ETSI TS 129 561 V17.5.0 (2022-05)

5G;
5G System;
Interworking between 5G Network
and external Data Networks;
Stage 3
(3GPP TS 29.561 version 17.5.0 Release 17)

Reference
RTS/TSGC-0329561vh50

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 http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

The present specification defines the stage 3 interworking procedures for 5G Network interworking between PLMN and external DN or Network Slice Specific AAA.

The stage 2 requirements and procedures are contained in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

For interworking between 5G PLMN and external DNs, the present document is valid for both 3GPP accesses and non-3GPP accesses.

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: "System Architecture for the 5G System; Stage 2".

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

[4] 3GPP TS 29.281: "General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U)".

[5] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[6] IETF RFC 3748: "Extensible Authentication Protocol (EAP)".

[7] IETF RFC 3579: "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)".

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

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

[10] IETF RFC 4818: "RADIUS Delegated-IPv6-Prefix Attribute".

[11] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[12] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[13] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[14] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[15] IETF RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[16] IETF RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[17] IETF RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

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

[19] IETF RFC 1542: "Clarification and Extensions for the Bootstrap Protocol".

[20] IETF RFC 4039: "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[21] IETF RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[22] IETF RFC 3736: "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[23] IETF RFC 7155: "Diameter Network Access Server Application".

[24] IETF RFC 6733: "Diameter Base Protocol".

[25] IETF RFC 4072: "Diameter Extensible Authentication Protocol (EAP) Application".

[26] IETF RFC 2866: "RADIUS Accounting".

[27] IETF RFC 5176: "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)".

[28] 3GPP TS 23.003: "Numbering, addressing and identification".

[29] IETF RFC 1825: "Security Architecture for the Internet Protocol".

[30] IETF RFC 1826: "IP Authentication Header".

[31] IETF RFC 1827: "IP Encapsulating Security Payload (ESP)".

[32] IETF RFC 4291: "IP Version 6 Addressing Architecture".

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

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

[35] IETF RFC 1027: "Using ARP to Implement Transparent Subnet Gateways".

[36] 802.3-2015 - IEEE Standard for Ethernet.

[37] IETF RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[38] 3GPP TS 23.380: "IMS Restoration Procedures".

[39] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces; Stage 3".

[40] 3GPP TS 29.502: "5G System; Session Management Services; Stage 3".

[41] 3GPP TS 29.229: "Cx and Dx interfaces based on Diameter protocol; Protocol details".

[42] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[43] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".

[44] IETF RFC 7761: "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)".

[45] IETF RFC 3973: "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)".

[46] 3GPP TS 29.571: "5G System; Common Data Types for Service Based Interfaces Stage 3".

[47] IETF RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

[48] IETF RFC 3925: "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)".

[49] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[50] 3GPP TS 29.274: "3GPP Evolved Packet System. Evolved GPRS Tunnelling Protocol for EPS (GTPv2)".

[51] CableLabs WR-TR-5WWC-ARCH: "5G Wireless Wireline Converged Core Architecture".

[52] BBF WT-470: "5G FMC Architecture".

[53] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[54] BBF TR-456: "AGF Functional Requirements".

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

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

[57] IETF RFC 2661: " Layer Two Tunneling Protocol "L2TP".

[58] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane of EPC Nodes; Stage 3".

[59] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G-BRG	5G Broadband Residential Gateway
5G-CRG	5G Cable Residential Gateway
AMF	Access and Mobility Management Function
BBF	Broadband Forum
CH	Credentials Holder
CHAP	Challenge Handshake Authentication Protocol
CHF	Charging Function
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DN	Data Network
DNAI	DN Access Identifier
DR	Designated Router
DSL	Digital Subscriber Line
FN-BRG	Fixed Network Broadband RG
FN-CRG	Fixed Network Cable RG
FQDN	Fully Qualified Domain Name
GCI	Global Cable Identifier
GLI	Global Line Identifier
GPSI	Generic Public Subscription Identifier

HFC	Hybrid Fiber Coax
I-SMF	Intermediate SMF
L2TP	Layer Two Tunneling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
N3IWF	Non-3GPP InterWorking Function
NGAP	NG Application Protocol
NSS	Network Slice Specific
NSSAAF	Network Slice-Specific Authentication and Authorization Function
PAP	Password Authentication Protocol
PIM	Protocol-Independent Multicast
PIM-DM	Protocol-Independent Multicast- Dense Mode
PIM-SM	Protocol-Independent Multicast- Sparse Mode
PON	Passive Optical Network
PtP	Point-to-Point
RG	Residential Gateway
RP	Rendezvous Point
RSN	Redundancy Sequence Number
SD	Slice Differentiator
SFD	Start Frame Delimiter
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SNPN	Stand-alone Non-Public Network
SSC	Session and Service Continuity
SST	Slice/Service Type
TNAP	Trusted Non-3GPP Access Point
TWAP	Trusted WLAN Access Point
UPF	User Plane Function
V-SMF	Visited SMF
WAN	Wide Area Network

4 Network Characteristics

4.1 Key characteristics of PLMN

The PLMN is fully defined in the 3GPP technical specifications. The 5G Network related key characteristics are defined in 3GPP TS 23.501 [2].

4.2 Key characteristics of IP Networks

The Internet is a conglomeration of networks utilising a common set of protocols. IP protocols are defined in the relevant IETF RFCs. The networks topologies may be based on LANs (e.g. Ethernet), Point to Point leased lines, PSTN, ISDN, X.25 or WANs using switched technology (e.g. SMDS, ATM).

4.3 Key characteristics of Ethernet

The Ethernet is a family of computer networking technologies commonly used in LAN and is often used to refer to all Carrier Sense Multiple Access/Collision Detection (CSMA/CD) LANs that generally conform to Ethernet Specifications, including IEEE 802.3 [36]. The key characteristics for Ethernet are defined in IEEE 802.3 [36].

5 Interworking Classifications

5.1 Service Interworking

Service interworking is required when the Teleservice at the calling and called terminals are different. No service interworking is specified in this specification.

5.2 Network Interworking

Network interworking is required whenever a PLMN is involved in communications with another network to provide end-to-end communications. The PLMN shall interconnect in a manner consistent with that of a normal Data Network (type defined by the requirements e.g. IP). Interworking appears exactly like that of Data Networks.

6 Reference Architecture

Figure 6-1 shows the access interfaces for the 5G Network. Figure 6-2 shows the access interfaces for the 5G and EPC interworking network.

The 5G Network includes both the 3GPP access and the non-3GPP access.

The NSS-AAA may belong to the H-PLMN in the 5G Network (without AAA-P interworking) or a 3rd party (with AAA-P interworking).

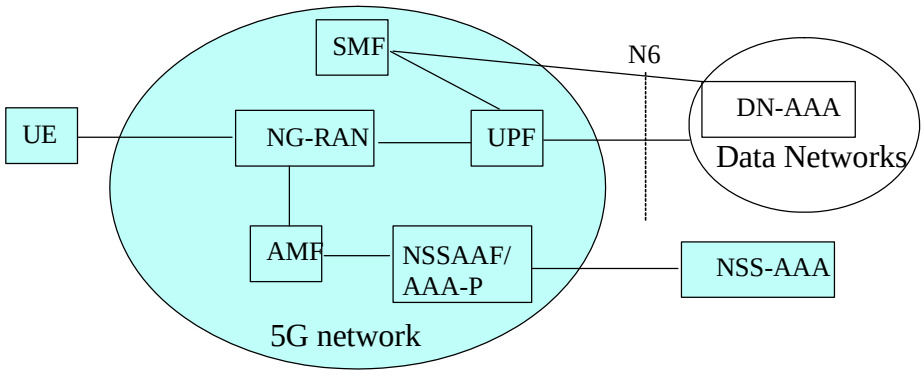

Figure 6-1: Reference Architecture for 5G Network Interworking

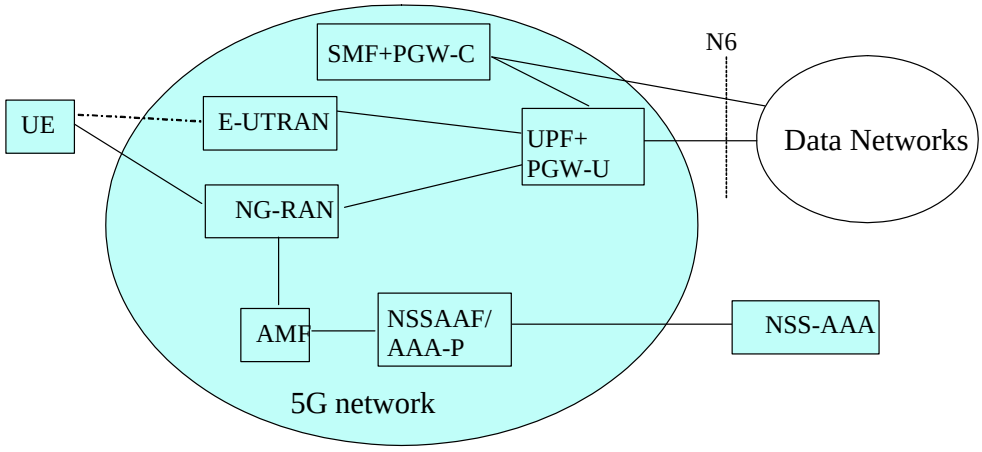

Figure 6-2: Reference Architecture for 5G and EPC Interworking

NOTE 1: The SMF represents the H-SMF and the SMF+PGW-C represents the H-SMF+ H-PGW-C in the home routed scenario.

NOTE 2: If the DN-AAA server located in 5GC or in the external PDN is reachable directly, then the SMF can communicate with the DN-AAA server directly without involving the UPF, applicable to all the message flows on N6 interface in clause 11 and clause 12 in this specification.

7 Interface to 5G Network services (User Plane)

The user plane for 5G Network services is defined in subclause 8.3 of 3GPP TS 23.501 [2] and 3GPP TS 29.281 [4].

8 Interworking with DN (IP)

8.1 General

5GS shall support interworking with DNs based on the Internet Protocol (IP). These interworked networks may be either intranets or the Internet.

8.2 DN Interworking Model

8.2.1 General

When interworking with the IP networks, the 5GS can operate IPv4 and/or IPv6. The interworking point is shown in clause 6.

The UPF for interworking with the IP network is the 5GS access point (see figure 8.2.1-1).

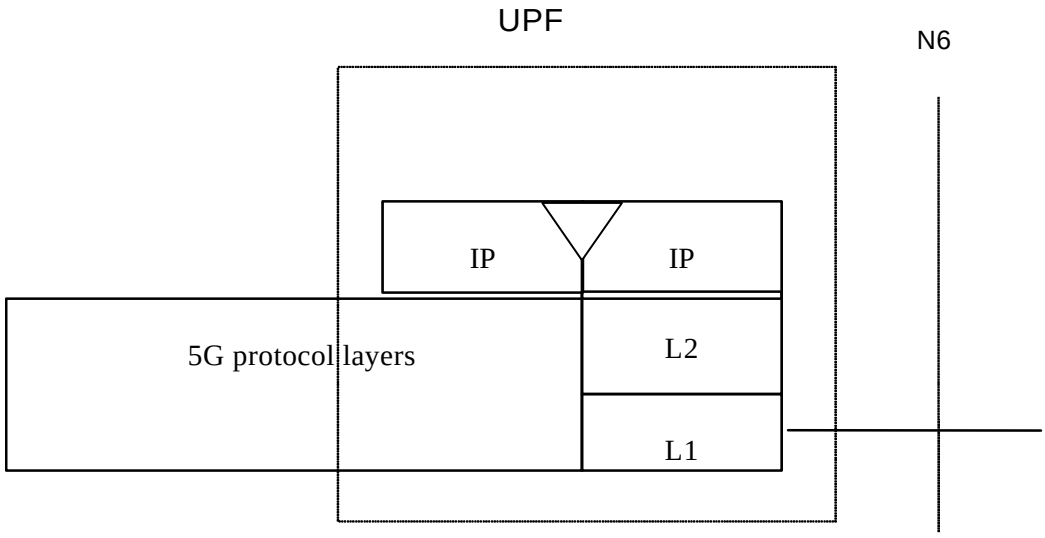

Figure 8.2.1-1: The protocol stacks of UPF for the IP network interworking

Typically, in the IP networks, the interworking with subnetworks is done via IP routers. The N6 reference point is between the UPF and the external IP network. From the external IP network's point of view, the UPF is seen as a normal IP router. The L2 and L1 layers are operator specific.

It is out of the scope of the present document to standardise the router functions and the used protocols in the N6 reference point.

Interworking with user defined ISPs and private/public IP networks is subject to interconnect agreements between the network operators.

8.2.2 Access to DN through 5G Network

8.2.2.1 Transparent access to DN

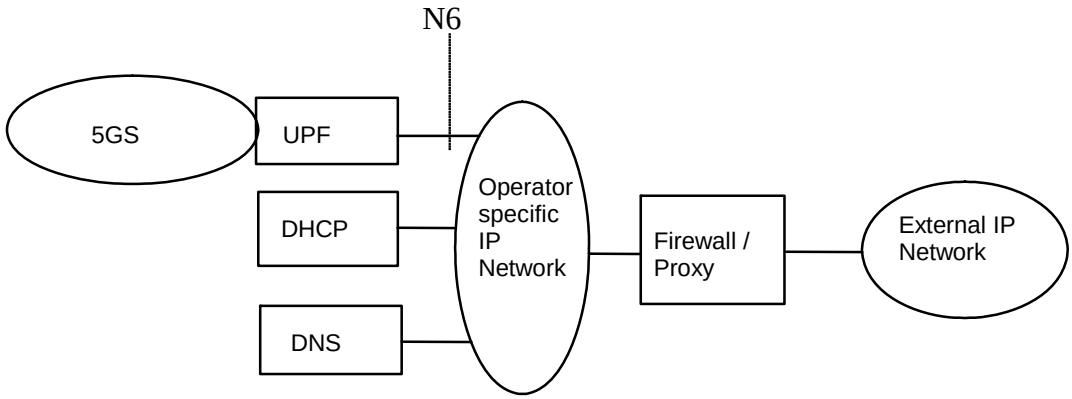

Figure 8.2.2.1-1: Example of the DN Interworking Model, transparent case

In figure 8.2.2.1-1, an example DN interworking model for transparent access to the Internet is provided for an UPF in the 5GS and its N6 reference point.

In transparent access to the Internet case:

- the UE is given an IPv4 address and/or an IPv6 prefix belonging to the operator addressing space. The IPv4 address and/or IPv6 prefix is assigned either at subscription in which case it is a static address or at PDU session establishment in which case it is a dynamic address. This IPv4 address and/or IPv6 prefix if applicable is used for packet forwarding between the Internet and the UPF and within the 5GS. With IPv6, Stateless Address Autoconfiguration shall be used to assign an IPv6 address to the UE. These procedures are as described in the IPv6 non-transparent access case except that the addresses belong to the operator addressing space.

- the UE need not send any authentication request at PDU session establishment procedure and the SMF/UPF need not take any part in the user authentication/authorization process.

The transparent case provides at least a basic ISP service. As a consequence of this it may therefore provide a QoS flow service for a tunnel to a private Intranet. The user level configuration may be carried out between the UE and the intranet, the 5GS is transparent to this procedure. The used protocol stack is depicted in figure 8.2.2.1-2.

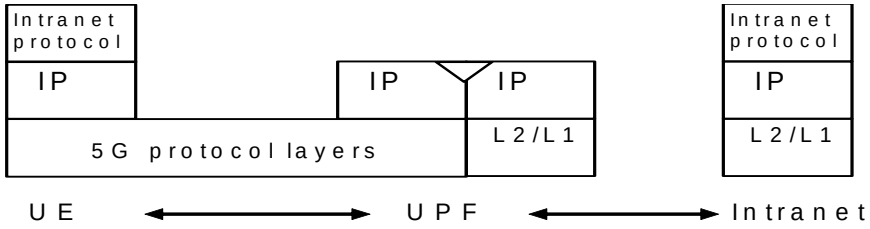

Figure 8.2.2.1-2: Transparent access to an Intranet

The communication between the PLMN and the Intranet may be performed over any network, even an insecure network e.g. the Internet. There is no specific security protocol between the UPF and the Intranet because security is ensured on an end to end basis between the UE and the intranet by the "Intranet Protocol".

User authentication and encryption of user data are done within the "Intranet Protocol" if either of them is needed. This "Intranet Protocol" may also carry private (IP) addresses belonging to the address space of the Intranet.

An example of an "Intranet Protocol" is IPsec (see IETF RFC 1825 [29]). If IPsec is used for this purpose, then IPsec authentication header or security header may be used for user (data) authentication and for the confidentiality of user data (see IETF RFC 1826 [30] and IETF RFC 1827 [31]). In this case private IP tunnelling within public IP takes place.

8.2.2.2 IPv4 Non-transparent access to DN

In this case:

- a static or a dynamic IPv4 address belonging to the Intranet/ISP addressing space is allocated to a UE at PDU session establishment. The methods of allocating IP address to the UE are specified in 3GPP TS 23.501 [2]. The allocated IPv4 address is used for packet forwarding within the UPF and for packet forwarding on the Intranet/ISP;

- as a part of the PDU session establishment, the SMF may request user authentication from an external DN-AAA server (i.e. RADIUS, Diameter) belonging to the Intranet/ISP;

- the IPv4 address allocation to the UE may be performed based on the subscription or a local address pool, which belongs to the Intranet/ISP addressing space, provisioned in the SMF; or via the address allocation servers (i.e. DHCPv4, RADIUS DN-AAA, Diameter DN-AAA) belonging to the Intranet/ISP;

- if requested by the UE at PDU session establishment, the SMF may retrieve the Protocol Configuration Options or IPv4 configuration parameters from a locally provisioned database in SMF and/or from some external server (i.e. DHCPv4, RADIUS DN-AAA, Diameter DN-AAA) belonging to the Intranet/ISP;

- the communication between the 5GS and the Intranet/ISP may be performed over any network, even an insecure network, e.g. the Internet. In case of an insecure connection between the UPF and the Intranet/ISP, there may be a specific security protocol in between. This security protocol is defined by mutual agreement between PLMN operator and Intranet/ISP administrator.

Table 8.2.2.2-1 summarizes the IPv4 address allocation and parameter configuration use cases between the UE and the SMF that may lead the SMF to interwork with the external DHCPv4, DN-AAA servers. For detailed description of the signalling flows between the UE and the SMF, see the references in the table.

Table 8.2.2.2-1: IPv4 address allocation and parameter configuration use cases

Signalling use cases between UE and SMF	Signalling use cases between SMF and external servers		
	Authentication via RADIUS or Diameter DN-AAA server (clauses 11 or 12) (NOTE 1 NOTE 2 and NOTE 4)	IPv4 Address allocation via DHCPv4 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12) (NOTE 1 and NOTE 2)	IPv4 parameter configuration via DHCPv4 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12) (NOTE 1 and NOTE 2)
(1) IPv4 address allocation and parameter configuration via activation of QoS flow associated with the default QoS rule (2) IPv4 address allocation and parameter configuration via DHCPv4 signalling from UE towards SMF (NOTE 3)	X	X	X
(3) IPv4 address allocation and parameter configuration in untrusted non-3GPP IP access	X	X	X

NOTE 1: When the SMF interworks with AAA servers, the DNN may be configured to interwork with either Diameter DN-AAA or RADIUS DN-AAA server.
NOTE 2: If RADIUS DN-AAA or Diameter DN-AAA server is used, the authentication, IPv4 address allocation and parameter configuration signalling may be combined. Similarly, if DHCPv4 server is used for IPv4 address allocation and parameter configuration, the signalling towards the DHCPv4 server may be combined.
NOTE 3: If the authentication and authorization procedure towards RADIUS DN-AAA or Diameter DN-AAA is required, it is performed by the SMF before the DHCPv4 signalling when it receives the initial access request (i.e. Nsmf_PDUSession_CreateSMContext).
NOTE 4: The UEs may provide PAP/CHAP user credentials in the ePCO IE when accessing to 5GS or 5GS interworking with EPS on 3GPP and non-3GPP IP accesses. If such information is provided to the SMF or SMF+PGW-C, the SMF or SMF+PGW-C may perform user authentication with the DN-AAA server based on these credentials.

NOTE: External network operators intending to use PAP/CHAP without proper underlying protection for authentication are warned about the respective vulnerabilities of PAP and CHAP protocols from a security point of view. It's up to the external network operator to perform the risk assessment if PAP/CHAP is used for authentication.

8.2.2.3 IPv6 Non-transparent access to DN

When using IPv6 Address Autoconfiguration, the process of setting up the access to an Intranet or ISP involves two signalling phases. The first signalling phase is done in the control plane and consists of the PDU session establishment for 5GS 3GPP or non-3GPP based access, followed by a second signalling phase done in the user plane.

The user plane signalling phase shall be stateless. The stateless procedure, which involves only the UE and the SMF, is described in subclause 10.2. 3.

For DNNs that are configured for IPv6 address allocation, the SMF shall only use the Prefix part of the IPv6 address for forwarding of mobile terminated IP packets. The size of the prefix shall be according to the maximum prefix length for a global IPv6 address as specified in the IPv6 Addressing Architecture, see IETF RFC 4291 [32].

The SMF indicates to the UE that Stateless Autoconfiguration shall be performed by sending Router Advertisements as described in subclause 10.2.3 and according to the principles defined in IETF RFC 4861 [33] and IETF RFC 4862 [34].

For UE supporting IPv6, IPv6 Stateless Address Autoconfiguration is mandatory.

In this case, the SMF provides the UE with an IPv6 Prefix belonging to the Intranet/ISP addressing space. A dynamic IPv6 address is given using stateless address autoconfiguration. This IPv6 address is used for packet forwarding within the UPF and for packet forwarding on the Intranet/ISP.

When an SMF receives an initial access request (i.e. Nsmf_PDUSession_CreateSMContext) message, the SMF deduces from local configuration data associated with the DNN:

- The source of IPv6 Prefixes (SMF internal prefix pool, or external address allocation server);
- Any server(s) to be used for address allocation, authentication and/or protocol configuration options retrieval (e.g. IMS related configuration, see 3GPP TS 24.229 [13]);
- The protocol, i.e. RADIUS, Diameter or DHCPv6, to be used with the server(s);
- The communication and security feature needed to communicate with the server(s).

As an example, the SMF may use one of the following options:

- SMF internal Prefix pool for IPv6 prefixes allocation and no authentication;
- SMF internal Prefix pool for IPv6 prefixes allocation and RADIUS for authentication. The RADIUS DN-AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the SMF;
- RADIUS for authentication and IPv6 prefix allocation. The RADIUS DN-AAA server responds with either an Access-Accept or an Access-Reject to the RADIUS client in the SMF.

The SMF includes the IPv6 address composed of a Prefix and an Interface-Identifier in the initial access response (Namf_Communication_N1N2MessageTransfer). The Interface-Identifier may have any value and it does not need to be unique within or across DNNs. It shall however not conflict with the Interface-Identifier that the SMF has selected for its own side of the UE-SMF link. The Prefix assigned by the SMF or the external DN-AAA server shall be globally or site-local unique (see the Note in subclause 11.3 of this document regarding the usage of site-local addresses).

Table 8.2.2.3-1 summarizes the IPv6 prefix allocation and parameter configuration use cases between the UE and the SMF that may lead the SMF to interwork with the external RADIUS DN-AAA, Diameter DN-AAA and DHCPv6 servers. For detailed description of the signalling flows between the UE and the SMF, see the references in the table.

Table 8.2.2.3-1: IPv6 prefix allocation and parameter configuration use cases

Signalling use cases between UE and SMF	Signalling use cases between SMF and external servers		
	Authentication via RADIUS or Diameter DN-AAA server (clauses 11 or 12) (NOTE 1 NOTE 2 and NOTE 3)	IPv6 prefix allocation via DHCPv6 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12) (NOTE 1 and NOTE 2)	IPv6 parameter configuration via DHCPv6 or RADIUS or Diameter DN-AAA server (clauses 10, 11 or 12) (NOTE 1 and NOTE 2)
(1) IPv6 address allocation and parameter configuration (2) IPv6 parameter configuration via stateless DHCPv6	X	X	X
(3) IPv6 address allocation and parameter configuration in untrusted non-3GPP IP access	X	X	X
NOTE 1: When the SMF interworks with DN-AAA servers, the DNN may be configured to interwork with either Diameter DN-AAA or RADIUS DN-AAA server. NOTE 2: If RADIUS DN-AAA or Diameter DN-AAA server is used, the authentication, IPv6 prefix allocation and parameter configuration signalling may be combined. Similarly, if DHCPv6 server is used for IPv6 prefix allocation and parameter configuration, the signalling towards the DHCPv6 server may be combined. NOTE 3: The UEs may provide PAP/CHAP user credentials in the ePCO IE when accessing to 5GS or 5GS interworking with EPS on 3GPP and non-3GPP IP accesses. If such information is provided to the SMF or SMF+PGW-C, the SMF or SMF+PGW-C may perform user authentication with the DN-AAA server based on these credentials.			

