policy Control	16.6.0
2020-09	SP-89E	SP-200688	0488	-	F	23.503 - Resolution of open items related to IEEE LS	16.6.0
2020-09	SP-89E	SP-200673	0489	1	F	PCC control for DDD status and availability after DDN failure events	16.6.0
2020-12	SP-90E	SP-200951	0483	2	F	Policy control for redundant PDU Session for URLLC	16.7.0
2020-12	SP-90E	SP-200959	0491	1	F	Location change (serving cell) for Policy Control Request Trigger	16.7.0
2020-12	SP-90E	SP-200953	0494	1	F	Correction to TSN Bridge Information on N7	16.7.0
2020-12	SP-90E	SP-200955	0495	1	F	Policy subscription information extension to include ATSSS information	16.7.0
2020-12	SP-90E	SP-200959	0496	1	F	Correction on the QoS Flow binding with Alternative QoS Parameter Set(s)	16.7.0
2020-12	SP-90E	SP-200950	0499	1	F	PCC rule resource allocation outcome and its usage in AQP-based QoS Flow establishment	16.7.0
2020-12	SP-90E	SP-200954	0502	1	F	Clarification on the UE procedure for selecting a WLAN access based on WLANSP rules	16.7.0
2020-12	SP-90E	SP-200959	0503	1	F	General cleanup of specification	16.7.0
2021-03	SP-91E	SP-210053	0514	1	A	Adding DNN, S-NSSAI, IP domain to the parameters provided by BSF registration to NRF	16.8.0
2021-03	SP-91E	SP-210082	0516	1	F	QoS control in the VPLMN	16.8.0
2021-03	SP-91E	SP-210055	0522	-	F	DDN failure and DDD status events handling with V-SMF and I-SMF	16.8.0
2021-03	SP-91E	SP-210243	0523	-	F	Remove the NEF pre-configuration option for PFD push and correct the handling of Allowed Delay	16.8.0
2021-06	SP-92E	SP-210329	0537	1	F	Updates to support QoS Monitoring control for service data flows	16.9.0
2021-06	SP-92E	SP-210324	0549	-	A	Delete NSI ID via N7 interface	16.9.0
2021-06	SP-92E	SP-210324	0571	1	A	Application Identifier in the PCC Rule	16.9.0
2021-06	SP-92E	SP-210333	0588	1	F	Clarify the BDT warning description with degraded Network performance	16.9.0
2021-09	SP-93E	SP-210911	0636	-	F	Clarification on 5GS Bridge information Notification when no AF Session exists	16.10.0
2021-12	SP-94E	SP-211279	0671	1	F	Access network information request without PCC rules	16.11.0
2021-12	SP-94E	SP-211279	0683	-	F	Clarifications on Support for Application Functions supporting Rx interface	16.11.0
2022-06	SP-96	SP-220390	0729	1	F	Removal of the UE Policy Provisioning Request indication for V2XP in the Registration Request	16.12.0
2022-12	SP-98E	SP-221061	0794	2	F	Fix for Packet Delay Failure Threshold	16.13.0
2023-03	SP-99	SP-230034	0801	1	F	PDU Session Type Selection in the URSP Rule	16.14.0
2023-03	SP-99	SP-230033	0917	-	F	Removal of unspecified QoS monitoring control options	16.14.0

History

Document history		
V16.5.0	July 2020	Publication (withdrawn)
V16.5.1	September 2020	Publication
V16.6.0	October 2020	Publication
V16.7.0	January 2021	Publication
V16.8.0	April 2021	Publication
V16.9.0	July 2021	Publication
V16.10.0	September 2021	Publication
V16.11.0	January 2022	Publication
V16.12.0	July 2022	Publication
V16.13.0	January 2023	Publication
V16.14.0	April 2023	Publication