NOTE: External network operators intending to use PAP/CHAP without proper underlying protection for authentication are warned about the respective vulnerabilities of PAP and CHAP protocols from a security point of view. It's up to the external network operator to perform the risk assessment if PAP/CHAP is used for authentication.

For IPv6 the PDU session establishment phase is followed by an address autoconfiguration phase. IPv6 prefix is delivered to UE in Router Advertisement message from the SMF which acts as an access router, in the process of IPv6 Stateless Address Autoconfiguration as described in subclause 10.2.2. Besides DHCPv6 protocol, the SMF may also use RADIUS or Diameter protocol for the retrieval of an IPv6 prefix from external DN.

9 Interworking with DN (Unstructured)

9.1 General

When support of unstructured PDU type data is provided at the N6 interface, different Point-to-Point (PtP) tunneling techniques may be used. When using PtP tunneling by UDP/IPv6 encapsulation subclause 9.2 below shall be followed. Other techniques as described in subclause 9.3 below may be used.

In the following subclauses, the AS is used as an example for the destination in the external DN.

9.2 N6 PtP tunnelling based on UDP/IP

N6 PtP tunnelling based on UDP/IPv6 may be used to deliver unstructured PDU type data to the AS.

The PtP tunnel is set up by configuration of tunnel parameters in both end of the tunnel. The following parameters are pre-configured in the UPF per DNN:

- the UDP destination port number to use when sending unstructured PDU type data;
- the UDP port number it wants to receive unstructured PDU type data;
- the destination IP address to be used for sending unstructured PDU type data.

The following is pre-configured in the AS:

- the UDP destination port number to use when sending unstructured PDU type data;
- the UDP port number it wants to receive unstructured PDU type data.

NOTE 1: The UPF as well as the AS can use any UDP port numbers not assigned by IANA. The port numbers used need to be aligned between peers.

IP address allocation procedures for the UE (i.e. PDU session) are performed by the SMF as described in subclause 6.3.2, but the IPv6 prefix is not provided to the UE, i.e. Router Advertisements and DHCPv6 are not performed. The SMF assigns a suffix (i.e. IPv6 Interface Identifier) for the PDU session. For the N6 PtP tunnel, the IPv6 prefix allocated for the PDU session plus suffix assigned for the PtP tunnel is used as source address for the uplink data and as destination address for the downlink data.

During the PDU session establishment, the UPF associates the GTP-U tunnel for the PDU session with the N6 PtP tunnel.

The UPF acts as a transparent forwarding node between the UE and the AS.

For uplink delivery, if the uplink data is received from the GTP-U tunnel, the UPF shall forward the received data to the AS over the N6 PtP tunnel associated with the GTP-U tunnel with the destination address of the AS and the configured UDP destination port number for unstructured PDU type data.

For downlink delivery, the AS shall send the data using UDP/IP encapsulation with the IPv6 prefix plus suffix as destination address and the configured UDP destination port number for unstructured PDU type data.

NOTE 2: The UPF decapsulates the received data (i.e. removes the UDP/IPv6 headers) and forwards the data on the GTP-U tunnel identified by the IPv6 prefix of the UE (i.e. PDU session) for delivery to the UE.

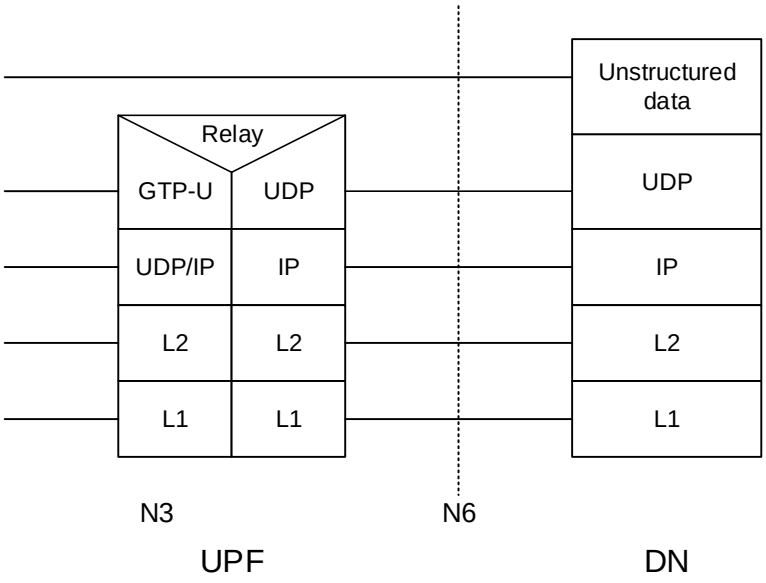

Figure 9.2-1: Protocol configuration for unstructured PDU type data (user plane) using N6 UDP/IPv6 PtP tunneling

9.3 Other N6 tunnelling mechanism

N6 PtP tunnelling mechanisms such as PMIPv6/GRE, L2TP, etc, may be used to deliver unstructured PDU type data to AS. The general handling of such delivery mechanisms is as described below.

A PtP tunnel is established by the UPF towards the AS. Depending on the type of protocol employed on the N6 PtP tunnel, the N6 PtP tunnel setup may be done at the time of PDU Session establishment or at the time of first MO datagram being sent by the UE. The UPF selects the AS based on its configuration (e.g. per DNN, or per PtP tunnel type, etc). However, IP address allocation procedures for the UE (according to subclause 6.3.2) are not performed by the SMF.

NOTE: An AS can be dedicated for handling a specific protocol for unstructured PDU type data.

The UPF acts as a transparent forwarding node between the UE and the AS.

For uplink delivery, the UPF forwards the received data to the AS over the established N6 PtP tunnel.

For downlink delivery, the AS locates the right N6 PtP tunnel for the UE (using information such as UE identifiers in the unstructured PDU type protocol itself, etc) to forward the data. The AS sends the data to UPF over the established N6 PtP tunnel. The UPF in turn sends the data on the GTP-U tunnel identified by the associated N6 PtP tunnel for delivery to the UE.

10 Interworking with DN (DHCP)

10.1 General

In current LAN environments the most commonly used configuration protocol is DHCP (Dynamic Host Configuration Protocol, RFC 2131 [18]) and DHCPv6 (Dynamic Host Configuration Protocol for IPv6, IETF RFC 3315 [21]). It provides a mechanism for passing a large set of configuration parameters to hosts connected to a TCP/IP network (IP address, sub-net mask, domain name, MTU, etc.) in an automatic manner. Moreover, DHCP may assign IP addresses to clients for a finite lease time, allowing for sequential reassignment of addresses to different users.

The lease time is chosen by the administrator of the DHCP server (in the external network), and is therefore out of the scope of the present document.

The 3GPP network may obtain IP address via external DHCP server during the PDU establishment procedure, the SMF acts a DHCP server towards the UE and it acts as a DHCP client towards the external DHCP server.

In the following cases the PDU session associated with the allocated IPv4 address or IPv6 prefix shall be released:

- if the DHCP lease expires;
- if the DHCP renewal is rejected by the DHCP server;
- if the IP address is changed during the renewal process. Usually when the lease is renewed, the IP address remains unchanged. However, if for any reason (e.g. poor configuration of the DHCP server), a different IP address is allocated during the lease renewal process the associated PDU session shall be released.

A RG may request DHCP singalling for a UE behind the RG as specified in 3GPP TS 23.316 [43].When handling DHCP signalling coming from the wireline BBF access, the SMF shall support the DHCP signalling as described in BBF TR-456 [54].

10.2 DN interworking Model of SMF for DHCP

10.2.1 Introduction

A DHCP client shall be located in the SMF used for interworking with the IP network as illustrated in figure 10.2.1-1.

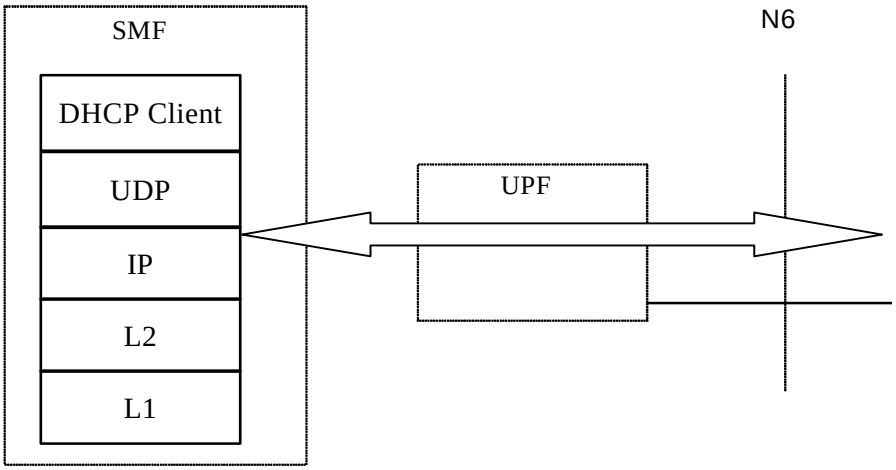

Figure 10.2.1-1: The protocol stacks for the N6 reference point for DHCP

The DHCP client function in the SMF shall be used to allocate IPv4 address or IPv6 prefix to the UE and/or to configure associated parameters via external DHCP servers. The SMF shall have both DHCPv4 and DHCPv6 client functions.

The procedures where the DHCP client function in the SMF is used are further described in 3GPP TS 23.501 [2]. The procedures are IPv4 address allocation and IPv4 parameter configuration via an external DHCPv4 server; IPv6 Prefix allocation via stateless address autoconfiguration; and IPv6 parameter configuration via stateless DHCPv6. These procedures are detailed in the subclauses below.

10.2.2 IPv4 Address allocation and IPv4 parameter configuration via DHCPv4

The UE may obtain the IPv4 address and/or its configuration parameters at or after the initial access signalling (i.e. Nsmf_PDUSession_CreateSMContext) to the 3GPP network. The request for IPv4 address and/or configuration parameters from the UE may trigger the SMF acting as a DHCPv4 client to request the IPv4 address and/or configuration parameters from an external DHCPv4 server and deliver them to the UE. The DHCPv4 functions in the SMF, the UE and the external DHCPv4 server shall be compliant to IETF RFC 2131 [18], IETF RFC 1542 [19] and IETF RFC 4039 [20].

The following system procedure describes the successful IPv4 address allocation and parameter configuration signalling flow between the SMF and the external DHCPv4 server as depicted in figure 10.2.2-1. For a detailed description of the DHCPv4 messages, refer to IETF RFC 2131 [18], IETF RFC 1542 [19] and IETF RFC 4039 [20].

1) The DHCPv4 client function in the SMF sends a DHCPDISCOVER as an IP limited broadcast message, i.e. the destination address 255.255.255.255, towards the external DN. If the SMF has the DHCPv4 server IP addresses configured for the DNN, the DHCPDISCOVER shall be send as unicast (or even multicast) to the external DHCPv4 servers.

2) Upon receiving the DHCPDISCOVER request message, the external DHCPv4 servers reply by sending a DHCPOFFER message including an offered IP address. Several DHCPOFFER messages may be received by the SMF if multiple DHCPv4 servers respond to the DHCPDISCOVER.

3) The DHCPv4 client function in the SMF processes the messages and sends a DHCPREQUEST towards the selected external DHCPv4 server.

NOTE: If the optimized signalling (Rapid Commit Option) is used as per IETF RFC 4039 [20], the messages 2-3 can be eliminated.

4) Upon receiving the DHCPREQUEST message, the selected external DHCPv4 server acknowledges the address allocation by sending a DHCPACK containing the lease period (T1), the time-out time (T2) and the

configuration information requested in DHCPREQUEST. The SMF stores the allocated IPv4 address, the lease timers and the configuration parameters. The SMF shall further deliver the IPv4 address and the configuration parameters to the UE by SM NAS message.

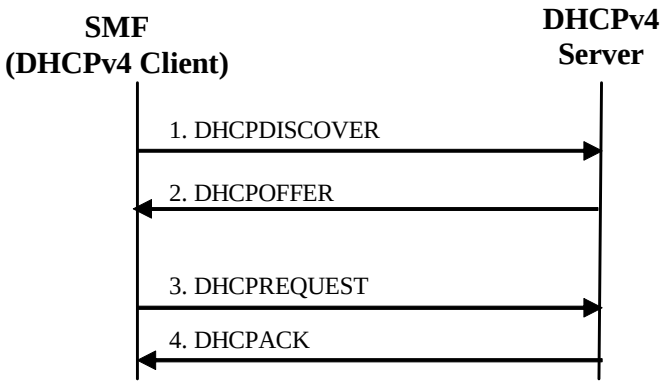

Figure 10.2.2-1: The signalling flow for IPv4 address allocation and parameter configuration using DHCPv4

Figure 10.2.2-2 is a signalling flow for IPv4 address lease renew by using DHCPv4 protocol as specified in IETF RFC 2131 [18].

1) The DHCPv4 client function in the SMF sends a unicast DHCPREQUEST towards the external DHCPv4 server to extend the lease period of the allocated IPv4 address.

2) The external DHCPv4 server replies with a DHCPACK message confirming the renewed lease and the T1 and T2 timers are restarted.

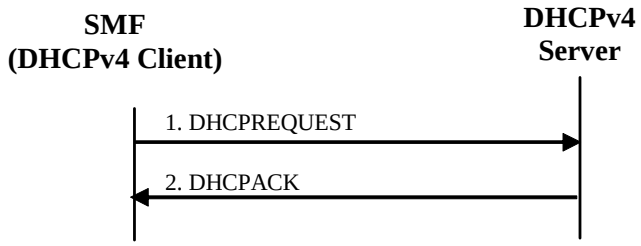

Figure 10.2.2-2: The signalling flow for IPv4 address lease renew using DHCPv4

10.2.3 IPv6 Prefix allocation via IPv6 stateless address autoconfiguration via DHCPv6

When the IPv6 prefix is allocated from the external DN, the SMF is responsible to obtain the IPv6 prefix for external DN, allocate and release the IPv6 prefix. The SMF may use DHCPv6 to obtain the IPv6 prefix from the external DN. In this context, the SMF shall act as a DHCP client as per IETF RFC 3315 [21] towards the external DHCPv6 server.

The SMF may allocate a second IPv6 prefix for routing traffic via a second UPF to enable simultaneous access via remote and local networks or to enable SSC mode 3 (i.e. make-before-break) mobility, as described in subclause 4.3.5.3 of 3GPP TS 23.502 [3].

The following system procedure describes the signalling flows for the IPv6 Stateless Address Autoconfiguration procedures for 5G system. The procedures are based on the descriptions in 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3].

1. UE initiates the PDU Session Establishment procedure, indicating IPv6 address is required.

2. The AMF sends PDU Session Establishment Request in Nsmf_PDUSession_CreateSMContext to the SMF.

3. The SMF may retrieve IPv6 prefix using DHCPv6 mechanism. This procedure is performed when an external DN allocates an IPv6 prefix, the signaling between the SMF and external DN is exchanged via UPF which is omitted in the figure 10.2.3-1.

4. The SMF sends PDU Session Establishment Accept included in Namf_Communication_N1N2MessageTransfer to the AMF. It includes the IPv6 prefix.

5. The AMF sends PDU Session Establishment Accept message to the UE without the IPv6 prefix. The UE shall ignore the IPv6 prefix if it receives it in the message.

6. The UE may send a Router Solicitation to the SMF via the UPF to solicit a Router Advertisement message.

7. The SMF sends a Router Advertisement message to the UE via the UPF, solicited or unsolicited. It shall include an IPv6 prefix in Prefix Information option field of the message. The prefix is the same as the one in the PDU Session Establishment Accept message, if it is provided during the previous PDU Session Establishment procedure.

8. At any time after PDU session establishment, the SMF may trigger the establishment on an alternative route via UPF2 for access to a local data network or for SSC mode 3 mobility.

9. Like step 3, the SMF may retrieve a second IPv6 prefix using DHCPv6 mechanism.

10. The SMF sends a Router Advertisement to the UE via UPF2 to update the UE. Note that this will occur without a Router Solicitation since the UE is unaware of the network's decision to form an alternative Route.

11. Specific to the case of SSC mode 3 mobility, the SMF sends a Router Advertisement to the UE via UPF1 with zero value in the preferred lifetime field and a value in the valid lifetime field according to IETF RFC 4862 [34]. The UE shall update the valid lifetime of the old IPv6 prefix to the signalled value, regardless of the remaining lifetime. The signalled lifetime value indicates how long the SMF is willing to keep the old IPv6 prefix.

NOTE: Alternative routes can be established repeatedly through additional UPFs and old routes can be terminated when required by the SMF. More complex scenarios are not described here for the sake of simplicity.

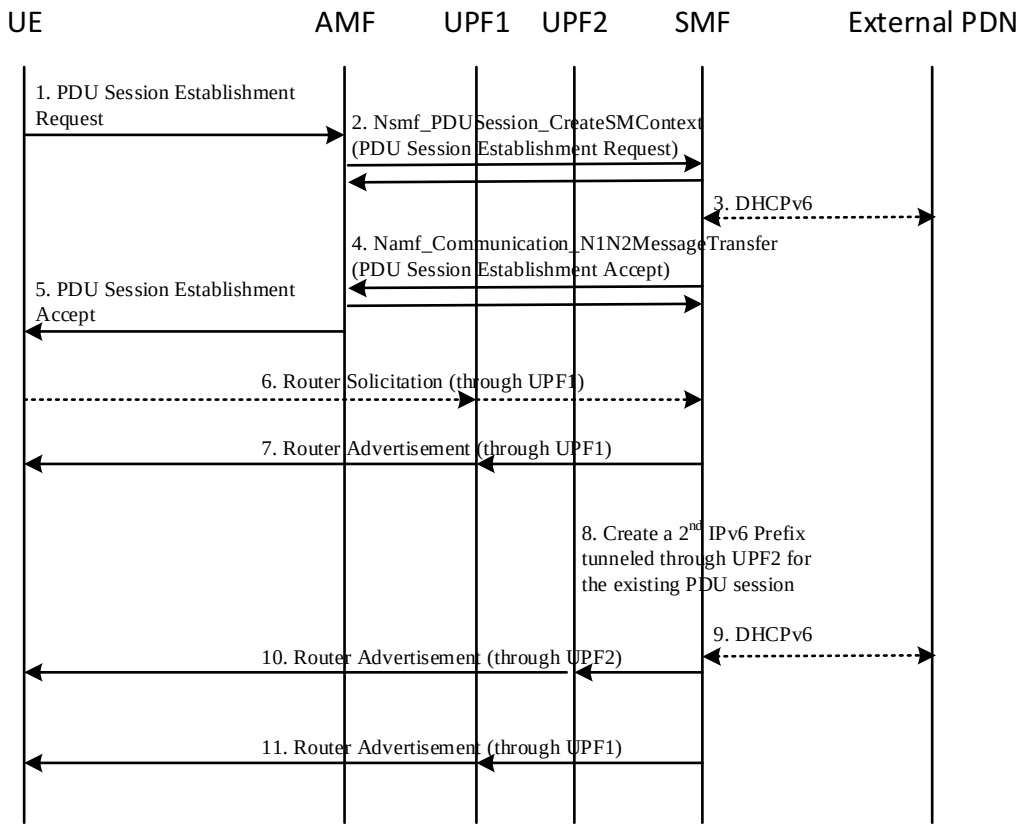

Figure 10.2.3-1: IPv6 Stateless Address Autoconfiguration

10.2.4 IPv6 parameter configuration via stateless DHCPv6

A UE that has obtained an IPv6 address may use stateless DHCP to request other configuration information such as a list of DNS recursive name servers or SIP servers.

For 3GPP networks, when an external DHCPv6 server in a DN is used to obtain the requested parameters, the SMF acts as a DHCPv6 client towards the external DHCPv6 server while acting a DHCPv6 server towards the UE.

The IPv6 parameter configuration via stateless DHCPv6 function in the UE, the SMF and the external DHCPv6 Server shall be compliant to IETF RFC 3736 [22]. The following system procedure describes the signalling flows for the IPv6 parameter configuration via stateless DHCPv6 procedures for 5G system. All messages in the following steps between the UE and the SMF are sent via the UPF.

1) A Router Advertisement with the O-flag set, is sent from SMF to UE to indicate to it to retrieve other configuration information.

2) The UE sends an INFORMATION-REQUEST message with the IP destination address set to the All_DHCP_Relay_Agents_and_Servers multicast address defined in the DHCPv6 IETF RFC 3315 [21]. The source address shall be the link-local address of the UE. The DHCP relay agent in the SMF shall forward the message.

3) DHCP servers receiving the forwarded INFORMATION-REQUEST message, reply by sending a RELAY-REPLY message, with the "Relay Message" option including a REPLY message with the requested configuration parameters.

   The UE chooses one of the possibly several REPLY messages and extracts the configuration information.

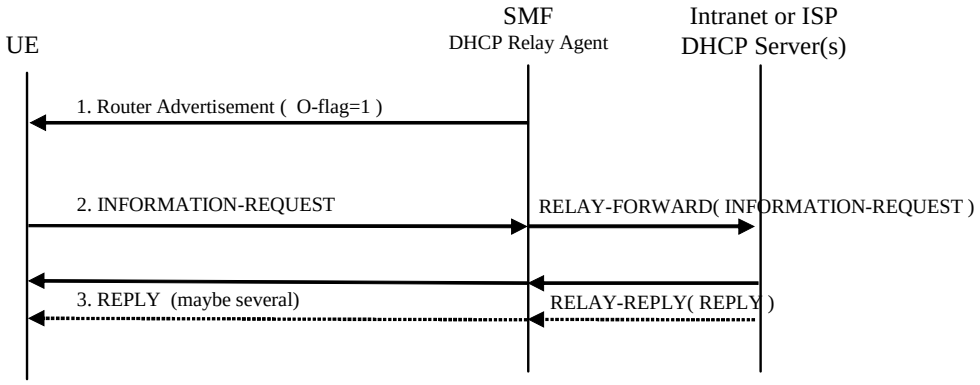

Figure 10.2.4-1: DHCPv6 Other configuration signal flow

10.2.5 IPv6 Prefix Delegation via DHCPv6

A RG may request IPv6 prefix allocation for UE behind the RG as specified in 3GPP TS 23.316 [43]. A SMF may receive both DHCP options for IA_NA and IA_PD together in a single DHCPv6 message, the SMF may provide a reply to both IA_NA and IA_PD in the same message or alternatively process the DHCPv6 IA_NA before the DHCPv6 IA_PD.

Optionally, a single network prefix shorter than the default /64 prefix may be assigned to a PDU Session. In this case, the /64 default prefix used for IPv6 stateless autoconfiguration will be allocated from this network prefix; the remaining address space from the network prefix can be delegated to the PDU Session using prefix delegation after the PDU session Setup/default QoS flow establishment and IPv6 prefix allocation via IPv6 stateless address autoconfiguration as defined in subclause 10.2.3. When PLMN based parameter configuration is used, the SMF provides the requested IPv6 prefix from a locally provisioned pool. When external DN based IPv6 prefix allocation is used, the SMF may obtain the prefix from the external DN.

For the detailed description of the RG uses DHCPv6 to request additional IPv6 prefixes refer to 3GPP TS 23.316 [43].The use of prefix exclude option is optional, and it is possible for SMF to assign a /64 prefix using stateless address autoconfiguration and a completely different shorter prefix using DHCPv6 Prefix Delegation.

10.3 3GPP Vendor-Specific Options

This clause describes 3GPP Vender-Specific Options that will be included in DHCP messages exchanged between SMF and DHCP Server. Other DHCP options may be used as defined in DHCP RFC(s). Unless otherwise stated, when the encoding scheme of an attribute is specified as UTF-8 encoding, this shall be interpreted as UTF-8 hexadecimal encoding.

The DHCPv4 vendor specific option is encoded as per IETF RFC 2132 [47] or IETF RFC 3925 [48]. The DHCPv6 vendor specific option is encoded as per IETF RFC 8415 [49]. For DHCP vendor specific option code 17 or 125, the Enterprise Number shall be set to value 10415.

The table 10.3-1 lists the encapsulated 3GPP Vendor-Specific Options in DHCP vendor specific option (17/43/125).

Table 10.3-1: List of the encapsulated 3GPP Vendor-Specific sub-options

Sub-opt #	Sub-option Name	Presence
1	3GPP-IP-Pool-Info	Optional

1 – 3GPP-IP-Pool-Info

DHCPv4

Octets	Bits 8 7 6 5 4 3 2 1
1	VS option code = 1
2	VS option length
3-m	IP address pool ID

DHCPv6

Octets	Bits 8 7 6 5 4 3 2 1
1-2	VS option code = 1
3-4	VS option length
5-m	IP address pool ID

VS option code: 1

Length: m-2 or m-4

The IP address pool ID is of Octet String type.

The SMF may determine an IP address pool ID based on UPF ID, S-NSSAI, DNN, and IP version as described in subclause 5.8.2.2.1 in 3GPP TS 23.501 [2] and includes the IP address pool ID within 3GPP Vendor-Specific-Option and send it to the DHCP server. The DHCP server assigns IPv6 prefix or IPv4 address from the requested IP address pool. Multiple 3GPP-IP-Pool-Info sub-options may be sent in a DHCP request message. The DHCP server shall return the selected IP address pool ID within 3GPP Vendor-Specific-Option to the SMF in the DHCP successful response message (e.g. DHCPACK).

11 Interworking with DN-AAA (RADIUS)

11.1 RADIUS procedures

11.1.1 RADIUS Authentication and Authorization

The SMF also represents the H-SMF in the home routed scenario in this subclause unless specified otherwise.

RADIUS Authentication and Authorization shall be used according to IETF RFC 2865 [8], IETF RFC 3162 [9] and IETF RFC 4818 [10]. In 5G, multiple authentication methods using Extensible Authentication Protocol (EAP) may be

used such as EAP-TLS (see IETF RFC 5216 [11]), EAP-TTLS (see IETF RFC 5281 [37]). The SMF shall implement the RADIUS extension to support EAP as specified in IETF RFC 3579 [7].

The RADIUS client function may reside in an SMF. When the SMF receives an initial access request (i.e. the SMF receives the Nsmf_PDUSession_CreateSMContext request with type "Initial request" for non-roaming case or local breakout case, or the H-SMF receives the Nsmf_PDUSession_Create Request with type "Initial request" for home routed case), the RADIUS client function may send the authentication information to a DN-AAA server, which is identified during the DNN provisioning.

When the legacy applications require PAP/CHAP authentication with the UE accessing to the 5GS or to the 5GC and EPC interworking scenario and the legacy DN-AAA server does not support EAP, PAP/CHAP may be used as the authentication protocol, with the external network performing the risk assessment.

The DN-AAA server performs authentication and authorization. The response (when positive) may contain network information, such as an IPv4 address and/or IPv6 prefix for the user when the SMF is interworking with the DN-AAA server.

The information delivered during the RADIUS authentication can be used to automatically correlate the user identity (e.g. SUPI) to the IPv4 address and/or IPv6 prefix, if applicable, assigned/confirmed by the SMF or the DN-AAA server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' DN-AAA server.

For 5G, RADIUS Authentication is applicable to the initial access request. When the SMF receives an Access-Accept message from the DN-AAA server it shall complete the initial access procedure. If Access-Reject or no response is received, the SMF shall reject the initial access procedure with a suitable cause code.

When DN-AAA server authorizes the PDU Session Establishment, it may send DN authorization data for the established PDU Session to the SMF. The DN authorization data for the established PDU Session may include one or more of the following:

- a reference to authorization data for policy and charging control locally configured in the SMF or PCF;
- a list of allowed MAC addresses (maximum 16) for the Ethernet PDU Session;
- a list of allowed VLAN Ids (maximum 16) for the Ethernet PDU Session;
- Session-AMBR for the PDU Session;
- L2TP information, such as LNS IP address and/or LNS host name; and
- Framed Route information for the PDU Session.

NOTE: If the DN-AAA server send L2TP information to SMF, the L2PT information can e.g. be provisioned per DNN/S-NSSAI or per SUPI or GPSI by configuration which is out of the scope of 3GPP specifications.

SMF policies may require DN authorization without DN authentication. In that case, when contacting the DN-AAA server for authorization, the SMF shall provide the GPSI of the UE if available.

The SMF may also use the RADIUS re-authorization procedure for the purpose of IPv4 address and/or IPv6 prefix allocation to the UE. The use cases that may lead this procedure are:

- IPv4 address and/or IPv6 prefix allocation after UPF selection during PDU session establishment procedure.
- IPv6 prefix allocation during adding additional PDU Session Anchor procedure for IPv6 multi-homing.
- IPv4 address allocation via DHCPv4 procedure after successful PDU session establishment procedure.

The SMF may also trigger request for DN authentication/authorization and/or IP address/prefix allocation based on UE subscription data retrieve from the UDM as defined in subclause 5.2.2.2.5 of 3GPP TS 29.503.

When an IPv4 address and/or IPv6 prefix (including any additional IPv6 prefix of IPv6 multi-homing) is (re-)allocated or de-allocated (not causing the PDU session to be released) by using a method not via the DN-AAA server and if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the authentication session that was established before to inform the DN-AAA server by sending RADIUS Access-Request with the latest list of IPv4 address and/or IPv6 prefix(es).

When the SMF is notified by the UPF regarding the UE MAC address change (a new one is detected or a used one is inactive), if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the authentication session that was established before to inform the DN-AAA server by sending RADIUS Access-Request with the latest list of UE MAC addresses in use.

DN-AAA may initiate QoS flow termination and re-authorization, see details in clause 11.2.3 and clause 11.2.4. In the present release, the DN-AAA initiated re-authentication is not supported.

For the 5GS interworking with EPS scenario, EAP based secondary authentication and re-authentication is not applicable to the PDN connection when the UE is in EPS in this release.

In case EAP based authentication and authorization has been performed for the PDU Session while the UE was in 5GS, and if SMF+PGW-C determines that the UE has moved to the EPS (i.e. the SMF+PGW-C receives the modify bearer request or create session request from the S-GW), the following applies:

- the SMF+PGW-C may initiate RADIUS re-authorization procedure without re-authentication with the DN-AAA server based on local policy.
- DN-AAA initiated re-authorization without re-authentication may be performed.

11.1.2 RADIUS Accounting

RADIUS Accounting shall be used according to IETF RFC 2866 [26], IETF RFC 3162 [9] and IETF RFC 4818 [10].

The RADIUS accounting client function may reside in an SMF. The RADIUS accounting client may send information to a DN-AAA server, which is identified during the DNN provisioning. The DN-AAA server may store this information and use it to automatically identify the user. This information can be trusted because the 3GPP network has authenticated the subscriber (i.e. USIM card and possibly other authentication methods).

The SMF may use the RADIUS Accounting-Request Start and Stop messages during QoS flow (e.g. QoS flow associated with the default QoS rule) establishment and termination procedures, respectively.

The use of Accounting-Request STOP and in addition the Accounting ON and Accounting OFF messages may be used to ensure that information stored in the DN-AAA server is synchronised with the SMF information.

If the DN-AAA server is used for IPv4 address and/or IPv6 prefix assignment, then, upon reception of a RADIUS Accounting-Request STOP message for all QoS flows associated to a PDU session defined by DNN and SUPI or GPSI, the DN-AAA server may make the associated IPv4 address and/or IPv6 prefix available for assignment.

When an IPv4 address and/or IPv6 prefix (including any additional IPv6 prefix of IPv6 multi-homing) is (re-)allocated or de-allocated (not causing the PDU session to be released) by using a method not via the DN-AAA server and if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the accounting session that was established before to inform the DN-AAA server by sending RADIUS Accounting-Request Interim-Update with the latest list of IPv4 address and/or IPv6 prefix(es).

When the SMF is notified by the UPF regarding the UE MAC address change (a new one is detected or a used one is inactive), if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the accounting session that was established before to inform the DN-AAA server by sending RADIUS Accounting-Request Interim-Update with the latest list of UE MAC addresses in use.

In order to avoid race conditions, the SMF shall include a 3GPP Vendor-Specific sub-attribute "Session Stop indicator" when it sends the Accounting-Request STOP for the last QoS flow of a PDU session and the PDU session is terminated (i.e. the IPv4 address and/or IPv6 prefix and any associated GTP tunnel can be released). The DN-AAA server shall not assume the PDU session terminated until an Accounting-Request STOP with the Session Stop indicator is received.

11.2 Message flows on N6 interface

11.2.1 Authentication, Authorization and Accounting procedures

The SMF also represents the H-SMF in the home routed scenario in this subclause unless specified otherwise.

When an SMF receives an initial access request (i.e. the SMF receives the Nsmf_PDUSession_CreateSMContext request with type "Initial request" for non-roaming case or local breakout case, or the H-SMF receives the Nsmf_PDUSession_Create Request with type "Initial request" for home routed case) message for a given DNN, the SMF may (depending on the configuration for this DNN) send a RADIUS Access-Request message with EAP extension to a DN-AAA server. The SMF may also (depending on the configuration for this DNN) send the S-NSSAI and the PDU Session ID that are associated with the PDU Session, respectively in the 3GPP-Session-S-NSSAI VSA and the 3GPP-Session-Id VSA, to a DN-AAA server. Upon receipt of the Access-Request message, the DN-AAA server shall respond with an Access-Challenge message. Multi-round authentication using the Access-Challenge (sent by DN-AAA) and Access-Request messages may be used. The DN-AAA server finally authenticates and authorizes the user by replying with an Access Accept message. If the DN-AAA server is also responsible for IPv4 address and/or IPv6 prefix allocation, the DN-AAA server shall return the allocated IPv4 address and/or IPv6 prefix in the Access-Accept message.

For re-authentication and re-authorization, the SMF shall send a RADIUS Access-Request message with EAP extension and the DN-AAA shall respond with an Access-Challenge message. Multi-round authentication using the Access-Challenge (sent by DN-AAA) and Access-Request messages may be used. The DN-AAA server finally authenticates and authorizes the user by replying with an Access Accept message.

The SMF may initiate RADIUS re-authorization procedures for the purpose of IPv4 address and/or IPv6 prefix allocation (or renew the lease). In this case, the SMF shall set the Service-Type attribute to "Authorize Only" and the 3GPP-Allocate-IP-Type subattribute to the type of IP address to be allocated in the Access-Request message sent to the DN-AAA server. If the SMF is using DHCP signalling towards the UE and the DN-AAA server includes the Session-Timeout attribute in the Access-Accept, the SMF may use the Session-Timeout value as the DHCP lease time. The SMF shall not set the DHCP lease time value higher than the Session-Timeout value. The SMF may renew the DHCP lease to the UE without re-authorization towards the DN-AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the SMF wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

Even if the SMF was not involved in user authentication, it may send a RADIUS Accounting-Request (START) message to a DN-AAA server. This message may contain parameters, e.g. the tuple which includes the user ID and IPv4 address and/or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message may also (depending on the configuration for the DNN) contains the S-NSSAI and the PDU Session ID that are associated with the PDU Session, respectively in the 3GPP-Session-S-NSSAI VSA and the 3GPP-Session-Id VSA, and/or AF traffic influence PCC rule provisioned and then SMF used DNAI in the 3GPP-DNAI VSA, to a DN-AAA server. This message also indicates to the AAA server that the user session has started. The user session is uniquely identified by the Acct-Session-Id that is composed of the Charging ID and the SMF IP address.

NOTE: If the accounting session is required by the DN-AAA server to be created per QoS flow, how to identify the different accounting sessions is implementation specific. The SMF can include the Acct-Session-Id which is extended to include the QFI of the QoS flow or the Acct-Session-Id without QFI extension and with 3GPP-NSAPI combination in the RADIUS Accounting-Request (START).

If some external applications require RADIUS Accounting-Request (START) information before they can process user packets, then the selected DNN (SMF) may be configured in such a way that the UPF is instructed to drop user data until the Accounting-Response (START) is received from the AAA server. The SMF may wait for the Accounting-Response (START) before sending the final authentication response message in Namf_Communication_N1N2MessageTransfer service operation. The SMF may reject the initial access request if the Accounting-Response (START) is not received. The authentication and accounting servers may be separately configured for each DNN.

For IPv4 PDU type, if IPv4 address is allocated via DHCPv4 signalling between the UE and the DN-AAA after PDU session establishment, the SMF may wait to send the Accounting-Request (START) message until the UE receives its IPv4 address in a DHCPACK.

When the SMF receives a message indicating a QoS flow or PDU session release request and providing a RADIUS Accounting-Request (START) message was sent previously, the SMF shall send a RADIUS Accounting-Request (STOP) message to the DN-AAA server, which indicates the termination of this particular QoS flow or PDU session. The SMF shall immediately send the corresponding response (e.g. Nsmf_PDUSession_UpdateSMContext response) to the AMF, without waiting for an Accounting-Response (STOP) message from the DN-AAA server.

The DN-AAA server shall deallocate the IPv4 address and/or IPv6 prefix initially allocated to the subscriber, if there is no session for the subscriber.

Accounting-Request (ON) and Accounting-Request (OFF) messages may be sent from the SMF to the DN-AAA server to ensure the correct synchronization of the session information in the SMF and the DN-AAA server.

The SMF may send an Accounting-Request (ON) message to the DN-AAA server to indicate that a restart has occurred. The DN-AAA server may then release the associated resources.

Prior to a scheduled restart, the SMF may send Accounting-Request (OFF) message to the DN-AAA server. The DN-AAA server may then release the associated resources.

The following figure 11.2.1-1 is an example message flow to show the procedure of RADIUS Authentication and Accounting between an SMF and a DN-AAA server:

1. UE initiates the PDU Session Establishment procedure, including authentication/authorization information.

2. The AMF sends Nsmf_PDUSession_CreateSMContext Request including the authentication/authorization information to the SMF and the SMF responds to the service operation.

   According to the configuration in the SMF, step 6 to step 9 are executed before step 3 if the SMF needs to send an EAP-Request message to the UE.

   In the case of home routed, the AMF sends Nsmf_PDUSession_CreateSMContext Request including the authentication/authorization information to the V-SMF and the V-SMF sends Nsmf_PDUSession_Create Request including the authentication/authorization information to the H-SMF.

3. If the N4 session has not been established before, the SMF triggers the N4 Session Establishment procedure to the UPF.

   In the case of home routed, the V-SMF triggers the N4 Session Establishment procedure to the V-UPF and the H-SMF triggers the N4 Session Establishment procedure to the H-UPF.

4. The SMF sends the Access-Request message to the DN-AAA via the UPF, the message is forwarded from the SMF to the DN-AAA by the UPF in N4 user plane message.

   In the case of home routed, the H-SMF sends the Access-Request message to the DN-AAA via the H-UPF, the message is forwarded from the H-SMF to the DN-AAA by the H-UPF in N4 user plane message.

5-10. The DN-AAA responds with the Access-Challenge message to the SMF via the UPF, the message is forwarded from the DN-AAA to the SMF by the UPF in N4 user plane message. The authentication/authorization information is further transferred to UE via Namf_Communication_N1N2MessageTransfer service and NAS SM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message and Nsmf_PDUSession_UpdateSMContext service, then finally sent to the DN-AAA by the SMF, via the UPF, in the Access-Request message.

   In the case of home routed, the DN-AAA responds with the Access-Challenge message to the H-SMF via the H-UPF, the message is forwarded from the DN-AAA to the H-SMF by the H-UPF in N4 user plane message. The authentication/authorization information is transferred to V-SMF via Nsmf_PDUSession_Update service and is further transferred to UE via Namf_Communication_N1N2MessageTransfer service and NAS SM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message, Nsmf_PDUSession_UpdateSMContext service and Nsmf_PDUSession_Update servic, then finally sent to the DN-AAA by the H-SMF, via the H-UPF, in the Access-Request message.

NOTE: Step 5 to step 10 can be repeated depending on the authentication/authorization mechanism used (e.g. EAP-TLS).

11. The SMF receives the final result of authentication/authorization from the DN-AAA in the Access-Accept message, via the UPF.

12. The SMF requests to start accounting by sending the Accounting-Request (START) message to the DN-AAA via the UPF.

13. The SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information in Namf_Communication_N1N2MessageTransfer service.

In the case of home routed, the H-SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information is transferred to V-SMF via Nsmf_PDUSession_Update service and is further transferred to the AMF via Namf_Communication_N1N2MessageTransfer service.

14. The DN-AAA responds with the Accounting-Response (START) message. The SMF may wait for the Accounting-Response (START) before sending the Namf_Communication_N1N2MessageTransfer request in step 13.

    In the case of home routed, the H-SMF may wait for the Accounting-Response (START) before sending the Nsmf_PDUSession_Update service in step 13.

15. The AMF sends the NAS PDU Session Establishment Request with the authentication/authorization information to the UE.

16. The UE sends a NAS message Deregistration Request to the AMF.

17. The AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the SMF and the SMF responds to the service operation.

    In the case of home routed, the AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the V-SMF and the V-SMF sends the Nsmf_PDUSession_Release Request to the H-SMF.

18-19. The SMF requests to stop accounting by sending the Accounting-Request (STOP) message to the DN-AAA via the UPF and the DN-AAA responds with the Accounting-Response (STOP) message.

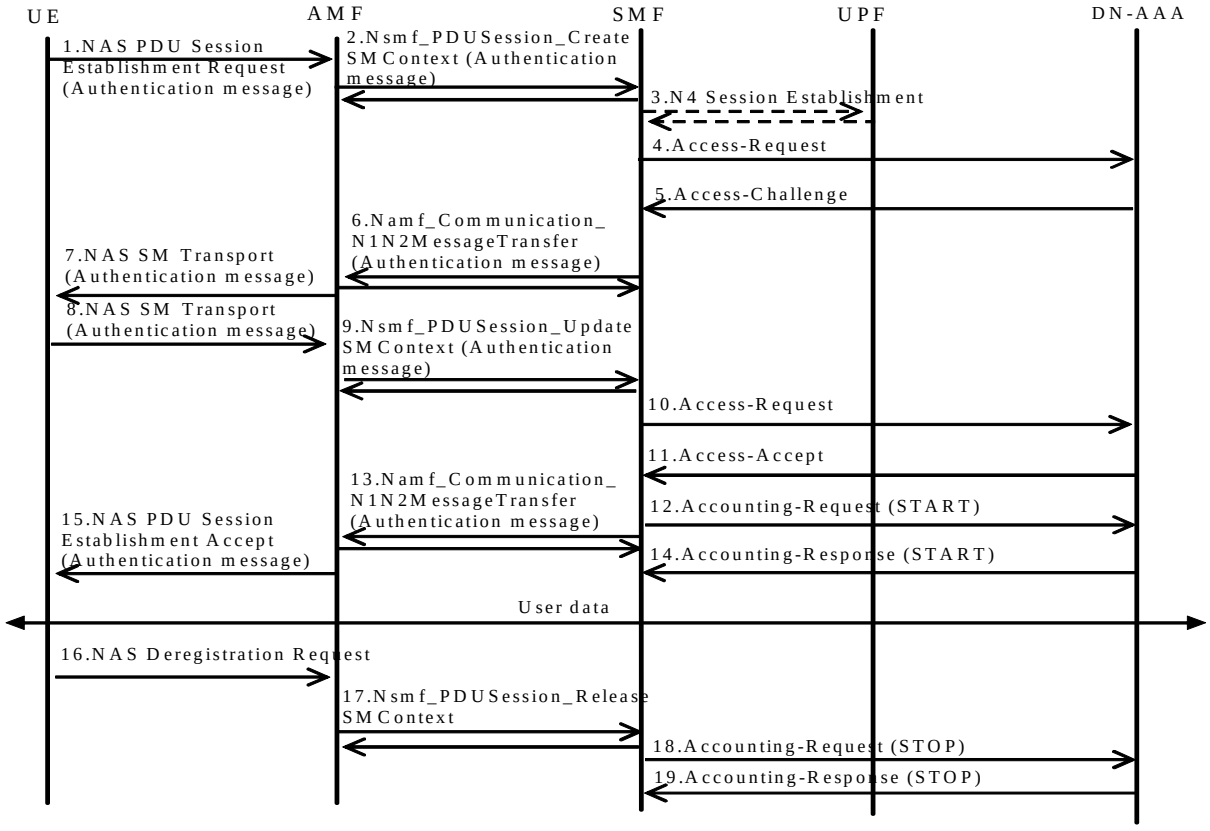

Figure 11.2.1-1: RADIUS Authentication and Accounting example (successful case)

When PAP/CHAP is used as the authentication protocol with the external DN-AAA server which does not support EAP for the 5GS or for the 5GC and EPC interworking scenarios, the RADIUS Authentication procedures refer to the non transparent access procedures in subclause 11.2.1 and the related RADIUS Authentication description in subclause 16.3a.1 in 3GPP TS 29.061 [5] are reused with the following differences:

- the SMF or SMF+PGW-C performs the actions specified for the P-GW;
- the external DN-AAA server performs the actions specified for AAA;

- PDU Session Establishment request is sent from the UE to the SMF or SMF+PGW-C instead of the Activate PDN connection request being sent from the UE to the S-GW and the Create Session request being sent from S-GW to P-GW;
- PDU Session Establishment accept is sent from the SMF or SMF+PGW-C to the UE instead of the Create Session Response message being sent from the P-GW to S-GW and the Activate PDN Connection Accept being sent from S-GW to the UE; and
- PDU Session Establishment reject is sent from the SMF or SMF+PGW-C to the UE instead of the Create Session Response message being sent from the P-GW to the S-GW and the Activate PDN Connection Reject being sent from S-GW to the UE.

11.2.2 Accounting Update

During the life of a QoS flow some information related to this QoS flow may change. The SMF may send RADIUS Accounting Request Interim-Update to the DN-AAA server upon occurrence of a chargeable event, e.g. RAT change, DNAI change or QoS change. Interim updates are also used when the IPv4 address and/or IPv6 prefix is allocated/released/re-allocated.

NOTE: DNAI change is only applicable when application relocation possible indicated in the AF traffic influenced PCC rule as described in clause 5.6.7 of TS 23.501 [2], align with the DNAI change in UP path management events as described in clause 4.3.6.3 of TS 23.502 [3]. Only the target DNAI is provided in the ACR message.

Editor's note: How to indicate the case that the source DNAI or target DNAI is not applicabe in the ACR message is FFS.

When the SMF receives a signalling request (i.e. Nsmf_PDUSession_UpdateSMContext) that indicates the occurrence of one of these chargeable events, the SMF may send an Accounting Request Interim-Update to the DN-AAA server to update the necessary information related to this QoS flow. It is not necessary for the SMF to wait for the RADIUS AccountingResponse message from the DN-AAA server before sending the response for the triggering signalling message (i.e. Namf_Communication_N1N2MessageTransfer). The SMF may delete the QoS flow if the AccountingResponse is not received from the DN-AAA server.

The SMF may also send interim updates at the expiry of an operator configured time limit.

Figure 11.2.2-1 is an example message flow to show the procedure of RADIUS accounting update, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

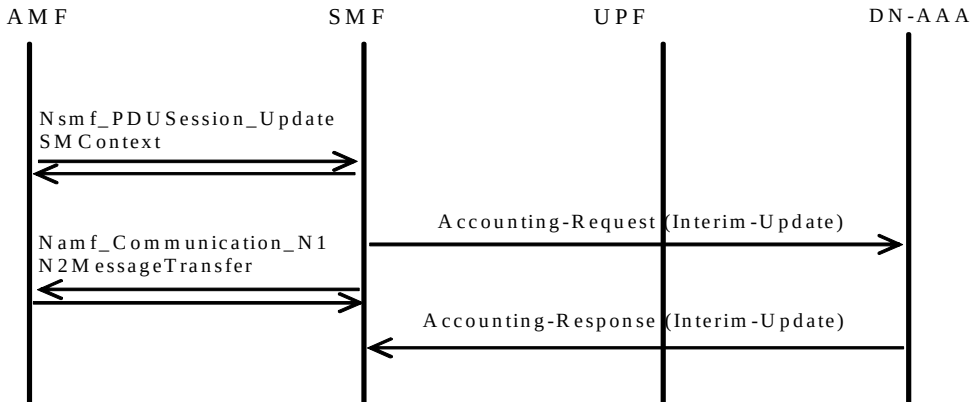

Figure 11.2.2-1: RADIUS accounting update

For the 5GC and EPC interworking scenario without authentication, authorization, re-authentication and/or re-authorization impacts, if the UE establishes the PDU session through the 5GC and initiates the accounting session, when the SMF+PGW-C determines that the UE has moved to the EPS (i.e. the SMF+PGW-C receives the modify bearer request or create session request from the S-GW), the SMF+PGW-C may perform the accounting session update with the following modifications:

- for the case that the accounting session is initiated per PDU session, the SMF+PGW-C may update the accounting session by including the identifier of the accounting session within the Acct-Session-Id, the "EUTRA" within the 3GPP-RAT-Type, the IPv4 address of S-GW within the 3GPP-SGSN-Address, the default EPS bearer id within the 3GPP-NSAPI, the user location in the EPC within the 3GPP-User-Location-Info if available and the new QoS profile within the 3GPP-GPRS-Negotiated-QoS-Profile if changed.

- for the case that the accounting session is initiated per QoS flow:

  - if the SMF+PGW-C mapped a QoS flow to an EPS bearer, the SMF may update the accounting session corresponding to the QoS flow with the information of the EPS bearer by including the identifier of the accounting session within the Acct-Session-Id, the "EUTRA" within the 3GPP-RAT-Type, the IPv4 address of S-GW within the 3GPP-SGSN-Address, the EPS bearer id within the 3GPP-NSAPI, the user location in the EPC within the 3GPP-User-Location-Info if available, the new QoS profile within the 3GPP-GPRS-Negotiated-QoS-Profile if changed, the new charging id within the 3GPP-Charging-Id if allocated and the new packet filters within the 3GPP-Packet-Filter if changed;

  - if the SMF+PGW-C mapped multiple QoS flows to one EPS bearer, the SMF shall select one of the accouting sessions corresponding to these QoS flows to update it as above and terminate the accounting session(s) corresponding to the other QoS flow(s).

  - if the SMF+PGW-C did not map a QoS flow to any EPS bearer, the SMF may decide to associate the corresponding account session to the default EPS bearer or terminate the corresponding accounting session.

11.2.3 DN-AAA initiated QoS flow termination

RADIUS is used as the protocol between the SMF and the DN-AAA server or proxy for applications (e.g. MMS) to deliver information related to user session. However some IP applications could need to interwork with the SMF to release the corresponding resource (e.g. terminate a particular QoS flow). For this purpose, the DN-AAA server or proxy may send a RADIUS Disconnect-Request to the SMF. On receipt of the Disconnect-Request from the DN-AAA server, the SMF shall release the corresponding resources and reply with a Disconnect-ACK. If the SMF is unable to release the corresponding resources, it shall reply to the DN-AAA server with a Disconnect-NAK. For more information on RADIUS Disconnect, see IETF RFC 5176 [27]. If the SMF deletes the corresponding QoS flow, it is not necessary for the SMF to wait for the response (i.e. Nsmf_PDUSession_UpdateSMContext) from the AMF before sending the RADIUS Disconnect-ACK to the DN-AAA server. The DN-AAA shall include the identification of the QoS flow to be disconnected within the Disconnect-Request. How to identify the QoS flow to be deleted is implementation specific.

NOTE: The QoS flow can be identified by the Acct-Session-Id which is extended to include QFI or by the Acct-Session-Id and 3GPP-NSAPI combination if provided by the SMF.

The Teardown-Indicator in the RADIUS Disconnect Request message indicates to the SMF that all QoS flows for this particular user and sharing the same user session shall be deleted. The QoS flows that belong to the same PDU session can be are identified by the Acct-Session-Id. The SMF is able to find out all the related QoS flows sharing the same user session once it has found the exact QoS flow from the Acct-Session-Id. If a user has the same user IP address for different sets of QoS flows towards different networks, only the QoS flows linked to the one identified by the Acct-Session-Id shall be deleted. If the value of Teardown-Indicator is set to "0" or if TI is missing, and if the Acct-Session-Id and 3GPP-NSAPI if provided identifies the QoS flow associated with the default QoS rule, the SMF shall tear down all the QoS flows that share the same user session identified by the Acct-Session-Id.

Figure 11.2.3-1 is an example message flow to show the procedure of DN-AAA initiated QoS flow termination, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

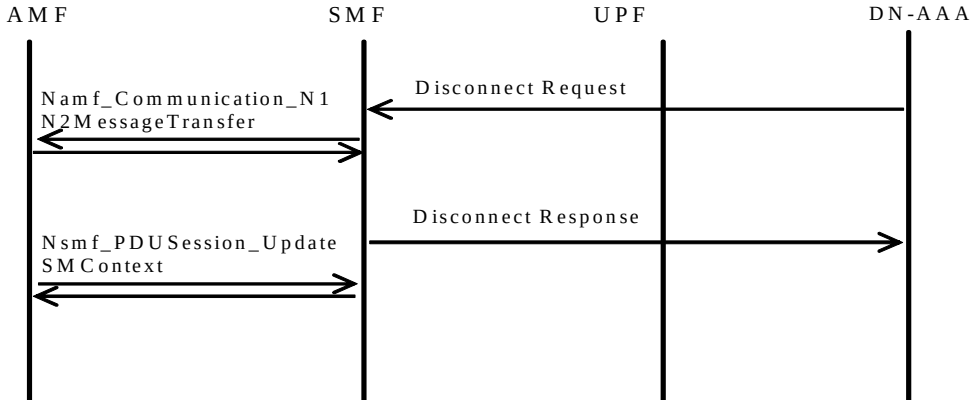

Figure 11.2.3-1: DN-AAA initiated QoS flow termination with RADIUS

For the 5GC and EPC interworking scenario, when the DN-AAA server initiates the QoS flow termination, the SMF+PGW-C shall send the delete bearer request to the S-GW as defined in subclause 5.4.4.1 of 3GPP TS 23.401 [53] to delete the EPS bearer corresponding to the accounting session if the UE has moved to the EPS.

11.2.4 DN-AAA initiated re-authorization

Some IP applications could need to interwork with the SMF to update the PDU session authorization attributes. For this purpose, the DN-AAA server or proxy may send a RADIUS CoA-Request to the SMF. On receipt of the CoA-Request from the DN-AAA server, if the service-type value of "Authorize Only" is not included, the SMF shall update the corresponding PDU session authorization attributes and reply with a CoA-ACK; otherwise it shall follow the procedure described in IETF RFC 5176 [27]. DN-AAA may also use CoA procedure to revoke the authorization of a PDU session, or to update the authorization data (e.g. allowed UE MAC addresses).

If the SMF updates/deletes the corresponding PDU session, it is not necessary for the SMF to wait for Nsmf_PDUSession_UpdateSMContext from the AMF before sending the RADIUS CoA-ACK to the DN-AAA server.

Figure 11.2.4-1 is an example message flow to show the procedure of DN-AAA initiated re-authorization, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

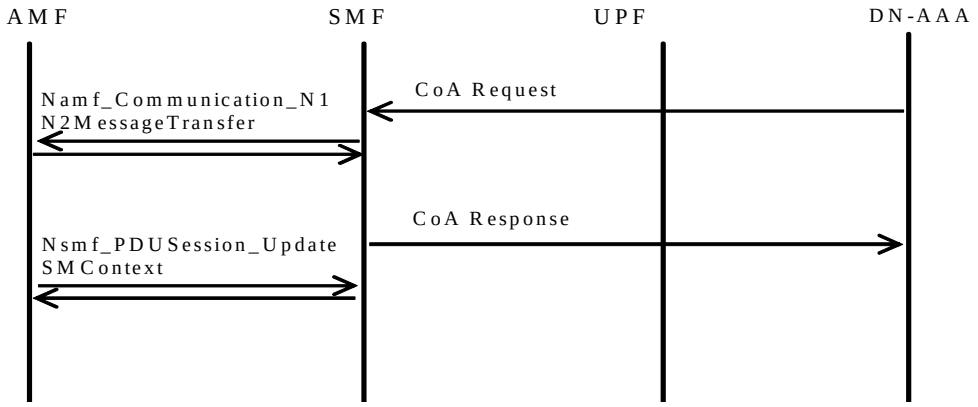

Figure 11.2.4-1: DN-AAA initiated re-authorization with RADIUS

NOTE: The DN-AAA initiated re-authorization procedure is not applicable for legacy DN-AAA supporting the RADIUS procedures over SGi interface as specified in 3GPP TS 29.061 [5].

11.3 List of RADIUS attributes

11.3.1 General

RADIUS attributes as defined in subclause 16.4 of 3GPP TS 29.061 [5] are re-used in 5G with the following differences:

- SMF or SMF+PGW-C replaces P-GW. GGSN and PPP PDP type related description are not applicable for 5G.
- 5G QoS flow replaces IP-CAN bearer and PDU session replaces IP-CAN session.
- N6 replaces Gi/Sgi and UE replaces MS.
- DNN replaces APN.
- Detailed information needed for 5G compared to 3GPP TS 29.061 [5] is described below.

Table 11.3-1: Additional information needed for 5G compared to the RADIUS attributes defined in 3GPP TS 29.061 [5]

Attr #	Attribute Name	Description	Content	Presence Requirement	Applicable message
79	EAP-Message	This attribute encapsulates EAP message (as defined in IETF RFC 3748 [6]) exchanged between the SMF and DN-AAA, see IETF RFC 3579 [7] for details.	String	Conditional NOTE	Access-Request, Access-Accept, Access-Reject, CoA-Request, CoA-ACK, Disconnect-Request, Disconnect-ACK
				Mandatory	Access-Challenge
80	Message-Authenticator	This attribute includes the message authenticator, see IETF RFC 3579 [7] for details.	String	Conditional NOTE	Access-Request, Access-Accept, Access-Reject, CoA-Request, CoA-ACK, CoA-NAK Disconnect-Request, Disconnect-ACK, Disconnect-NAK
				Mandatory	Access-Challenge
NOTE: Shall be present if EAP is used.					

Table 11.3-2: Different information needed for 5G compared to the RADIUS VSA defined in subclause 16.4.7 of 3GPP TS 29.061 [5]

Sub-attr #	Sub-attribute Name	Differences
1	3GPP-IMSI	Re-used.
2	3GPP-Charging-Id	Charging ID for this PDU Session.
3	3GPP-PDP-Type	Re-used. For SMF, this sub-attribute represents PDU session type and only the values "0", "2", "3", "5" and "6" are applicable.
4	3GPP-CG-Address	Re-used. IPv4 address of CHF.
5	3GPP-GPRS-Negotiated-QoS-Profile	Re-used. For SMF, it uses the format for Release indicator value "15" as defined in 3GPP TS 29.061 [5].
6	3GPP-SGSN-Address	Re-used. It includes AMF, I-SMF or V-SMF control plane IPv4 address.
7	3GPP-GGSN-Address	Re-used. It includes (home) SMF control plane IPv4 address providing the Nsmf_PDUSession service.
8	3GPP-IMSI-MCC-MNC	Re-used.
9	3GPP-GGSN-MCC-MNC	Re-used. MCC and MNC of the network the (home) SMF belongs to.
10	3GPP-NSAPI	Re-used. It identifies QFI with value range 0-255.
11	3GPP-Session-Stop-Indicator	Re-used.
12	3GPP-Selection-Mode	Re-used. SMF maps the selection mode value from the enumeration value of DnnSelectionMode in 3GPP TS 29.502 [40].
13	3GPP-Charging-Characteristics	Re-used.
14	3GPP-CG-IPv6-Address	Re-used. IPv6 address of CHF.
15	3GPP-SGSN-IPv6-Address	Re-used. It includes AMF, I-SMF or V-SMF control plane IPv6 address.
16	3GPP-GGSN-IPv6-Address	Re-used. It includes (home) SMF control plane IPv6 address providing the Nsmf_PDUSession service.
17	3GPP-IPv6-DNS-Servers	Re-used.
18	3GPP-SGSN-MCC-MNC	Re-used. MCC and MNC of the network the AMF belongs to
19	3GPP-Teardown-Indicator	Re-used.
20	3GPP-IMEISV	Re-used.
21	3GPP-RAT-Type	Re-used. For SMF, it uses the sub-attribute definition for P-GW and only the values "3", "6" - "9", and "51" - "58" are applicable.
22	3GPP-User-Location-Info	Re-used. For SMF, only the values "128", "129", "130", "135" and "136" of Geographic Location Type are applicable.
23	3GPP-MS-TimeZone	Re-used.
24	3GPP-CAMEL-Charging-Info	Not applicable.
25	3GPP-Packet-Filter	Re-used.
26	3GPP-Negotiated-DSCP	Re-used.
27	3GPP-Allocate-IP-Type	Re-used.
28	External-Identifier	Re-used.
29	TWAN-Identifier	Re-used by TWAP Identifier field, supporting ssid, bssid and/or civicAddress.
30	3GPP-User-Location-Info-Time	Re-used.
31	3GPP-Secondary-RAT-Usage	Re-used. For SMF, the RAT values "0", "1", "2" and "3" are applicable, and the SESS field is used to indicate secondary RAT usage of the PDU session.
32	3GPP-UE-Local-IP-Address	Re-used. Extended with TWAN applicability.
33	3GPP-UE-Source-Port	Re-used. Extended with TWAN applicability.
110	3GPP-Notification	Added.
111	3GPP-UE-MAC-Address	Added.
112	3GPP-Authorization-Reference	Added.
113	3GPP-Policy-Reference	Added. It is not used in this release.
114	3GPP-Session-AMBR	Added.
115	3GPP-NAI	Added.
116	3GPP-Session-AMBR-v2	Added.
117	3GPP-Supported-Features	Added.
118	3GPP-IP-Address-Pool-Info	Added.
119	3GPP-VLAN-Id	Added.
120	3GPP-TNAP-Identifier	Added.
121	3GPP-HFC-NodeId	Added.
122	3GPP-GLI	Added.
123	3GPP-Line-Type	Added.
124	3GPP-NID	Added.
125	3GPP-Session-S-NSSAI	Added.
126	3GPP-CHF-FQDN	Added. FQDN of CHF.
127	3GPP-Serving-NF-FQDN	Added. It includes AMF, I-SMF or V-SMF FQDN address.
128	3GPP-Session-Id	Added.

Sub-attr #	Sub-attribute Name	Differences
129	3GPP-GCI	Added.
130	3GPP-DNAI	Added.
131	3GPP-RSN	Added.
132	3GPP-Session-Pair-Id	Added.
NOTE: 5G specific RADIUS VSAs are numbered from 110.		

110 – 3GPP-Notification

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 110							
2	3GPP Length= 3							
3	Spare						ACC	AUTH

3GPP Type: 110

Length: 3

Octet 3 is Octet String type.

For bit 1 AUTH,

- if the value of AUTH is set to "1", and there is IPv4 address and/or IPv6 prefix change (not allocated/de-allocated by the DN-AAA itself) and the PDU session is not terminated, the SMF shall send Access-Request message to the DN-AAA with GPSI in Calling-Station-Id or External-Identifier attribute and IP address in:

  1) Framed-IP-Address and Framed-IPv6-Prefix, if both IPv4 address and IPv6 prefix(es) exist for the PDU session; or

  2) Framed-IP-Address, if only IPv4 address exists for the PDU session; or

  3) Framed-IPv6-Prefix, if only IPv6 prefix(es) exists for the PDU session.

  For Ethernet PDU session, if there is UE MAC address change, the SMF shall send Access-Request message to the DN-AAA with GPSI in Calling-Station-Id or External-Identifier attribute and the complete list of used UE MAC addresses in the 3GPP-UE-MAC-Address attribute.

- if the value is set to "0", the SMF may notify authentication DN-AAA with the UE address and GPSI based on local configuration.

For bit 2 ACC,

- if the value is set to "1", and there is IPv4 address and/or IPv6 prefix change (not allocated/de-allocated by the DN-AAA itself) and the PDU session is not terminated, the SMF shall send Accounting-Request Interim-Update message to the DN-AAA with GPSI in Calling-Station-Id or External-Identifier attribute and IP address in:

  1) Framed-IP-Address and Framed-IPv6-Prefix, if both IPv4 address and IPv6 prefix(es) exist for the PDU session; or

  2) Framed-IP-Address, if only IPv4 address exists for the PDU session; or

  3) Framed-IPv6-Prefix, if only IPv6 prefix(es) exists for the PDU session.

  For Ethernet PDU session, if there is UE MAC address change, the SMF shall send Accounting-Request Interim-Update message to the DN-AAA with GPSI in Calling-Station-Id or External-Identifier attribute and the complete list of used UE MAC addresses in the 3GPP-UE-MAC-Address attribute.

- if the value is set to "0", the SMF may notify accounting DN-AAA with the UE address and GPSI based on local configuration.

111 – 3GPP-UE-MAC-Address

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 111							
2	3GPP Length= 8							
3-8	MAC Address (octet string)							

3GPP Type: 111

Length: 8

It is sent from the DN-AAA to authorize UE MAC addresses. Multiple 3GPP- UE-MAC-Address sub-attributes (maximum 16) may be sent in one RADIUS CoA or Access-Accept message. The DN-AAA shall always provide the full list of allowed MAC addresses, and SMF shall replace the existing list with the newly received one. When omitted, there is no restriction and all UE MAC addresses are permitted for the Ethernet PDU session.

When sending from the SMF to the DN-AAA, it indicates UE MAC addresses in use. Multiple 3GPP- UE-MAC-Address sub-attributes may be sent in one RADIUS Access-Request or Accounting-Request Interim-Update message.

MAC address is Octet String type. The encoding is defined as MacAddr48 in 3GPP TS 29.571 [39] without dashes as delimiter, encoded as 12-digit hexadecimal numbers.

112 – 3GPP-Authorization-Reference

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 112							
2	3GPP Length= m							
3-m	Authorization Data Reference (octet string)							

3GPP Type: 112

Length: m

Authorization Data Reference: Octet String. It is sent from the DN-AAA to refer to the local authorization data in the SMF or PCF.

113 – 3GPP-Policy-Reference

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 113							
2	3GPP Length= m							
3-m	Policy Data Reference (octet string)							

3GPP Type: 113

Length: m

Policy Data Reference: Octet String. It is sent from the DN-AAA and used by the SMF to retrieve the SM or QoS policy data from the PCF. It is not used in this release.

114 – 3GPP-Session-AMBR

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 114							
2	3GPP Length= m							
3-m	Session AMBR (octet string)							

3GPP Type: 114

Length: m

Session AMBR: Octet String. It is sent from the DN-AAA to authorize the PDU Session AMBR in the downlink and uplink direction. The encoding is defined as BitRate in 3GPP TS 29.571 [39]. Same value is applied to downlink and uplink via this VSA.

115 – 3GPP-NAI

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 115							
2	3GPP Length= m							
3-m	NAI (octet string)							

3GPP Type: 115

Length: m

NAI: Octet String. It shall be formatted according to subclause 14.3 of 3GPP TS 23.003 [28] that describes an NAI.

116 – 3GPP-Session-AMBR-v2

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 116							
2	3GPP Length= m							
3	Spare						DL	UL
4-5	UL Session-AMBR length (octet string)							
6-m	UL Session-AMBR (octet string)							
(m+1)-(m+2)	DL Session-AMBR length (octet string)							
(m+3)-n	DL Session-AMBR (octet string)							

3GPP Type: 116

Length: m

Octet 3 is Octet String type.

Bit 1 UL and bit 2 DL indicate if the corresponding UL and DL Session-AMBR shall be present in a respective field or not. If one of these bits is set to "0", the corresponding field shall not be present at all.

UL/DL Session AMBR: Octet String. It is sent from the DN-AAA to authorize the PDU Session AMBR. The encoding is defined as BitRate in 3GPP TS 29.571 [39].

If the feature eSessionAMBR is supported and if applicable, the DN-AAA shall send this VSA; otherwise, the DN-AAA shall send the VSA 3GPP-Session-AMBR.

117 – 3GPP-Supported-Features

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 117							
2	3GPP Length= m							
3-6	Vendor ID (octet string)							
7-10	Feature List ID (octet string)							
11-14	Feature List (octet string)							

3GPP Type: 117

Length: m

This VSA may be present in the Access-Request (initial one) message and either the Access-Challenge (initial one) or the Access-Accept message. If present, this VSA informs the destination entity about the features that the origin entity requires to successfully complete the message exchange. The Vendor ID, Feature List ID and Feature List are encoded according to 3GPP TS 29.229 [41]. See clause 12.4.1 for more detailed information regarding the general principle of the feature negotiation with the difference that RADIUS terms replace Diameter terms. The table 12.4.1-1 defines the features applicable to the RADIUS N6 interfaces for the feature lists with a Feature-List-ID of 1.

118 – 3GPP-IP-Address-Pool-Info

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 118							
2	3GPP Length= m							
3	Spare							IP version
4-5	IP address pool id length (octet string)							
6-m	IP address pool id (octet string)							

3GPP Type: 118

Length: m

Octet 3 is Octet String type.

For bit 1 and bit 2 IP version:- if the value is set to "0", it indicates the IP address pool id is applicable for both IPv4 and IPv6;

- if the value is set to "1", it indicates the IP address pool id is applicable for IPv4;
- if the value is set to "2", it indicates the IP address pool id is applicable for IPv6; and
- value "3" is reserved.

The SMF may determine an IP address pool ID based on UPF ID, S-NSSAI, DNN, and IP version as described in subclause 5.8.2.2.1 in 3GPP TS 23.501 [2] and includes the IP address pool ID within 3GPP-IP-Address-Pool-Info and send it to the DN-AAA. The DN-AAA assigns IPv6 prefix or IPv4 address from the requested IP address pool. Multiple 3GPP-IP-Address-Pool-Info sub-attributes may be sent in the RADIUS Access-Request message. The DN-AAA shall include the selected IP address pool in the 3GPP-IP-Address-Pool-Info sub-attribute of the RADIUS Access-Accept message. For accounting, if Framed-IP-Address or Framed-IPv6-Prefix attribute is included in RADIUS Accounting-Request (START/Interim-Update/STOP), the SMF shall also include the 3GPP-IP-Address-Pool-Info sub-attribute.

119 – 3GPP-VLAN-Id

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 119							
2	3GPP Length= 4							
3	VID value				Spare			
4	VID value							

3GPP Type: 119

Length: 4

VLAN Id: Octet String. Octet 3/ Bit 1 to Bit 4 shall be zero, Octet 3 / Bit 8 shall be the most significant bit of the VLAN Id and Octet 4 / Bit 1 shall be the least significant bit.

It is sent from the DN-AAA to authorize the allowed VLAN Ids for the Ethernet PDU session. Multiple 3GPP-VLAN-Id sub-attributes (maximum 16) may be sent in one RADIUS CoA or Access-Accept message. The DN-AAA shall always provide the full list of allowed VLAN Ids, and SMF shall replace the existing list with the newly received one. When omitted, there is no restriction and all VLAN Ids are permitted for the Ethernet PDU session.

120 – 3GPP-TNAP-Identifier

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 120							
2	3GPP Length= m							
3-m	TNAP Identifier (octet string)							

3GPP Type: 120

Length=m, where m depends on the type of location that is present as described in 3GPP TS 29.274 [50].

TNAP Identifier field is used to convey the location information in a Trusted Non-3GPP Access Network. The coding of this field shall be the same as for the GTP TWAN Identifier starting with Octet 5, till Octet (q+r) +2 as per clause 8.100 in 3GPP TS 29.274 [50], with LAII flag, OPNAI flag and PLMNI flag in Octet 5 shall be set as zero.

TNAP Identifier field is Octet String type.

The SMF may indicate the UE location in a Trusted Non-3GPP Access Network, in Access-Request, Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages.

121 – 3GPP-HFC-NodeId

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 121							
2	3GPP Length= n							
3-n	HFCNodeId (octet string)							

3GPP Type: 121

Length: n≤6+2

HFCNodeId field is the identifier of the HFC node Id as specified in CableLabs WR-TR-5WWC-ARCH [51]. It is provisioned by the wireline operator as part of wireline operations and may contain up to six characters.

HFCNodeId field is Octet String type.

The SMF may indicate the HFC Node Identifier received over NGAP. Present for a 5G-CRG accessing the 5GC via wireline access network, in Access-Request, Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages. Present for a FN-CRG accessing the 5GC via wireline access network, in Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages.

122 – 3GPP-GLI

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 122							
2	3GPP Length= n							
3-n	GLI (octet string)							

3GPP Type: 122

Length: n≤150+2

GLI field is the Global Line Identifier uniquely identifying the line connecting the 5G-BRG or FN-BRG to the 5GS. See clause 28.16.3 of 3GPP TS 23.003 [28]. Shall be encoded as a string with format "byte", i.e. base64-encoded characters, representing the GLI value (up to 150 bytes) encoded as specified in BBF WT-470 [52].

GLI field is Octet String type.

The SMF may indicate the Global Line Identifier. Present for a 5G-BRG accessing the 5GC via wireline access network, in Access-Request, Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages. Present for a 5G-BRG accessing the 5GC via wireline access network, in Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages.

123 – 3GPP-Line-Type

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 123							
2	3GPP Length= 3							
3	Line-Type (octet string)							

3GPP Type: 123

The Line-Type sub-attribute may be present for a 5G-BRG/FN-BRG accessing the 5GC via wireline access network.

When present, it shall indicate the type of the wireline (DSL or PON).

Line-Type field is Octet String type. It shall be coded as follows:

0 (DSL):

This value shall be used to indicate DSL line.

1 (PON):

This value shall be used to indicate PON line.

The SMF may indicate the type of the wireline (DLS or PON). Present for a 5G-BRG accessing the 5GC via wireline access network, in Access-Request, Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages. Present for a FN-BRG accessing the 5GC via wireline access network, in Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages.

124 – 3GPP-NID

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 124							
2	3GPP Length= 13							
3-13	Network ID (octet string)							

3GPP Type: 124

Length: 13

The Network ID field is Octet String type. The encoding is defined as Nid in 3GPP TS 29.571 [39].

Table 11.3-3 describes the sub-attributes of the 3GPP Vendor-Specific attribute described above in different RADIUS messages.

125 – 3GPP-Session-S-NSSAI

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 125							
2	3GPP Length= m							
3	SST							
4-6	SD (octet string)							

3GPP Type: 125

Length: 3 or 6

SST: the Slice/Service Type with value range 0 to 255.

SD: 3-octet string, representing the Slice Differentiator, the encoding follows sd attribute specified in subclause 5.4.4.2 of 3GPP TS 29.571 [46]. Its presence depends on the Length field.

It is sent from the SMF to the DN-AAA server to indicate the S-NSSAI that is associated with the PDU Session.

126 – 3GPP-CHF-FQDN

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 126							
2	3GPP Length= m							
3-m	CHF FQDN							

3GPP Type: 126

Length: m

CHF FQDN: string, indicates the FQDN of the CHF.

It is sent from the SMF to the DN-AAA server to indicate the FQDN of the CHF.

127 – 3GPP-Serving-NF-FQDN

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 127							
2	3GPP Length= m							
3-m	Serving NF FQDN							

3GPP Type: 127

Length: m

Serving NF FQDN: string, indicates the FQDN of the Serving NF (including AMF, I-SMF or V-SMF).

It is sent from the SMF to the DN-AAA server to indicate the Serving NF FQDN address.

128 – 3GPP-Session-Id

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type = 128							
2	3GPP Length= 3							
3	PduSessionId							

3GPP Type: 128

Length: 3

PduSessionId: 1-octet unsigned integer identifying a PDU session, within the range 0 to 255, as specified in subclause 5.4.2 of 3GPP TS 29.571 [46].

It is sent from the SMF to the DN-AAA server to indicate the PDU Session Identifier.

129 – 3GPP-GCI

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type = 129							
2	3GPP Length= m							
3-m	GCI (octet string)							

3GPP Type: 129

Length: m

GCI field is Octet String type.

The GCI is the Global Cable Identifier uniquely identifies the line connecting the 5G-CRG or FN-CRG to the 5GS. See clause 28.15.4 of 3GPP TS 23.003 [28].

The GCI is a variable length opaque identifier, shall be encoded as specified in CableLabs WR-TR-5WWC-ARCH [51] and CableLabs DOCSIS MULPI [55]. It shall comply with the syntax specified in clause 2.2 of IETF RFC 7542 [56] for the username part of a NAI.

The SMF may indicate the Global Cable Identifier. Present for a 5G-CRG accessing the 5GC via wireline access network, in Access-Request, Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages. Present for a FN-CRG accessing the 5GC via wireline access network, in Accounting-Request START, Accounting-Request STOP, or Accounting-Request Interim-Update messages.

130 – 3GPP-DNAI

	Bits							
Octets	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**
1	3GPP type = 130							
2	3GPP Length= m							
3-m	DNAI (string)							

3GPP Type: 130

Length: m

DNAI: string, indicates the Data Network Access Identifier.

It is sent from SMF to DN-AAA server to indicate the SMF selected or used DNAI interworking with the external DN.

131 – 3GPP-RSN

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 1xx							
2	3GPP Length= 3							
3	RSN							

3GPP Type: 1xx

Length: 3

RSN: 1-octet unsigned integer identifying a RSN (see 3GPP TS 24.501 [42] for encoding).

It is sent from the SMF to the DN-AAA accounting server to indicate the RSN.

132 – 3GPP-Session-Pair-Id

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 1xy							
2	3GPP Length= 3							
3	PDU Session Pair Id							

3GPP Type: 1xy

Length: 3

PDU Session Pair Id: 1-octet unsigned integer identifying a PDU session pair information (see 3GPP TS 24.501 [42] for encoding).

It is sent from the SMF to the DN-AAA accounting server to indicate the PDU Session Pair Identifier. Two redundant PDU sessions share the same PDU Session Pair Identifier.

Table 11.3-3: List of the 3GPP Vendor-Specific sub-attributes for N6

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicability
110	3GPP-Notification	It includes all notifications that the DN-AAA wants to receive from the SMF.	Optional	Access-Accept	
111	3GPP-UE-MAC-Address	It is sent from the DN-AAA to authorize UE MAC addresses, or it indicates UE MAC addresses in use when sending from the SMF to the DN-AAA.	Optional	Access-Request, Access-Accept, Accounting-Request Interim-Update, Change-of-Authorization	
112	3GPP-Authorization-Reference	It is sent from the DN-AAA to refer to the local	Optional	Access-Accept, Change-of-Authorization	

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicability
		authorization data in the SMF.			
113	3GPP-Policy-Reference	It is sent from the DN-AAA and used by the SMF to retrieve the SM or QoS policy data from the PCF. It is not used in this release.	Optional	Access-Accept, Change-of-Authorization	
114	3GPP-Session-AMBR	It is sent from the DN-AAA to authorize the PDU Session AMBR in the downlink and uplink.	Optional	Access-Accept, Change-of-Authorization	
115	3GPP-NAI	The Network Access Identifier identifying the UE.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
116	3GPP-Session-AMBR-v2	It is sent from the DN-AAA to authorize the PDU Session AMBR, it includes separate session AMBR for UL and DL.	Optional	Access-Accept, Change-of-Authorization	eSession AMBR
117	3GPP-Supported-Features	It indicates the supported features as specified in clause 12.4.1.	Optional	Access-Request, Access-Accept, Access-Challenge, Accounting-Request START, Accounting-Response START	
118	3GPP-IP-Address-Pool-Info	It indicates the IP address pool identifier.	Optional	Access-Request, Access-Accept, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
119	3GPP-VLAN-Id	It is sent from the DN-AAA to authorize the allowed VLAN Id for the Ethernet PDU session.	Optional	Access-Accept, Change-of-Authorization	
120	3GPP-TNAP-Identifier	Indicates the UE location in a Trusted Non-3GPP Access Network.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
121	3GPP-HFC-NodeId	Indicates the HFC Node Identifier received over NGAP. Present for a 5G-CRG/FN-CRG accessing the 5GC via wireline access network	Optional	Access-Request (NOTE 1), Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
122	3GPP-GLI	Indicates the Global Line Identifier. Present for a 5G-BRG/FN-BRG	Optional	Access-Request (NOTE 1),	

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicability
		accessing the 5GC via wireline access network.		Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
123	3GPP-Line-Type	Indicates the type of the wireline (DLS or PON). Present for a 5G-BRG/FN-BRG accessing the 5GC via wireline access network.	Optional	Access-Request (NOTE 1), Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
124	3GPP-NID	Indicates the network identifier. It shall only be present together with 3GPP-SGSN-MCC-MNC to identify an SNPN.	Optional	Access-Request, Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
125	3GPP-Session-S-NSSAI	Indicates the S-NSSAI that is associated with the PDU Session.	Optional	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update (NOTE 2)	
126	3GPP-CHF-FQDN	Indicates the FQDN of the CHF.	Optional	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
127	3GPP-Serving NF-FQDN	Indicates the FQDN of the Serving NF (includes AMF, I-SMF or V-SMF).	Optional	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
128	3GPP-Session-Id	Indicates the PDU Session Identifier.	Optional	Access-Request Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update (NOTE 2)	
129	3GPP-GCI	Indicates the line connecting the 5G-CRG or FN-CRG to the 5GS	Optional	Access-Request (NOTE 1), Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
130	3GPP-DNAI	Indicates the SMF selected or used DN Access Identifier interworking with the external DN.	Optional	Accounting-Request START, Accounting-Request STOP,	

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicability
				Accounting-Request Interim-Update	
131	3GPP-RSN	Indicates the RSN.	Optional	Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
132	3GPP-Session-Pair-Id	Indicates the PDU Session Pair Identifier	Optional	Accounting-Request START, Accounting-Request STOP, Accounting-Request Interim-Update	
NOTE 1: Access-Request is not applicable for FN-CRG or FN-BRG. NOTE 2: This VSA is optional in the Accounting-Request Interim-Update message.					

RADIUS attributes related to the DN-AAA initiated re-authorization and authentication challenge are described in the following subclauses.

11.3.2 Change-of-Authorization Request (optionally sent from DN-AAA server to SMF)

Table 11.3.2-1 describes the attributes of the Change-of-Authorization Request message. Other RADIUS attributes may be used as defined in IETF RFC 5176 [27].

Table 11.3.2-1: The attributes of the Change-of-Authorization Request message

Attr #	Attribute Name	Description	Content	Presence Requirement
1	User-Name	Username provided by the user (extracted from the PCO field received during PDN connection establishment). If no username is available a generic username, configurable on a per DNN basis, shall be present. If the User-Name has been sent in the Access-Accept message, this user-name shall be used in preference to the above	String	Optional
6	Service-Type	Indicates the type of service for this user.	17 (Authorize Only)	Optional
8	Framed-IP-Address	User IPv4 address	Ipv4	Conditional NOTE 2
10	3GPP-NSAPI	identifies QFI with value range 0-255 in this user session.	UTF-8 encoded character	Optional
30	Called-Station-Id	Identifier for the target network	DNN (UTF-8 encoded characters)	Optional
31	Calling-Station-Id	This attribute is the identifier for the UE, and it shall be configurable on a per DNN basis.	MSISDN in international format according to 3GPP TS 23.003 [28], UTF-8 encoded decimal character. (NOTE 5)	Optional
96	Framed-Interface-Id	User IPv6 Interface Identifier	IPv6	Conditional NOTE 1 NOTE 2
44	Acct-Session-Id	User session identifier.	SMF IP address (IPv4 or IPv6) and Charging-ID concatenated in a UTF-8 encoded hexadecimal characters. (NOTE 6)	Mandatory
79	EAP-Message	This attribute encapsulates EAP message (as defined in IETF RFC 3748 [6]) exchanged between the SMF and DN-AAA, see IETF RFC 3579 [7] for details.	String	Conditional NOTE 3
80	Message-Authenticator	This attribute includes the message authenticator, see IETF RFC 3579 [7] for details.	String	Conditional NOTE 3
97	Framed-IPv6-Prefix	User IPv6 prefix	IPv6	Conditional NOTE 2
123	Delegated-IPv6-Prefix	Delegated IPv6 prefix to the user.	IPv6	Conditional NOTE 4
26/10415	3GPP Vendor-Specific	Sub-attributes according clause 11.3, the encoding of this attribute is specified in 3GPP TS 29.061 [5].	See clause 11.3	Optional

NOTE 1: Included if the prefix alone is not unique for the user. This may be the case, for example, if a static IPv6 address is assigned.
NOTE 2: If the 3GPP-PDP-Type is IPv4, IPv6 or IPv4v6, either IPv4 or IPv6 address/prefix attribute shall be present. The IP protocol version for end-user and network may be different.
NOTE 3: Shall be present if EAP is used.
NOTE 4: The delegated IPv6 prefix shall be present if IPv6 prefix delegation is required from the external DN-AAA server.
NOTE 5: There are no leading characters in front of the country code.
NOTE 6: If the accounting session is created per QoS flow, Acct-Session-Id may be extended to include the QFI of the QoS flow.

11.3.3 Access-Challenge (sent from DN-AAA server to SMF)

Table 11.3.3-1 describes the attributes of the Access-Challenge Request message. Other RADIUS attributes may be used as defined in IETF RFC 2865 [8].

Table 11.3.3-1: The attributes of the Access-Challenge message

Attr #	Attribute Name	Description	Content	Presence Requirement
27	Session-Timeout	Indicates the timeout value (in seconds) for the user session	32 bit unsigned Integer	Optional
79	EAP-Message	This attribute encapsulates EAP message (as defined in IETF RFC 3748 [6]) exchanged between the SMF and DN-AAA, see IETF RFC 3579 [7] for details.	String	Mandatory
80	Message-Authenticator	This attribute includes the message authenticator, see IETF RFC 3579 [7] for details.	String	Mandatory
NOTE: Included if the prefix alone is not unique for the user. This may be the case, for example, if a static IPv6 address is assigned.				

12 Interworking with DN-AAA (Diameter)

12.1 Diameter Procedures

12.1.1 Diameter Authentication and Authorization

The SMF also represents the H-SMF in the home routed scenario in this subclause unless specified otherwise.

Diameter Authentication and Authorization shall be used according to IETF RFC 7155 [23]. In 5G, multiple authentication methods using Extensible Authentication Protocol (EAP) may be used such as EAP-TLS (see IETF RFC 5216 [11]), EAP-TTLS (see IETF RFC 5281 [37]). The SMF shall support Diameter EAP application as specified in IETF RFC 4072 [25].

The SMF and the DN-AAA shall advertise the support of the Diameter NASREQ and EAP applications by including the value (1 and 5) of the application identifier in the Auth-Application-Id AVP (as specified in IETF RFC 4072 [25]) and the value of the 3GPP (10415) in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands as specified in IETF RFC 6733 [24], i.e. as part of the Vendor-Specific-Application-Id AVP.

The Diameter client function may reside in an SMF. When the SMF receives an initial access request (i.e. the SMF receives the Nsmf_PDUSession_CreateSMContext request with type "Initial request" for non-roaming case or local breakout case, or the H-SMF receives the Nsmf_PDUSession_Create Request with type "Initial request" for home routed case), the Diameter client function may send the authentication information to a DN-AAA server, which is identified during the DNN provisioning.

When the legacy applications require PAP/CHAP authentication with the UE accessing to the 5GS or to the 5GC and EPC interworking scenario and the legacy DN-AAA server does not support EAP, PAP/CHAP may be used as the authentication protocol, with the external network performing the risk assessment.

The DN-AAA server performs authentication and authorization. The response (when positive) may contain network information, such as an IPv4 address and/or IPv6 prefix for the user when the SMF is interworking with the DN-AAA server.

The information delivered during the Diameter authentication can be used to automatically correlate the user identity (e.g. SUPI) to the IPv4 address and/or IPv6 prefix, if applicable, assigned/confirmed by the SMF or the DN-AAA server respectively. The same procedure applies, in case of sending the authentication to a 'proxy' DN-AAA server.

For 5G, Diameter Authentication is applicable to the initial access request. When the SMF receives a positive response from the DN-AAA server it shall complete the initial access procedure. If Access-Reject or no response is received, the SMF shall reject the initial access procedure with a suitable cause code.

When DN-AAA server authorizes the PDU Session Establishment, it may send DN authorization data for the established PDU Session to the SMF. The DN authorization data for the established PDU Session may include one or more of the following:

- a reference to authorization data for policy and charging control locally configured in the SMF;
- a list of allowed MAC addresses (maximum 16) for the Ethernet PDU Session;
- a list of allowed VLAN Ids (maximum 16) for the Ethernet PDU Session;
- Session-AMBR for the PDU Session;
- L2TP information, such as LNS IP address and/or LNS host name; and
- Framed Route information for the PDU Session.

NOTE 1: If the DN-AAA server send L2TP information to SMF, the L2PT information can e.g. be provisioned per DNN/S-NSSAI or per SUPI or GPSI by configuration which is out of the scope of 3GPP specifications.

SMF policies may require DN authorization without DN authentication. In that case, when contacting the DN-AAA server for authorization, the SMF shall provide the GPSI of the UE if available.

The SMF may also use the Diameter re-authorization procedure for the purpose of IPv4 address and/or IPv6 prefix allocation to the UE. The use cases that may lead this procedure are:

- IPv4 address and/or IPv6 prefix allocation after UPF selection during PDU session establishment procedure.
- IPv6 prefix allocation during adding additional PDU Session Anchor procedure for IPv6 multi-homing.
- IPv4 address allocation via DHCPv4 procedure after successful PDU session establishment procedure.

The SMF may also trigger request for DN authentication/authorization and/or IP address/prefix allocation based on UE subscription data retrieve from the UDM as defined in subclause 5.2.2.2.5 of 3GPP TS 29.503.

When an IPv4 address and/or IPv6 prefix (including any additional IPv6 prefix of IPv6 multi-homing) is (re-)allocated or de-allocated (not causing the PDU session to be released) by using a method not via the DN-AAA server and if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the authentication session that was established before to inform the DN-AAA server by sending Diameter DER or AAR with the latest list of IPv4 address and/or IPv6 prefix(es).

When the SMF is notified by the UPF regarding the UE MAC address change (a new one is detected or a used one is inactive), if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the authentication session that was established before to inform the DN-AAA server by sending Diameter DER or AAR with the latest list of UE MAC addresses in use.

DN-AAA may initiate QoS flow termination, see details in clause 12.2.3. DN-AAA may initiate re-authorization and optional re-authentication, see details in clause 12.2.4 and 12.2.5.

For the 5GS interworking with EPS scenario, EAP based secondary authentication and re-authentication is not applicable to the PDN connection when the UE is in EPS in this release.

In case EAP based authentication and authorization has been performed for the PDU Session while the UE was in 5GS, and if SMF+PGW-C determines that the UE has moved to the EPS (i.e. the SMF+PGW-C receives the modify bearer request or create session request from the S-GW), the following applies:

- the SMF+PGW-C may initiate Diameter re-authorization procedure without re-authentication with the DN-AAA server based on local policy.
- DN-AAA initiated re-authorization without re-authentication may be performed.
- when the SMF+PGW-C receives a re-authentication request from the DN-AAA server, the SMF+PGW-C shall execute the procedure as described in clause 12.2.5.

NOTE 2: The DN-AAA server decided actions to take (e.g. to request another re-authorization without the association with EAP based re-authentication or release the session) are out of 3GPP scope.

12.1.2 Diameter Accounting

Diameter Accounting shall be used according to IETF RFC 7155 [23].

The SMF and the DN-AAA may advertise the support of the Diameter base accounting application by including the value (3) of the application identifier in the Acct-Application-Id AVP and the value of the 3GPP (10415) in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands as specified in IETF RFC 6733 [24], i.e. as part of the Vendor-Specific-Application-Id AVP.

The Diameter accounting client function may reside in an SMF. The Diameter accounting client may send information to a DN-AAA server, which is identified during the DNN provisioning. The DN-AAA server may store this information and use it to automatically identify the user. This information can be trusted because the 3GPP network has authenticated the subscriber (i.e. USIM card and possibly other authentication methods).

The SMF may use the Diameter Accounting messages during QoS flow (e.g. QoS flow associated with the default QoS rule) establishment and termination procedures, respectively.

If the DN-AAA server is used for IPv4 address and/or IPv6 prefix assignment, then, upon reception of a Diameter Accounting-Request STOP message for all QoS flows associated to a PDU session defined by DNN and SUPI or GPSI, the DN-AAA server may make the associated IPv4 address and/or IPv6 prefix available for assignment.

When an IPv4 address and/or IPv6 prefix (including any additional IPv6 prefix of IPv6 multi-homing) is (re-)allocated or de-allocated (not causing the PDU session to be released) by using a method not via the DN-AAA server and if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the accounting session that was established before to inform the DN-AAA server by sending Diameter Accounting-Request Interim-Update with the latest list of IPv4 address and/or IPv6 prefix(es).

When the SMF is notified by the UPF regarding the UE MAC address change (a new one is detected or a used one is inactive), if the SMF was required by the DN-AAA server to report such change during authentication procedure or by local configuration, the SMF shall, if applicable, use the accounting session that was established before to inform the DN-AAA server by sending Diameter Accounting-Request Interim-Update with the latest list of UE MAC addresses in use.

12.2 Message flows on N6 interface

12.2.1 Authentication, Authorization and Accounting procedures

The SMF also represents the H-SMF in the home routed scenario in this subclause unless specified otherwise.

When an SMF receives an initial access request (i.e. the SMF receives the Nsmf_PDUSession_CreateSMContext request with type "Initial request" for non-roaming case or local breakout case, or the H-SMF receives the Nsmf_PDUSession_Create Request with type "Initial request" for home routed case) message for a given DNN, the SMF may (depending on the configuration for this DNN) send a Diameter DER message to a DN-AAA server. The SMF may also (depending on the configuration for this DNN) send the S-NSSAI and the PDU Session ID that are associated with the PDU Session, respectively in the 3GPP-Session-S-NSSAI AVP and the 3GPP-Session-Id AVP, to a DN-AAA server. Upon receipt of the DER message, the DN-AAA server shall respond with an DEA message. Multi-round authentication using the DEA and DER messages may be used. The DN-AAA server finally authenticates and authorizes the user by replying with the DEA message. If the DN-AAA server is also responsible for IPv4 address and/or IPv6 prefix allocation, the DN-AAA server shall return the allocated IPv4 address and/or IPv6 prefix in the DEA message.

For re-authentication and re-authorization, the SMF shall send a DER message to the DN-AAA server and the DN-AAA server shall respond with a DEA message. Multi-round authentication using the DEA and DER messages may be used. The DN-AAA server finally authenticates and authorizes the user by replying with the DEA message.

The SMF may initiate Diameter re-authorization procedures for the purpose of IPv4 address and/or IPv6 prefix allocation (or renew the lease). In this case, the SMF shall set the Session-Id to the value used in the initial request, the Auth-Request-Type AVP to "AUTHORIZE_ONLY" and the 3GPP-Allocate-IP-Type AVP to the type of IP address to be allocated in the AA-Request message sent to the AAA server. If the SMF is using DHCP signalling towards the UE and the DN-AAA server includes the Session-Timeout attribute in the Access-Accept, the SMF may use the Session-Timeout value as the DHCP lease time. The SMF shall not set the DHCPv4 lease time value higher than the Session-

Timeout value. The SMF may renew the DHCP lease to the UE without re-authorization towards the DN-AAA server providing that the new lease expiry is no later than the Session-Timeout timer expiry. If the SMF wishes to extend the lease time beyond the current Session-Timeout expiry, it shall initiate a new AAA re-authorization.

Even if the SMF was not involved in user authentication, it may send a Diameter Accounting-Request (START) message to a DN-AAA server. If no Diameter session is already open for the same PDU session a Diameter session needs to be activated, otherwise the existing Diameter session is used to send the Accounting-Request (START). If accounting is used per QoS flow, the QFI will identify the particular bearer this accounting message refers to. This message contains parameters, e.g. the tuple which includes the user ID and IPv4 address and/or IPv6 prefix, to be used by application servers (e.g. WAP gateway) in order to identify the user. This message may also (depending on the configuration for the DNN) contains the S-NSSAI and the PDU Session ID that are associated with the PDU Session, respectively in the 3GPP-Session-S-NSSAI AVP and the 3GPP-Session-Id AVP, and/or AF traffic influence PCC rule provisioned and then SMF used DNAI in the 3GPP-DNAI AVP, to a DN-AAA server. This message also indicates to the DN-AAA server that the user session has started.

If some external applications require Diameter Accounting-Request (START) information before they can process user packets, then the selected DNN (SMF) may be configured in such a way that the SMF drops user data until an Accounting-Answer (START) indicating success is received from the DN-AAA server. The SMF may wait for the Accounting-Answer (START) before sending the final authentication response message in Namf_Communication_N1N2MessageTransfer service operation. The SMF may reject the initial access request if the Accounting-Answer (START) is not received. The authentication and accounting servers may be separately configured for each DNN.

For IPv4 PDU type, if IPv4 address is allocated via DHCPv4 signalling between the UE and the DN-AAA after PDU session establishment, the SMF may wait to send the Accounting-Request START message until the UE receives its IPv4 address in a DHCPACK.

When the SMF receives a message indicating a QoS flow or PDU session release request and providing a Diameter Accounting-Request START message was sent previously, the SMF shall send a Diameter Accounting-Request (STOP) message to the DN-AAA server, which indicates the termination of this particular QoS flow or PDU session. The SMF shall immediately send the corresponding response (e.g. Nsmf_PDUSession_UpdateSMContext response) to the AMF, without waiting for an Accounting-Answer (STOP) message from the DN-AAA server.

If the last QoS flow of a PDU session is deactivated, the SMF shall additionally send an STR message to the DN-AAA server. The DN-AAA server shall reply with an STA message and shall deallocate the IPv4 address and/or IPv6 prefix initially allocated to the subscriber.

The following figure 12.2.1-1 is an example message flow to show the procedure of Diameter Authentication and Accounting between an SMF and a DN-AAA server:

1. UE initiates the PDU Session Establishment procedure, including authentication/authorization information.

2. The AMF sends Nsmf_PDUSession_CreateSMContext Request including the authentication/authorization information to the SMF and the SMF responds to the service operation.

   According to the configuration in the SMF, step 6 to step 9 are executed before step 3 if the SMF needs to send an EAP-Request message to the UE.

   In the case of home routed, the AMF sends Nsmf_PDUSession_CreateSMContext Request including the authentication/authorization information to the V-SMF and the V-SMF sends Nsmf_PDUSession_Create Request including the authentication/authorization information to the H-SMF.

3. If the N4 session has not been established before, the SMF triggers the N4 Session Establishment procedure to the UPF.

   In the case of home routed, the V-SMF triggers the N4 Session Establishment procedure to the V-UPF and the H-SMF triggers the N4 Session Establishment procedure to the H-UPF.

4. The SMF sends the DER message to the DN-AAA via the UPF, the message is forwarded from the SMF to the DN-AAA by the UPF in N4 user plane message.

   In the case of home routed, the H-SMF sends the Access-Request message to the DN-AAA via the H-UPF, the message is forwarded from the H-SMF to the DN-AAA by the H-UPF in N4 user plane message.

5-10. The DN-AAA responds with the DEA message to the SMF via the UPF, the message is forwarded from the DN-AAA to the SMF by the UPF in N4 user plane message. The authentication/authorization information is further transferred to UE via Namf_Communication_N1N2MessageTransfer service and NAS SM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message and Nsmf_PDUSession_UpdateSMContext service, then finally sent to the DN-AAA by the SMF, via the UPF, in the DER message.

In the case of home routed, the DN-AAA responds with the Access-Challenge message to the H-SMF via the H-UPF, the message is forwarded from the DN-AAA to the H-SMF by the H-UPF in N4 user plane message. The authentication/authorization information is transferred to V-SMF via Nsmf_PDUSession_Update service and is further transferred to UE via Namf_Communication_N1N2MessageTransfer service and NAS SM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS SM Transport message, Nsmf_PDUSession_UpdateSMContext service and Nsmf_PDUSession_Update servic, then finally sent to the DN-AAA by the H-SMF, via the H-UPF, in the Access-Request message.

NOTE: Step 5 to step 10 can be repeated depending on the authentication/authorization mechanism used (e.g. EAP-TLS).

11. The SMF receives final result of authentication/authorization from the DN-AAA in the DEA message, via the UPF.

12. The SMF requests to start accounting by sending the Accounting-Request (START) message to the DN-AAA via the UPF.

13. The SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information in Namf_Communication_N1N2MessageTransfer service.

In the case of home routed, the H-SMF proceeds with the PDU session establishment procedure and includes the authentication/authorization information is transferred to V-SMF via Nsmf_PDUSession_Update service and is further transferred to the AMF via Namf_Communication_N1N2MessageTransfer service.

14. The DN-AAA responds with the Accounting-Response (START) message. The SMF may wait for the Accounting-Response (START) before sending the Namf_Communication_N1N2MessageTransfer request in step 13.

In the case of home routed, the H-SMF may wait for the Accounting-Response (START) before sending the Nsmf_PDUSession_Update service in step 13.

15. The AMF sends the NAS PDU Session Establishment Request with the authentication/authorization information to the UE.

16. The UE sends a NAS message Deregistration Request to the AMF.

17. The AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the SMF and the SMF responds to the service operation.

In the case of home routed, the AMF sends Nsmf_PDUSession_ReleaseSMContext Request to the V-SMF and the V-SMF sends the Nsmf_PDUSession_Release Request to the H-SMF.

18-19. The SMF requests to stop accounting by sending the Accounting-Request (STOP) message to the DN-AAA via the UPF and the DN-AAA responds with the Accounting-Response (STOP) message.

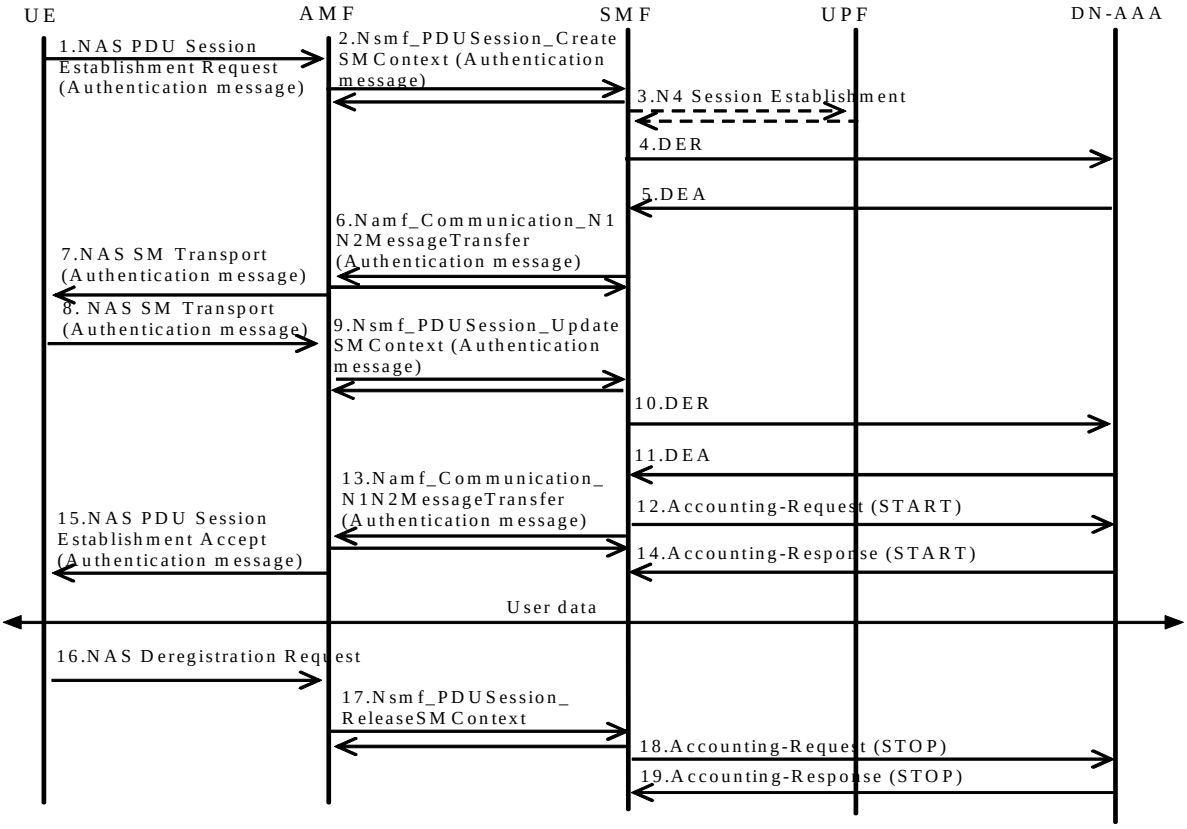

Figure 12.2.1-1: Diameter Authentication and Accounting example (successful case)

When PAP/CHAP is used as the authentication protocol with the external DN-AAA server which does not support EAP for the 5GS or for the 5GC and EPC interworking scenarios, the Diameter Authentication procedures refer to the non transparent access procedures in subclause 11.2.1 and related Diameter Authentication descriptions in subclause 16a.3a.1 in 3GPP TS 29.061 [5] are reused with the following differences:

- the SMF SMF+PGW-C performs the actions specified for the P-GW;
- the external DN-AAA server performs the actions specified for AAA;
- PDU Session Establishment request is sent from the UE to the SMF or SMF+PGW-C instead of or the Activate PDN connection request being sent from the UE to the S-GW and the Create Session request being sent from S-GW to P-GW;
- PDU Session Establishment accept is sent from the SMF or SMF+PGW-C to the UE instead of the Create Session Response message being sent from the P-GW to S-GW and the Activate PDN Connection Accept being sent from S-GW to the UE; and
- PDU Session Establishment reject is sent from the SMF or SMF+PGW-C to the UE instead of the Create Session Response message being sent from the P-GW to the S-GW and the Activate PDN Connection Reject being sent from S-GW to the UE.

12.2.2 Accounting Update

During the life of a QoS flow some information related to this QoS flow may change. The SMF may send an Accounting Request (Interim) to the DN-AAA server upon occurrence of a chargeable event, e.g. RAT change, DNAI change or QoS change. Interim updates are also used when the IPv4 address and/or IPv6 prefix is allocated/released/re-allocated.

NOTE: DNAI change is only applicable when application relocation possible indicated in the AF traffic influenced PCC rule as described in clause 5.6.7 of TS 23.501 [2], align with the DNAI change in UP path management events as described in clause 4.3.6.3 of TS 23.502 [3]. Only the target DNAI is provided in the ACR message.

Editor's note: How to indicate the case that the source DNAI or target DNAI is not applicabe in the ACR message is FFS.

When the SMF receives a signalling request (i.e. Nsmf_PDUSession_UpdateSMContext) that indicates the occurrence of one of these chargeable events, the SMF may send an Accounting Request Interim-Update to the DN-AAA server to update the necessary information related to this QoS flow. It is not necessary for the SMF to wait for the Diameter Accounting Answer message from the DN-AAA server before sending the response for the triggering signalling message (i.e. Namf_Communication_N1N2MessageTransfer). The SMF may delete the QoS flow if the Accounting Answer is not received from the DN-AAA server.

The SMF may also send interim updates at the expiry of an operator configured time limit.

Figure 12.2.2-1 is an example message flow to show the procedure of Diameter accounting update, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

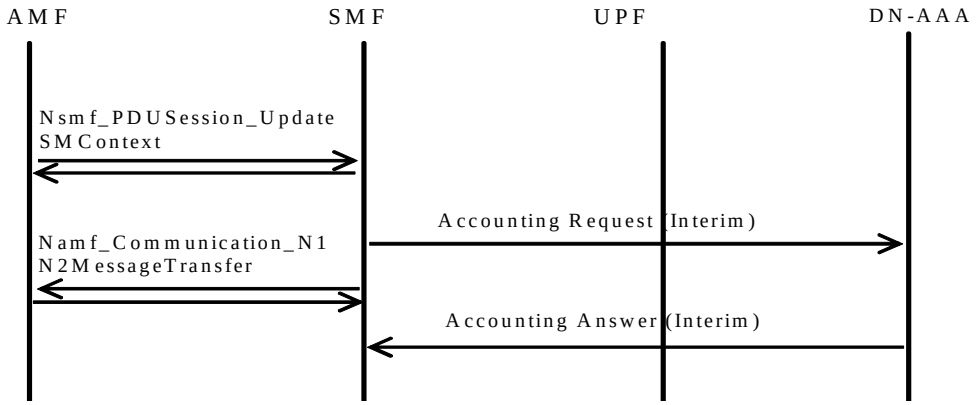

Figure 12.2.2-1: Diameter accounting update

For the 5GC and EPC interworking scenario without authentication, authorization, re-authentication and/or re-authorization impacts, if the UE establishes the PDU session through the 5GC and initiates the accounting session, when the SMF+PGW-C determines that the UE has moved to the EPS (i.e. the SMF+PGW-C receives the modify bearer request or create session request from the S-GW), the SMF+PGW-C may perform the accounting session update with the following modifications:

- for the case that the accounting session is initiated per PDU session, the SMF+PGW-C may update the accounting session by including the identifier of the accounting session within the Session-Id AVP, the "EUTRA" within the 3GPP-RAT-Type AVP, the IPv4 address of S-GW within the 3GPP-SGSN-Address AVP or IPv6 address of S-GW within the 3GPP-SGSN-IPv6-Address AVP, the default EPS bearer id within the 3GPP-NSAPI AVP, the user location in the EPC within the 3GPP-User-Location-Info AVP if available and the new QoS profile within the 3GPP-GPRS-Negotiated-QoS-Profile AVP if changed.

- for the case that the accounting session is initiated per QoS flow:

  - if the SMF+PGW-C mapped a QoS flow to an EPS bearer, the SMF may update the accounting session corresponding to the QoS flow with the information of the EPS bearer by including the identifier of the accounting session within the Session-Id AVP, the "EUTRA" within the 3GPP-RAT-Type AVP, the IPv4 address of S-GW within the 3GPP-SGSN-Address AVP or IPv6 address of S-GW within the 3GPP-SGSN-IPv6-Address AVP, the default EPS bearer id within the 3GPP-NSAPI AVP, the user location in the EPC within the 3GPP-User-Location-Info AVP if available and the new QoS profile within the 3GPP-GPRS-Negotiated-QoS-Profile AVP if changed, the new charging id within the 3GPP-Charging-Id AVP if allocated and the new packet filters within the 3GPP-Packet-Filter AVP if changed;

  - if the SMF+PGW-C mapped multiple QoS flows to one EPS bearer, the SMF shall select one of the accounting sessions corresponding to these QoS flows to update it as above and terminate the accounting session(s) corresponding to the other QoS flow(s).

  - if the SMF+PGW-C did not map a QoS flow to any EPS bearer, the SMF may decide to associate the corresponding account session to the default EPS bearer or terminate the corresponding accounting session.

12.2.3 DN-AAA initiated QoS flow termination

Diameter is used as the protocol between the SMF and the DN-AAA server or proxy for applications (e.g. MMS) to deliver information related to user session. However some IP applications could need to interwork with the SMF to release the corresponding resource (e.g. terminate a particular QoS flow). For this purpose, the DN-AAA server or proxy may send a Diameter ASR along with the QoS flow Identifier in 3GPP-NSAPI, if available, to identify the particular QoS flow to be terminated to the SMF. The SMF should react by deleting the corresponding QoS flow and reply with ASA. If the SMF deletes the corresponding QoS flow, it is not necessary for the SMF to wait for the response (i.e. Nsmf_PDUSession_UpdateSMContext) from the AMF before sending the ASA to the DN-AAA server.

The absence of the QoS flow Identifier in the Diameter ASR message indicates to the SMF that all QoS flows for this particular user and sharing the same user session shall be deleted. The QoS flows belonging to the same PDU session are identified by the Diameter Session-Id. If a user has the same user IP address for different sets of QoS flows towards different networks, only the QoS flows linked to the one identified by the Diameter Session-Id shall be deleted.

Figure 12.2.3-1 is an example message flow to show the procedure of DN-AAA initiated QoS flow termination, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

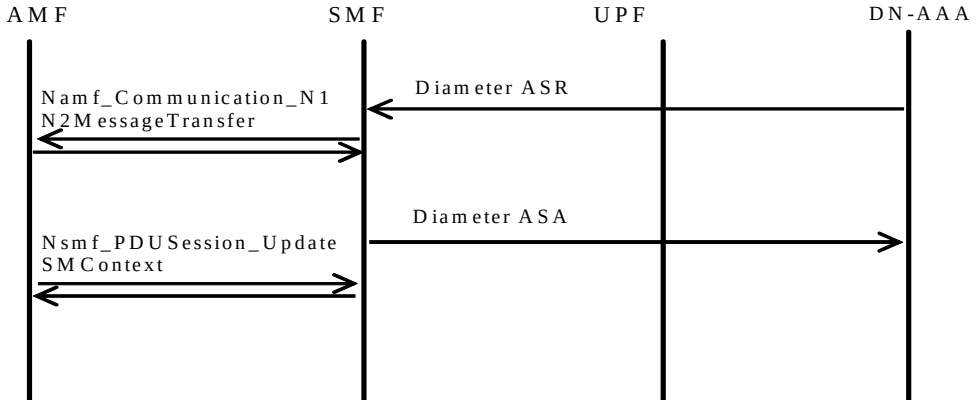

Figure 12.2.3-1: DN-AAA initiated QoS flow termination with Diameter

For the 5GC and EPC interworking scenario, when the DN-AAA initiates the QoS flow termination, the SMF+PGW-C shall send the delete bearer request to the S-GW as defined in subclause 5.4.4.1 of 3GPP TS 23.401 [53] to delete the EPS bearer corresponding to the if the UE has moved to the EPS.

12.2.4 DN-AAA initiated re-authorization

Some IP applications could need to interwork with the SMF to update the PDU session authorization attributes. For this purpose, the DN-AAA server or proxy may send a Diameter RAR with Re-Auth-Request-Type value "AUTHORIZE_ONLY" to the SMF. On receipt of the RAR from the DN-AAA server, the SMF shall update the corresponding PDU session authorization attributes and reply with RAA. DN-AAA may also use such procedure to revoke the authorization of a PDU session, or to update the authorization data (e.g. allowed UE MAC addresses).

If the SMF updates/deletes the corresponding PDU session, it is not necessary for the SMF to wait for Nsmf_PDUSession_UpdateSMContext from the AMF before sending the RAA to the DN-AAA server.

Figure 12.2.4-1 is an example message flow to show the procedure of DN-AAA initiated re-authorization, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

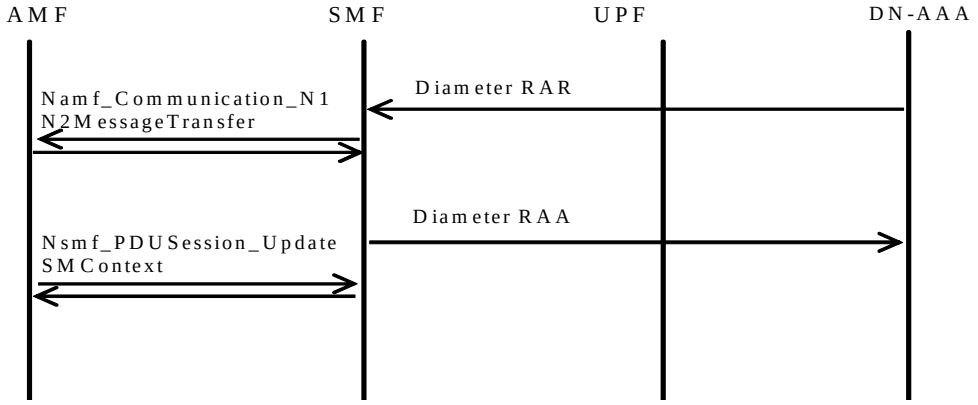

Figure 12.2.4-1: DN-AAA initiated re-authorization with Diameter

NOTE: The DN-AAA initiated re-authorization procedure is not applicable for legacy DN-AAA supporting the Diameter procedures over SGi interface as specified in 3GPP TS 29.061 [5].

12.2.5 DN-AAA initiated re-authentication and re-authorization

Some IP applications could need to interwork with the SMF to request re-authentication and re-authorization for the PDU session. For this purpose, the DN-AAA server or proxy may send a Diameter RAR with Re-Auth-Request-Type value "AUTHORIZE_AUTHENTICATE" to the SMF. The RAR should not include any authorization attribute.

NOTE: Since the SMF will initiate authentication procedure upon receipt of the RAR and in the end the DN-AAA will authorize the session, the DN-AAA does not have to apply authorization change immediately.

On receipt of the RAR from the DN-AAA server, the SMF shall reply with RAA and start authentication and authorization procedure as described in figure 12.2.1-1, from step 4 to step 11, step 13 and with PDU SESSION AUTHENTICATION RESULT message (successful case) sent from the AMF to the UE. The Auth-Request-Type in the DER is set to "AUTHORIZE_AUTHENTICATE".

Figure 12.2.5-1 is an example message flow to show the procedure of DN-AAA initiated re-authentication and re-authorization, messages between the SMF and DN-AAA are forwarded by the UPF in N4 user plane message.

When the SMF+PGW-C receives a re-authentication request from the DN-AAA server, the SMF+PGW-C shall inform the DN-AAA server that the re-authentication is not supported with error code 3002 and optionaly the "EUTRA" within the 3GPP-RAT-Type to indicated the UE is in EPS not available for re-authentication. The SMF+PGW-C should not initiate PDN connection release.

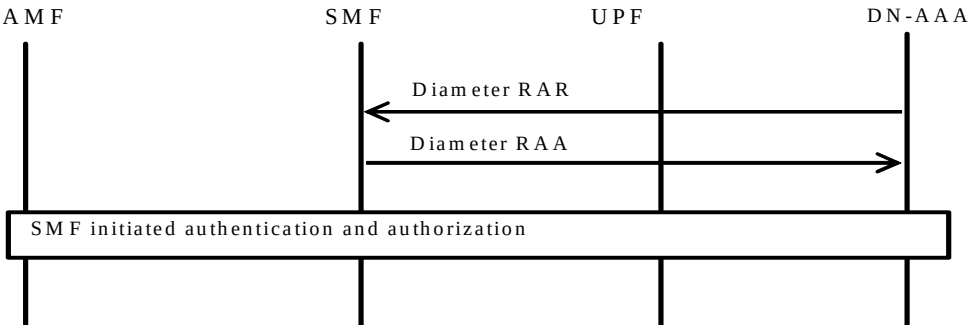

Figure 12.2.5-1: DN-AAA initiated re-authentication and re-authorization with Diameter

When PAP/CHAP is used as the authentication protocol with the external DN-AAA server which does not support EAP, the Diameter DN-AAA initiated re-authentication and re-authorization procedures are not applicable.

12.3 N6 specific AVPs

There is no specific AVP defined in the present release.

12.4 N6 re-used AVPs

12.4.0 General

Table 12.4-1 lists the Diameter AVPs re-used by the N6 reference point from existing Diameter Applications, reference to the respective specifications and a short description of the usage within the N6 reference point.

Table 12.4-1: N6 re-used Diameter AVPs

Attribute Name	AVP Code	Section defined	Value Type (NOTE 2)	AVP Flag rules (NOTE 1)				May Encr.	Applicability
				Must	May	Should not	Must not		
3GPP-IMSI	1	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-Charging-Id	2	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-PDP-Type	3	3GPP TS 29.061 [5] (NOTE 3)	Enumerated	V	P		M	Y	
3GPP-CG-Address	4	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-GPRS-Negotiated-QoS-Profile	5	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-SGSN-Address	6	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-GGSN-Address	7	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-IMSI-MCC-MNC	8	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-GGSN-MCC-MNC	9	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-NSAPI	10	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-Selection-Mode	12	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-Charging-Characteristics	13	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-CG-IPv6-Address	14	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-SGSN-IPv6-Address	15	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-GGSN-IPv6-Address	16	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-IPv6-DNS-Servers	17	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-SGSN-MCC-MNC	18	3GPP TS 29.061 [5] (NOTE 3)	UTF8String	V	P		M	Y	
3GPP-IMEISV	20	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-RAT-Type	21	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-User-Location-Info	22	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-MS-TimeZone	23	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-Packet-Filter	25	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-Negotiated-DSCP	26	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-Allocate-IP-Type	27	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
External-Identifier	28	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
TWAN-Identifier	29	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-User-Location-Info-Time	30	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-Secondary-RAT-Usage	31	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-UE-Local-IP-Address	32	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-UE-Source-Port	33	3GPP TS 29.061 [5] (NOTE 3)	OctetString	V	P		M	Y	
3GPP-Notification	110	11.3.1	OctetString	V	P		M	Y	

3GPP-UE-MAC-Address	111	11.3.1	OctetString	V	P		M	Y	
3GPP-Authorization-Reference	112	11.3.1	OctetString	V	P		M	Y	
3GPP-Policy-Reference	113	11.3.1	OctetString	V	P		M	Y	NOTE 4
3GPP-Session-AMBR	114	11.3.1	OctetString	V	P		M	Y	
3GPP-NAI	115	11.3.1	OctetString	V	P		M	Y	
3GPP-Session-AMBR-v2	116	11.3.1	OctetString	V	P		M	Y	eSessionAMBR
3GPP-IP-Address-Pool-Info	118	11.3.1	OctetString	V	P		M	Y	
3GPP-VLAN-Id	119	11.3.1	OctetString	V	P		M	Y	
3GPP-TNAP-Identifier	120	11.3.1	OctetString	V	P		M	Y	
3GPP-HFC-NodeId	121	11.3.1	OctetString	V	P		M	Y	
3GPP-GLI	122	11.3.1	OctetString	V	P		M	Y	
3GPP-Line-Type	123	11.3.1	OctetString	V	P		M	Y	
3GPP-NID	124	11.3.1	OctetString	V	P		M	Y	
3GPP-Session-S-NSSAI	125	11.3.1	OctetString	V	P		M	Y	
3GPP-CHF-FQDN	126	11.3.1	OctetString	V	P		M	Y	
3GPP-Serving-NF-FQDN	127	11.3.1	OctetString	V	P		M	Y	
3GPP-Session-Id	128	11.3.1	OctetString	V	P		M	Y	
3GPP-GCI	129	11.3.1	OctetString	V	P		M	Y	
3GPP-DNAI	130	11.3.1	OctetString	V	P		M	Y	
3GPP-RSN	1xx	11.3.1	OctetString	V	P		M	Y	
3GPP-Session-Pair-Id	1xy	11.3.1	OctetString	V	P		M	Y	
Supported-Features	628	3GPP TS 29.229 [41]	Grouped	V	M			N	

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 6733 [24].
NOTE 2: The value types are defined in IETF RFC 6733 [24].
NOTE 3: The use of Radius VSA as a Diameter vendor AVP is described in Diameter NASREQ (IETF RFC 7155 [23]) and the P flag may be set.
NOTE 4: It is not used in this release.

NOTE 1: Attribute 3GPP-CAMEL-Charging-Info (24) is not applicable for 5G in the present specification.

NOTE 2: Table 11.3-2 lists the differences between the RADIUS VSAs used in 5G and the VSAs defined in subclause 16.4.7 of 3GPP TS 29.061 [5].

12.4.1 Use of the Supported-Features AVP on the N6 reference point

The Supported-Features AVP is used during session establishment to inform the destination host about the required and optional features that the origin host supports. The client shall, in the first request in a Diameter session indicate the set of supported features. The server shall, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server shall support within the same Diameter session. Any further command messages shall always be compliant with the list of supported features indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported shall not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP on the N6 reference point shall be compliant with the requirements for dynamic discovery of supported features and associated error handling on the Cx reference point as defined in clause 7.2.1 of 3GPP TS 29.229 [41].

The base functionality for the N6 reference point is the 3GPP Rel-15 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent from the N6 commands. As defined in clause 7.1.1 of 3GPP TS 29.229 [41], when extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [41], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. On the N6 reference point, the Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined for the N6 reference point, the Feature-List-ID AVP shall differentiate those lists from one another.

On receiving an initial request application message, the destination host shall act as defined in clause 7.2.1 of 3GPP TS 29.229 [41].

Once the SMF and DN-AAA have negotiated the set of supported features during session establishment, the set of common features shall be used during the lifetime of the Diameter session.

The table below defines the features applicable to the N6 interfaces for the feature lists with a Feature-List-ID of 1.

Table 12.4.1-1: Features of Feature-List-ID 1 used in N6

Feature bit	Feature	M/O	Description
0	eSessionAMBR	M	This feature indicates the support of enhanced Session AMBR function. If supported, the DN-AAA authorizes DL and/or UL Session AMBR separately.
Feature bit: The order number of the bit within the Feature-List AVP where the least significant bit is assigned number "0". Feature: A short name that can be used to refer to the bit and to the feature, e.g. "5GC". M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O") in this 3GPP Release. Description: A clear textual description of the feature.			

12.5 N6 specific Experimental-Result-Code AVP

Diameter Base IETF RFC 6733 [24] defines a number of Result-Code AVP values that are used to report protocol errors and how those are used. Those procedures and values apply for the present specification.

Due to the N6 specific AVPs, new application results can occur and the Experimental-Result AVP is used to transfer the 3GPP-specific result codes. The Experimental-Result AVP is a grouped AVP containing the Vendor-Id AVP set to the value of 3GPP's vendor identifier (10415) and an Experimental-Result-Code AVP.

The following N6 specific Experimental-Result-Code value is defined:

DIAMETER_QOS_FLOW_DELETION_INDICATION (2421)

For SMF this is an indication to the server that the requested 5G QoS flow or PDU session has been deleted.

12.6 N6 Diameter messages

12.6.1 General

This clause describes the N6 Diameter messages.

The relevant AVPs that are of use for the N6 interface are detailed in this subclause. Other Diameter AVPs as defined in IETF RFC 4072 [25] and IETF RFC 7155 [23], even if their AVP flag rules are marked with "M", are not required for being compliant with the current specification.

Diameter messages as defined in subclause 16a.4 of 3GPP TS 29.061 [5] are re-used in 5G with the following differences:

- SMF or SMF+PGW-C replaces P-GW, and GGSN related description are not applicable for 5G.
- 5G QoS flow replaces IP-CAN/EPS bearer and PDU session replaces IP-CAN session.
- N6 replaces Gi/Sgi.

NOTE: N6 re-used and specific AVPs are specified in subclause 12.3 and subclause 12.4.

- 3GPP-NAI AVP may be included in the AAR and ACR command.
- 3GPP-NID AVP may be included together with 3GPP-SGSN-MCC-MNC AVP in the AAR and ACR command.
- 3GPP-Session-S-NSSAI AVP and/or 3GPP-Session-Id AVP may be included in the AAR and ACR command.
- 3GPP-DNAI AVP, 3GPP-RSN AVP and/or 3GPP-Session-Pair-Id AVP may be included in the ACR command.
- Multiple 3GPP-IP-Address-Pool-Info AVPs may be included in the AAR command and one or two 3GPP-IP-Address-Pool-Info AVPs may be included in the AAA and ACR command.
- Multiple 3GPP-UE-MAC-Address AVPs may be included in the AAR and ACR command.
- For indicating user location, TWAN-Identifier AVP, 3GPP-TNAP-Identifier AVP, 3GPP-HFC-NodeId AVP, 3GPP-GLI AVP, 3GPP-Line-Type AVP, 3GPP-UE-Local-IP-Address and optionally UDP or TCP source port number (if NAT is detected) may be included in the AAR and ACR command.
- Acct-Application-Id AVP shall be included in the ACR and ACA command as specified in IETF RFC 7155 [23].
- Additional Diameter messages needed for 5G compared to the 3GPP TS 29.061 [5] are described in the following subclauses.
- Multiple Supported-Features AVPs may be included in the ACR and ACA command.

12.6.2 DER Command

The DER command, defined in IETF RFC 4072 [25], is indicated by the Command-Code field set to 268 and the 'R' bit set in the Command Flags field. It is sent by the SMF to the DN-AAA server upon reception of an initial access request (e.g. Nsmf_PDUSession_CreateSMContext) message for a given DNN to request user authentication and authorization.

The relevant AVPs that are of use for the N6 interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for N6 purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for N6, or modified existing AVPs.

Message Format:

```
<Diameter-EAP-Request> ::= < Diameter Header: 268, REQ, PXY >
                         < Session-Id >
                         { Auth-Application-Id }
                         { Origin-Host }
                         { Origin-Realm }
                         { Destination-Realm }
                         { Auth-Request-Type }
                         [ Destination-Host ]
                         [ NAS-Port ]
                         [ NAS-Port-Id ]
                         [ NAS-Port-Type ]
                         [ Origin-State-Id ]
                         [ Port-Limit ]
                         [ User-Name ]
                         { EAP-Payload }
                         [ EAP-Key-Name ]
                         [ Service-Type ]
                         [ Authorization-Lifetime ]
                         [ Auth-Grace-Period ]
                         [ Auth-Session-State ]
                         [ Callback-Number ]
                         [ Called-Station-Id ]
                         [ Calling-Station-Id ]
                         [ Originating-Line-Info ]
                         [ Connect-Info ]
                       * [ Framed-Compression ]
                         [ Framed-Interface-Id ]
                         [ Framed-IP-Address ]
                       * [ Framed-IPv6-Prefix ]
                       * [ Delegated-IPv6-Prefix ]
                         [ Framed-IP-Netmask ]
                         [ Framed-MTU ]
                         [ Framed-Protocol ]
```

```
                    * [ Tunneling ]
                    * [ Proxy-Info ]
                    * [ Route-Record ]
                      [ External-Identifier ]
                      [ 3GPP-IMSI ]
                      [ 3GPP-NAI ]
                    * [ 3GPP-UE-MAC-Address ]
                      [ 3GPP-Charging-ID ]
                      [ 3GPP-PDP-Type ]
                      [ 3GPP-CG-Address ]
                      [ 3GPP-CHF-FQDN ]
                      [ 3GPP-GPRS-Negotiated-QoS-Profile ]
                      [ 3GPP-SGSN-Address ]
                      [ 3GPP-GGSN-Address ]
                      [ 3GPP-Session-S-NSSAI ]
                      [ 3GPP-Session-Id ]
                      [ 3GPP-IMSI-MCC-MNC ]
                      [ 3GPP-GGSN-MCC-MNC ]
                      [ 3GPP-NSAPI ]
                      [ 3GPP-Selection-Mode ]
                      [ 3GPP-Charging-Characteristics ]
                      [ 3GPP-CG-IPv6-Address ]
                      [ 3GPP-SGSN-IPv6-Address ]
                      [ 3GPP-Serving-NF-FQDN ]
                      [ 3GPP-GGSN-IPv6-Address ]
                      [ 3GPP-SGSN-MCC-MNC ]
                      [ 3GPP-NID ]
                      [ 3GPP-User-Location-Info ]
                      [ 3GPP-RAT-Type ]
                      [ 3GPP-Negotiated-DSCP ]
                      [ 3GPP-Allocate-IP-Type ]
                      [ TWAN-Identifier ]
                      [ 3GPP-TNAP-Identifier ]
                      [ 3GPP-HFC-NodeId ]
                      [ 3GPP-GCI ]
                      [ 3GPP-GLI ]
                      [ 3GPP-Line-Type ]
                      [ 3GPP-UE-Local-IP-Address ]
                      [ 3GPP-UE-Source-Port ]
                    * [ 3GPP-IP-Address-Pool-Info]
                    * [ Supported-Features ]
                    * [ AVP ]
```

12.6.3 DEA Command

The DEA command, defined in IETF RFC 4072 [25], is indicated by the Command-Code field set to 268 and the 'R' bit cleared in the Command Flags field. It is sent by the DN-AAA server to the SMF in response to the DER command.

The relevant AVPs that are of use for the N6 interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for N6 purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for N6, or modified existing AVPs.

Message Format:

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
                          < Session-Id >
                          { Auth-Application-Id }
                          { Auth-Request-Type }
                          { Result-Code }
                          { Origin-Host }
                          { Origin-Realm }
                          [ User-Name ]
                          [ EAP-Payload ]
                          [ EAP-Reissued-Payload ]
                          [ EAP-Master-Session-Key ]
                          [ EAP-Key-Name ]
                          [ Multi-Round-Time-Out ]
                          [ Accounting-EAP-Auth-Method ]
                          [ Service-Type ]
                        * [ Class ]
                          [ Acct-Interim-Interval ]
                          [ Error-Message ]
                          [ Error-Reporting-Host ]
                          [ Failed-AVP ]
```

```
                        [ Idle-Timeout ]
                        [ Authorization-Lifetime ]
                        [ Auth-Grace-Period ]
                        [ Auth-Session-State ]
                        [ Re-Auth-Request-Type ]
                        [ Session-Timeout ]
                      * [ Reply-Message ]
                        [ Origin-State-Id ]
                      * [ Filter-Id ]
                        [ Port-Limit ]
                        [ Callback-Id ]
                        [ Callback-Number ]
                      * [ Framed-Compression ]
                        [ Framed-Interface-Id ]
                        [ Framed-IP-Address ]
                      * [ Framed-IPv6-Prefix ]
                        [ Framed-IPv6-Pool ]
                      * [ Framed-IPv6-Route ]
                      * [ Delegated-IPv6-Prefix ]
                        [ Framed-IP-Netmask ]
                      * [ Framed-Route ]
                        [ Framed-Pool ]
                        [ Framed-IPX-Network ]
                        [ Framed-MTU ]
                        [ Framed-Protocol ]
                        [ Framed-Routing ]
                      * [ NAS-Filter-Rule ]
                      * [ QoS-Filter-Rule ]
                      * [ Tunneling ]
                      * [ Redirect-Host ]
                        [ Redirect-Host-Usage ]
                        [ Redirect-Max-Cache-Time ]
                      * [ Proxy-Info ]
                      * [ External-Identifier ]
                        [ 3GPP-IPv6-DNS-Servers ]
                        [ 3GPP-Notification ]
                   0*16 [ 3GPP-UE-MAC-Address ]
                   0*16 [ 3GPP-VLAN-Id ]
                        [ 3GPP-Authorization-Reference ]
                        [ 3GPP-Policy-Reference ]
                        [ 3GPP-Session-AMBR ]
                        [ 3GPP-Session-AMBR-v2 ]
                    0*2 [ 3GPP-IP-Address-Pool-Info]
                      * [ Supported-Features ]
                      * [ AVP ]
```

12.6.4 RAR Command

The RAR command, defined in IETF RFC 7155 [23], is indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field. It is sent by the DN-AAA server to the SMF to initiate re-authorization and optional re-authentication service.

The relevant AVPs that are of use for the N6 interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for N6 purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for N6, or modified existing AVPs.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                       < Session-Id >
                       { Origin-Host }
                       { Origin-Realm }
                       { Destination-Realm }
                       [ Destination-Host ]
                       { Auth-Application-Id }
                       { Re-Auth-Request-Type }
                       [ User-Name ]
                       [ Origin-State-Id ]
                       [ NAS-Port ]
                       [ NAS-Port-Id ]
                       [ NAS-Port-Type ]
                       [ Service-Type ]
                       [ Framed-IP-Address ]
                       [ Framed-IPv6-Prefix ]
```

```
                    [ Framed-Interface-Id ]
                    [ Called-Station-Id ]
                    [ Calling-Station-Id ]
                    [ Originating-Line-Info ]
                    [ Acct-Session-Id ]
                  * [ Class ]
                    [ Reply-Message ]
                  * [ Proxy-Info ]
                  * [ Route-Record ]
               0*16 [ 3GPP-UE-MAC-Address ]
               0*16 [ 3GPP-VLAN-Id ]
                    [ 3GPP-Authorization-Reference ]
                    [ 3GPP-Policy-Reference ]
                    [ 3GPP-Session-AMBR ]
                    [ 3GPP-Session-AMBR-v2 ]
                  * [ AVP ]
```

12.6.5 RAA Command

The RAA command, defined in IETF RFC 7155 [23], is indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field. It is sent by the SMF to the DN-AAA server in response to the RAR command.

The relevant AVPs that are of use for the N6 interface are detailed in the ABNF description below. Other valid AVPs for this command are not used for N6 purposes and should be ignored by the receiver or processed according to the relevant specifications.

The bold marked AVPs in the message format indicate new optional AVPs for N6, or modified existing AVPs.

Message Format:

```
<RA-Answer> ::= < Diameter Header: 258, PXY >
                      < Session-Id >
                      { Result-Code }
                      { Origin-Host }
                      { Origin-Realm }
                      [ User-Name ]
                      [ Origin-State-Id ]
                      [ Error-Message ]
                      [ Error-Reporting-Host ]
                      [ Failed-AVP ]
                    * [ Redirect-Host ]
                      [ Redirect-Host-Usage ]
                      [ Redirect-Max-Cache-Time ]
                      [ Service-Type ]
                      [ Idle-Timeout ]
                      [ Authorization-Lifetime ]
                      [ Auth-Grace-Period ]
                      [ Re-Auth-Request-Type ]
                    * [ Class ]
                    * [ Reply-Message ]
                    * [ Proxy-Info ]
                      [ 3GPP-RAT-Type ]
                    * [ AVP ]
```

13 Interworking with IMS

13.1 General

Interworking with the IP Multimedia Core Network Subsystem (IMS) puts specific requirements on the SMF.

The SMF shall use the following mechanisms to support the interworking with the IMS:

- the P-CSCF discovery;
- N7 interface for the policy and charging control of QoS flows for IMS media flows; and
- the P-CSCF restoration.

These mechanisms are however not restricted only to the interworking with the IMS and may be used for other services that could benefit from these mechanisms.

If the PDU Session is used for IMS (identified by DNN), the SMF shall not modify the fields Type of Service (IPv4) and Traffic Class (IPv6).

NOTE: The P-CSCF can support paging policy differentiation for different traffic or service types over NG-RAN by marking the fields Type of Service (IPv4) and Traffic Class (IPv6) (see subclause L.3.2.4 of 3GPP TS 24.229 [13]).

13.2 IMS interworking Model

13.2.1 Introduction

The signalling interface between the UE and the P-CSCF is a logical interface, i.e. it uses 5GC as a QoS flow. The Npcf_SMPolicyControl services, offered via N7 interface, are used for network communication between the SMF and the PCF. For a description of the IMS architecture, refer to 3GPP TS 23.228 [12].

13.2.2 IMS specific configuration in the SMF

The SMF shall have a list of preconfigured addresses of signalling servers (the P-CSCF servers). This list shall be provided to the UE at PDU session establishment. It shall be possible to preconfigure the list of preconfigured addresses of signalling servers per DNN.

The SMF/UPF may have the locally preconfigured packet filters, and/or the applicable PCC rules, to be applied on the QoS flow. The packet filters shall filter up-link and down-link packets, and shall only allow traffic to/from the signalling servers and to the DNS and the DHCP servers. It shall be possible to locally preconfigure the packet filters per DNN.

It shall be possible to enable/disable the use of the services offered via N7 interface per DNN.

The SMF shall support IPv4 and/or IPv6 addresses and protocol for IMS signalling and IMS QoS flows.

The methods for the UE to discover the P-CSCF address(es) may vary depending on the access technology that the UE is on. The details of the P-CSCF discovery mechanisms for various accesses are specified in 3GPP TS 23.228 [12] and 3GPP TS 24.229 [13]. The P-CSCF discovery mechanisms are:

- a 5GC procedure for the P-CSCF discovery;
- via DHCP servers i.e. the SMF shall provide the functionality of a DHCP relay agent; and
- if the UE has a P-CSCF FQDN locally configured and request the DNS IP address(es) from the SMF (via 5GC mechanism or DHCP procedures), the SMF shall be able to provide DNS IP address(es) to the UE.

The SMF shall have similar functional support depending on the P-CSCF discovery methods supported by the UE on the access technology. For example, for the UE in 3GPP 5G access network the SMF shall have DHCP server function towards the UE while acting as a DHCP client towards external DHCP server, if the SMF is configured to request DNS and/or P-CSCF IP addresses from the external DHCP servers.

The SMF shall be able to deliver DNS and/or P-CSCF addresses to the UE if requested by the UE via the 5G network or via DHCP procedures using the relevant DHCP options for IPv4/IPv6 DNS and SIP servers (see IETF RFC 2132 [14], IETF RFC 3361 [15], IETF RFC 3646 [16] and IETF RFC 3319 [17]).

On DNNs providing IMS services, the information advertised in Router Advertisements from the SMF to the UEs shall be configured in the same manner as for other DNNs providing IPv6 services except that the "O-flag" shall be set.

The "O-flag" shall be set in IPv6 Router Advertisement messages sent by the SMF for DNNs used for IMS services. This will trigger a DHCP capable UE to start a DHCPv6 session to retrieve server addresses and other configuration parameters. The UE which doesn't support DHCP shall ignore the "O-flag" and shall request the IMS specific configuration (e.g. the P-CSCF address) via other discovery methods supported in the UE (i.e. via locally configured P-CSCF address/FQDN in the UE or via 5G procedure, if applicable).

The SMF shall have configurable policy rules for controlling QoS flows used for signalling.

13.2.3 IMS specific procedures in the SMF

13.2.3.1 Provisioning of Signalling Server Address

At a PDU Session establishment procedure related to the IMS, the SMF shall support the capability to send the P-CSCF address(es) to the UE. The P-CSCF address information is sent by the visited SMF if LBO is used. For Home routed, the P-CSCF address information is sent by the SMF in the HPLMN. The P-CSCF address(es) shall be sent transparently through the AMF, and in case of Home Routed also through the SMF in the VPLMN.

NOTE 1: The SMF is located in the VPLMN if LBO is used.

NOTE 2: Other options to provide the P-CSCF address(es) to the UE as defined in 3GPP TS 23.228 [12] is not excluded.

NOTE 3: A PDU session for IMS is identified by "APN" or "DNN".

13.2.3.2 Failure of Signalling Server Address

If the SMF detects a failure:

- upon receiving the N4 session report from the UPF for the monitored P-CSCF address being used by the UE (as specified in 3GPP TS 23.380 [38], subclause 5.8.3); or

- upon receiving a P-CSCF restoration indication from the UDM or the PCF,

then the SMF shall act as specified in 3GPP TS 23.380 [38], subclause 5.8.

14 Interworking with DN (Ethernet)

When support of Ethernet PDU type data is provided at the N6 interface, the SMF and UPF may support ARP proxying as specified in IETF RFC 1027 [35] and/or IPv6 Neighbour Solicitation Proxying as specified in IETF RFC 4861 [33] functionality. Based on operator configuration, during the PDU session establishment, the SMF may request the UPF acting as the PDU Session Anchor to proxy ARP/IPv6 Neighbour Solicitation or to forward the ARP/IPv6 Neighbour Solicitation traffic from the UPF to the SMF.

Ethernet Preamble, Start Frame Delimiter (SFD) and Frame Check Sequence (FCS) are not sent over 5GS:

- For UL traffic the UE strips the Preamble, SFD and FCS from the Ethernet frame, those fields shall be added by the UPF acting as the PDU Session Anchor.

- For DL traffic the UPF acting as the PDU Session Anchor shall strip the Preamble, SFD and FCS from the Ethernet frame.

IP address is not allocated by the SMF to the UE for this PDU Session. The UPF shall store the MAC addresses, received from the UE, and associate those with the appropriate PDU Session.

NOTE 1: The UE can operate in bridge mode with regard to a LAN it is connecting to the 5GS, thus different MAC addresses can be used as source address of different frames sent UL over a single PDU Session (and destination MAC address of different frames sent DL over the same PDU Session)

NOTE 2: Entities on the LAN connected to the 5GS by the UE can have an IP address allocated by the external DN, but the IP layer is considered as an application layer which is not part of the Ethernet PDU Session.

NOTE 3: In this Release of the specification, only the UE connected to the 5GS is authenticated, not the devices behind such UE.

When a PDU Session of Ethernet PDU type is authorized by a DN, the DN-AAA server may, as part of authorization data, provide the SMF with a list of allowed MAC addresses (maximum 16) for this PDU Session. When such a list has been provided for a PDU Session, the SMF sets corresponding filtering rules in the UPF(s) acting as PDU Session Anchor for the PDU Session and the UPF discards any UL traffic that does not contain any of these MAC addresses as a source address.

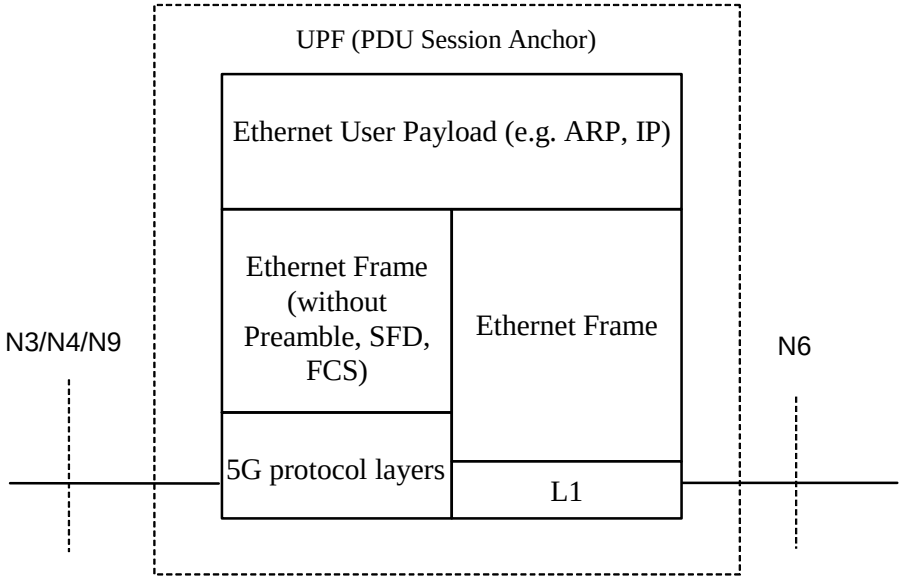

Figure 14-1: Protocol stacks for Ethernet PDU type data (user plane) for N6 reference point

15 Interworking with DN (Multicast Routing Protocol)

15.1 General

The 3GPP network support IPTV multicast packets transmission over PDU Session as specified in 3GPP TS 23.316 [43] subclause 7.7.1. When support of multicast routing protocol is provided at the N6 interface, different techniques may be used.

15.2 DN interworking Model of UPF for PIM

If PIM (Protocol-Independent Multicast) is used as Multicast Routing Protocol, including PIM-SM (Protocol-Independent Multicast-Sparse Mode, IETF RFC 7761 [44]) and PIM-DM (Protocol-Independent Multicast- Dense Mode, IETF RFC 3973 [45]), are commonly used to efficiently routing multicast groups that may span wide-area (and inter-domain) internets.

UPF acts as the PIM router which is clostest to UE and receive multicast packets originated from multicast source via perform PIM function. Based on local policy, UPF support either PIM-SM or PIM-DM or both.

UPF shall acts as PIM router used for interworking with the IP network as illustrated in figure 15.2-1.

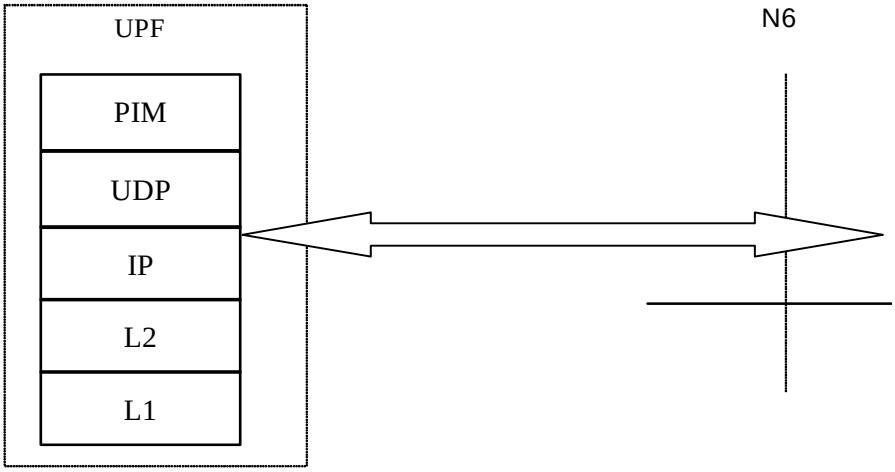

Figure 15.2-1: The protocol stacks for the N6 reference point for PIM

PIM function in UPF shall interacts with PIM routers in IP network.

- In case of PIM-SM, PIM router in UPF acts as DR (Designated Router) which is clostest to UE and send register message to RP (Rendezvous Point). It receive multicast packets over shared tree from RP. Refer to IETF RFC 7761 [44] for more details.
- In case of PIM-DM, PIM router in UPF sends Upstream Prune Messages to indicate that designated multicast traffic is not desired, It sends Upstream Graft message to re-join a previously pruned branch to the delivery tree. Refer to IETF RFC 3973 [45] for more details.

16 Interworking with NSS-AAA (RADIUS)

16.1 RADIUS procedures

16.1.1 General

The Network Slice Specific Authentication and Authorization procedure is triggered for a network slice requiring Network Slice Specific Authentication and Authorization with an NSS-AAA server which may be hosted by the H-PLMN operator or by a third party which has a business relationship with the H-PLMN. An AAA Proxy (AAA-P) in the HPLMN may be involved e.g. if the NSS-AAA Server belongs to a third party.

16.1.2 RADIUS Authentication and Authorization

RADIUS Authentication and Authorization shall be used according to IETF RFC 2865 [8], IETF RFC 3162 [9] and IETF RFC 4818 [10]. In 5G, multiple authentication methods using Extensible Authentication Protocol (EAP) may be used such as EAP-TLS (see IETF RFC 5216 [11]), EAP-TTLS (see IETF RFC 5281 [37]). The NSSAAF or AAA-P shall implement the RADIUS extension to support EAP as specified in IETF RFC 3579 [7].

The RADIUS client function may reside in an NSSAAF. When the NSSAAF receives Nnssaaf_NSSAA_Authenticate request from AMF, the RADIUS client function shall send the authentication information with network slice information to a NSS-AAA server directly or via an AAA-P.

The NSS-AAA server performs authentication and authorization for the user and requested network slice information. When the NSSAAF receives an Access-Accept message from the NSS-AAA server or AAA-P, it shall complete the network slice specific authentication procedure. If Access-Reject or no response is received, the NSSAAF shall reject the network slice specific authentication procedure with a suitable cause code.

The NSS-AAA may revoke the authorization for the network slice, see details in clause 16.2.2. In the present release, the NSS-AAA initiated re-authentication is not supported.

16.2 Message flows for network slice specific authentication

16.2.1 Authentication and Authorization procedures

When the NSSAAF receives Nnssaaf_NSSAA_Authenticate request from AMF, it shall send a RADIUS Access-Request message with EAP extension to an NSS-AAA server directly or via an AAA-P if AAA-P is involved. The Access-Request message shall include GPSI in Calling-Station-Id or External-Identifier attribute and network slice information in 3GPP-S-NSSAI attribute. Upon receipt of the Access-Request message, the NSS-AAA server shall respond with an Access-Challenge message. Multi-round authentication using the Access-Challenge (sent by NSS-AAA) and Access-Request messages may be used. The NSS-AAA server finally authenticates and authorizes the user and the network slice by replying with an Access Accept message.

For re-authentication and re-authorization, the NSSAAF shall send a RADIUS Access-Request message with EAP extension to the NSS-AAA server directly or via the AAA-P if AAA-P is used and the NSS-AAA shall respond with an Access-Challenge message. Multi-round authentication using the Access-Challenge (sent by NSS-AAA) and Access-Request messages may be used. The NSS-AAA server finally authenticates and authorizes the user and the network slice by replying with an Access Accept message.

The following figure 16.2.1-1 is an example message flow to show the procedure of RADIUS Authentication and Authorization between an AMF and a NSS-AAA server:

1. AMF decides to trigger the start of the Network Slice Specific Authentication and Authorization procedure.

2. The AMF may send an EAP Identity Request in a NAS Network Slice-Specific Authentication Command message.

3. The UE provides the EAP Identity Response in a NAS Network Slice-Specific Authentication Complete message towards the AMF.

4. The AMF sends Nnssaaf_NSSAA_Authenticate Request to the NSSAAF including the authentication/authorization information.

5-6. If the AAA-P is present (e.g. because the NSS-AAA belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF sends the Access-Request message to the NSS-AAA via the AAA-P to forward the authentication/authorization information, otherwise the NSSAAF sends the Access-Request message directly to the NSS-AAA.

7-14. The NSS-AAA responds with the Access-Challenge message to the NSSAAF directly or via the AAA-P. The authentication/authorization information is further transferred to UE via AMF by Nnssaaf_NSSAA_Authenticate service and NAS Network Slice-Specific Authentication Command message. UE responds to the received authentication/authorization data and such information is transferred in NAS Network Slice-Specific Authentication Complete message and Nnssaaf_NSSAA_Authenticate service, then finally sent to the NSS-AAA by the NSSAAF, via the AAA-P if the AAA-P is used, in the Access-Request message.

NOTE: Step 7 to step 14 can be repeated depending on the authentication/authorization mechanism used (e.g. EAP-TLS).

15-16. If the AAA-P is used, the NSS-AAA sends a Access-Accept message with the final result of authentication/authorization to the NSSAAF via the AAA-P, otherwise the NSS-AAA sends the Access-Accept message directly to the NSSAAF.

17. The NSSAAF sends a Nnssaaf_NSSAA_Authenticate Response with the final result of authentication/authorization information to the AMF.

18. The AMF transfers the final result of authentication/authorization information in a NAS Network Slice-Specific Authentication Result message to the UE.

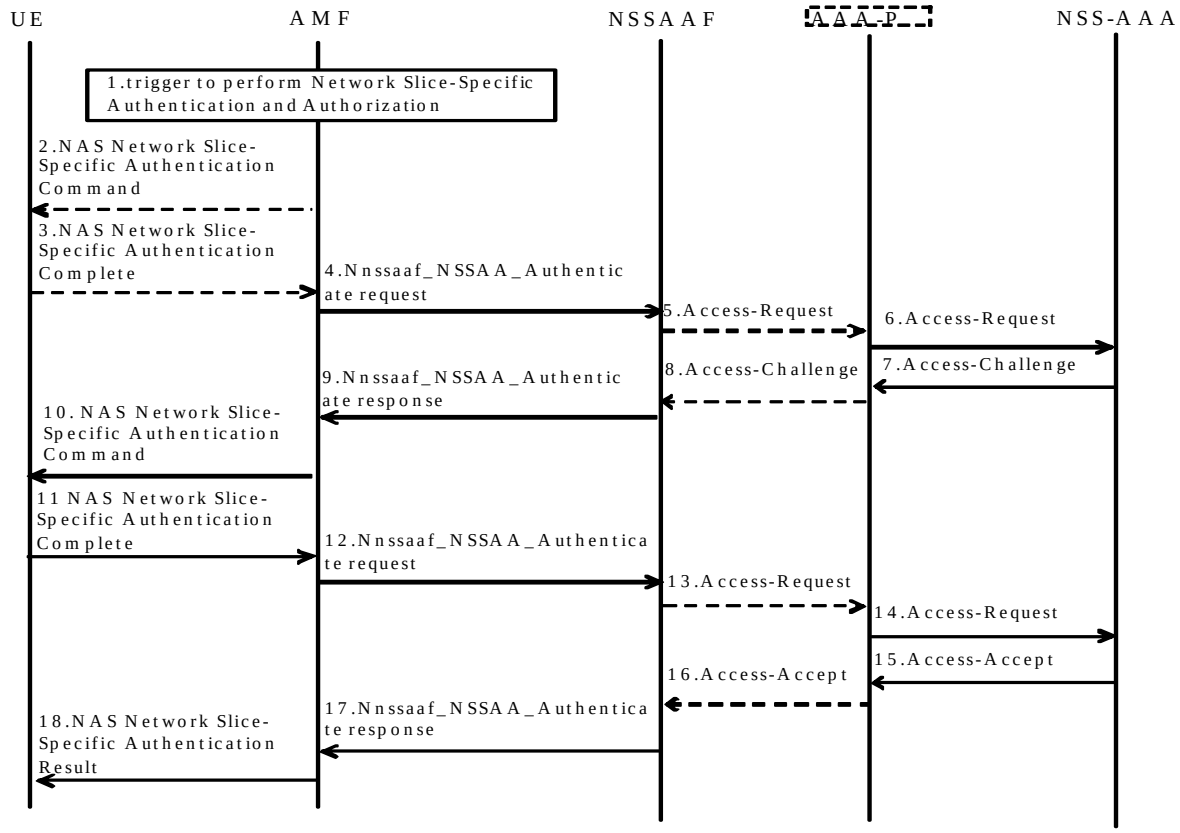

Figure 16.2.1-1: Network slice specific authentication and Authorization procedure (RADIUS)

16.2.2 NSS-AAA initiated revocation of network slice authorization

The NSS-AAA server may send a RADIUS Disconnect-Request to the NSSAAF directly or via AAA-P (if AAA-P is used) asking for revocation of network slice authorization. On receipt of the Disconnect-Request from the NSS-AAA server, the NSSAAF shall check whether the NSS-AAA server is authorized to request the revocation by verifying the local configuration of the address of the NSS-AAA server per S-NSSAI, if successful, the NSSAAF shall release the resources, interact with its succeeding Network Function AMF which is got from the UDM by Nudm_UECM_GET service operation with GPSI and reply with a Disconnect-ACK. If the NSSAAF is unable to release the corresponding resources, it shall reply to the NSS-AAA server with a Disconnect-NAK. For more information on RADIUS Disconnect, see IETF RFC 5176 [27]. It is not necessary for the NSSAAF to wait for the response (i.e. Nudm_UECM_GET or Nnssaaf_NSSAA_Notify response) from the succeeding Network Function before sending the RADIUS Disconnect-ACK to the NSS-AAA server or AAA-P (if AAA-P is used).

Editor's Note: It is FFS whether the RADIUS is applicable.

Figure 16.2.2-1 is an example message flow to show the procedure of NSS-AAA initiated revocation of network slice authorization. If the AAA-P is not used, the Disconnect Request and Response messages are exchanged between the NSS-AAA and the NSSAAF.

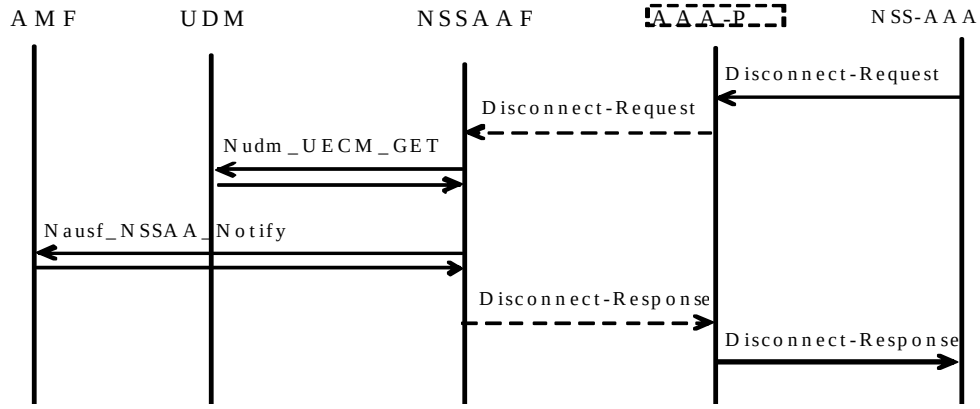

Figure 16.2.2-1: NSS-AAA initiated revocation of network slice authorization with RADIUS

16.3 List of RADIUS attributes

16.3.1 General

Information defined in clause 11.3 are re-used for network slice specific authentication with the following differences:

- NSSAAF replaces SMF.
- IP, Ethernet and PDU session related descriptions and attributes are not applicable.
- RADIUS messages for accounting function (Accounting Request/Response) are not applicable.
- Additional detailed information needed for network slice specific authentication are described below.

Table 16.3-1: Additional information needed for network slice specific authentication

Sub-attr #	Sub-attribute Name	Differences
200	3GPP-S-NSSAI	Added.
NOTE: 5G specific RADIUS VSAs for network slice specific authentication are numbered from 200.		

200 – 3GPP-S-NSSAI

Bits

Octets	8	7	6	5	4	3	2	1
1	3GPP type = 200							
2	3GPP Length= m							
3	SST							
4-6	SD (octet string)							

3GPP Type: 200

Length: 3 or 6

SST: the Slice/Service Type with value range 0 to 255.

SD: 3-octet string, representing the Slice Differentiator, the encoding follows sd attribute specified in subclause 5.4.4.2 of 3GPP TS 29.571 [46]. Its presence depends on the Length field.

Table 16.3-2 describes the sub-attributes of the 3GPP Vendor-Specific attribute described above in different RADIUS messages.

Table 16.3-2: List of the 3GPP Vendor-Specific sub-attributes for network slice specific authentication

Sub-attr #	Sub-attribute Name	Description	Presence Requirement	Associated attribute (Location of Sub-attr)	Applicability
200	3GPP-S-NSSAI	It includes the S-NSSAI.	Conditional (NOTE)	Access-Request	
NOTE: This VSA shall be included in the initial Access-Request message.					

17 Interworking with NSS-AAA (Diameter)

17.1 Diameter procedures

17.1.1 General

The Network Slice Specific Authentication and Authorization procedure is triggered for a network slice requiring Network Slice Specific Authentication and Authorization with an NSS-AAA server which may be hosted by the H-PLMN operator or a third party which has a business relationship with the H-PLMN. An AAA Proxy (AAA-P) in the HPLMN may be involved e.g. if the NSS-AAA Server belongs to a third party.

17.1.2 Diameter Authentication and Authorization

Diameter Authentication and Authorization shall be used according to IETF RFC 7155 [23]. In 5G, multiple authentication methods using Extensible Authentication Protocol (EAP) may be used such as EAP-TLS (see IETF RFC 5216 [11]), EAP-TTLS (see IETF RFC 5281 [37]). The NSSAAF or AAA-P shall support Diameter EAP application as specified in IETF RFC 4072 [25].

The NSSAAF or AAA-P and the NSS-AAA shall advertise the support of the Diameter NASREQ and EAP applications by including the value (1 and 5) of the application identifier in the Auth-Application-Id AVP (as specified in IETF RFC 4072 [25]) and the value of the 3GPP (10415) in the Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands as specified in IETF RFC 6733 [24], i.e. as part of the Vendor-Specific-Application-Id AVP.

The Diameter client function may reside in an NSSAAF. When the NSSAAF receives Nnssaaf_NSSAA_Authenticate request from AMF, the Diameter client function shall send the authentication information with network slice information to a NSS-AAA server directly or via an AAA-P (if AAA-P is used).

The NSS-AAA server performs authentication and authorization for the requested network slice information. When the Nnssaaf receives a positive response from the NSS-AAA server or AAA-P (if AAA-P is used), it shall complete the network slice specific authentication procedure. If negative response or no response is received, the NSSAAF shall reject the network slice specific authentication procedure with a suitable cause code.

The NSS-AAA may revoke the authorization for the network slice, see details in clause 17.2.2. NSS-AAA may initiate re-authentication and re-authorization, see details in clause 17.2.3.

17.2 Message flows for network slice specific authentication

17.2.1 Authentication and Authorization procedures

For network slice specific authentication and authorization, when the NSSAAF receives Nnssaaf_NSSAA_Authenticate request from AMF, it shall send a Diameter DER message with GPSI in Calling-Station-Id or External-Identifier attribute and network slice information in 3GPP-S-NSSAI attribute to a NSS-AAA server directly or via AAA-P if AAA-P is involved. Upon receipt of the DER message, the DN-AAA server shall respond with an DEA message.

Multi-round authentication using the DEA and DER messages may be used. The NSS-AAA server finally authenticates and authorizes the user and the network slice by replying with a Diameter DEA message.

For re-authentication and re-authorization, the NSSAAF shall send a DER message to the NSS-AAA server directly or via AAA-P if AAA-P is used and the NSS-AAA server shall respond with a DEA message. Multi-round authentication using the DEA and DER messages may be used. The NSS-AAA server finally authenticates and authorizes the user and the network slice by replying with a Diameter DEA message.

If the network slice specific authentication is not required, the NSSAAF shall send a Diameter STR message to the NSS-AAA server directly or via AAA-P if AAA-P is involved. The NSS-AAA server shall reply with a Diameter STA message.The following figure 17.2.1-1 is an example message flow to show the procedure of Diameter Authentication and Authorization between an AMF and a NSS-AAA server:

1. AMF decides to trigger the start of the Network Slice Specific Authentication and Authorization procedure.

2. The AMF may send an EAP Identity Request in a NAS Network Slice-Specific Authentication Command message.

3. The UE provides the EAP Identity Response in a NAS Network Slice-Specific Authentication Complete message towards the AMF.

4. The AMF sends Nnssaaf_NSSAA_Authenticate Request to the NSSAAF including the authentication/authorization information.

5-6. If the AAA-P is present (e.g. because the NSS-AAA belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF sends the DER message to the NSS-AAA via the AAA-P to forward the authentication/authorization information, otherwise the NSSAAF sends the DER message directly to the NSS-AAA.

7-14. The NSS-AAA responds with the DEA message to the NSSAAF directly or via the AAA-P. The authentication/authorization information is further transferred to UE via AMF by Nnssaaf_NSSAA_Authenticate service and NAS MM Transport message. UE responds to the received authentication/authorization data and such information is transferred in NAS Network Slice-Specific Authentication Complete message and Nnssaaf_NSSAA_Authenticate service, then finally sent to the NSS-AAA by the NSSAAF, via the AAA-P if the AAA-P is used, in the DER message.

NOTE: Step 7 to step 14 can be repeated depending on the authentication/authorization mechanism used (e.g. EAP-TLS).

15-16. If the AAA-P is used, the NSS-AAA sends a DEA message with the final result of authentication/authorization to the NSSAAF via the AAA-P, otherwise the NSS-AAA sends the DEA message directly to the NSSAAF.

17. The NSSAAF sends a Nnssaaf_NSSAA_Authenticate Response with the final result of authentication/authorization information to the AMF.

18. The AMF transfers the final result of authentication/authorization information in a NAS Network Slice-Specific Authentication Result message to the UE.

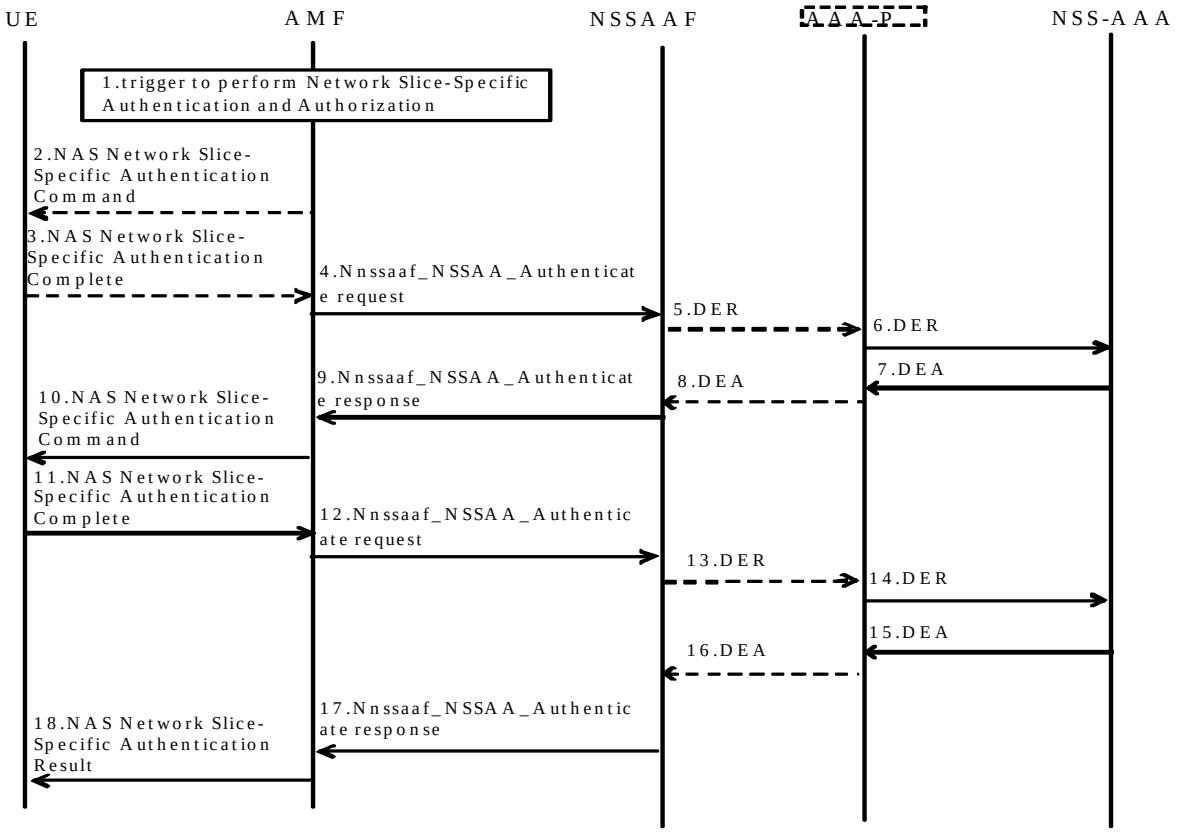

Figure 17.2.1-1: Network slice specific authentication and Authorization procedure (Diameter)

17.2.2 NSS-AAA initiated revocation of network slice authorization

The NSS-AAA server may send a Diameter ASR message to the NSSAAF directly or via AAA-P (if AAA-P is used) asking for revocation of network slice authorization. On receipt of the ASR message from the NSS-AAA server, the NSSAAF shall check whether the NSS-AAA server is authorized to request the revocation by verifying the local configuration of the address of the NSS-AAA server per S-NSSAI, if successful, the NSSAAF shall release the corresponding resources, interact with its succeeding Network Function AMF which is got from the UDM by Nudm_UECM_GET service operation with GPSI and reply with a Diameter ASA message. It is not necessary for the NSSAAF to wait for the response (i.e. Nudm_UECM_GET or Nnssaaf_NSSAA_Notify response) from its succeeding Network Function before sending the ASA message to the NSS-AAA server or AAA-P.

NOTE: In the Diameter ASR request, the Origin-Host AVP with the FQDN/domain format indicates the address of the NSS-AAA server for NSSAAF check.

Figure 17.2.2-1 is an example message flow to show the procedure of NSS-AAA initiated revocation of network slice authorization. If the AAA-P is not used, the ASR and ASA messages are exchanged between the NSS-AAA and the NSSAAF.

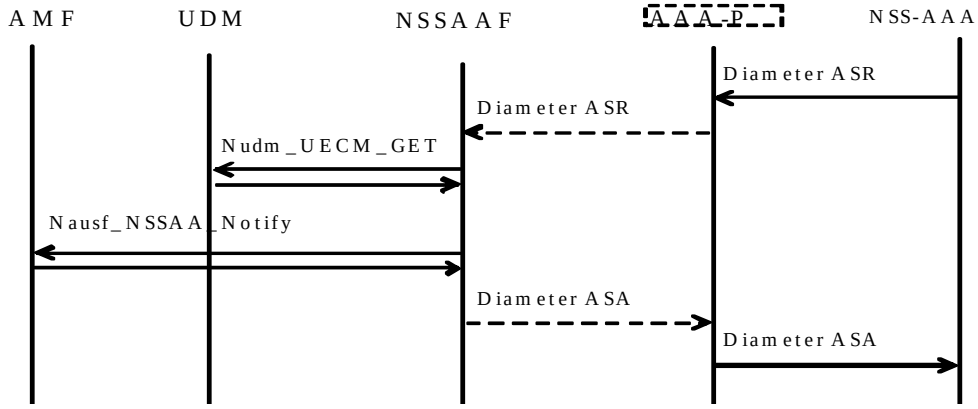

Figure 17.2.2-1: NSS-AAA initiated revocation of network slice authorization with Diameter

17.2.3 NSS-AAA initiated re-authentication and re-authorization

The NSS-AAA server may send a Diameter RAR message to the NSSAAF directly or via AAA-P (if AAA-P is used) asking for re-authentication and re-authorization. On receipt of the RAR message from the NSS-AAA server, the NSSAAF shall check whether the NSS-AAA server is authorized to request the re-authentication and re-authorization by verifying the local configuration of the address of the NSS-AAA server per S-NSSAI, if successful, the NSSAAF shall interact with its succeeding Network Function AMF which is got from the UDM by Nudm_UECM_GET service operation with GPSI and reply with a Diameter RAA message. It is not necessary for the NSSAAF to wait for the response (i.e. Nudm_UECM_GET or Nnssaaf_NSSAA_Notify response) from its succeeding Network Function before sending the RAA message to the NSS-AAA server or AAA-P.

NOTE: In the Diameter RAR request, the Origin-Host AVP with the FQDN/domain format indicates the address of the NSS-AAA server for NSSAAF check.

After replying Nnssaaf_NSSAA_Notify response, the AMF shall start authentication and authorization procedure as described in clause 17.2.1. The Auth-Request-Type in the DER is set to "AUTHORIZE_AUTHENTICATE".

Figure 17.2.3-1 is an example message flow to show the procedure of NSS-AAA initiated re-authentication and re-authorization. If the AAA-P is not used, the RAR and RAA messages are exchanged between the NSS-AAA and the NSSAAF.

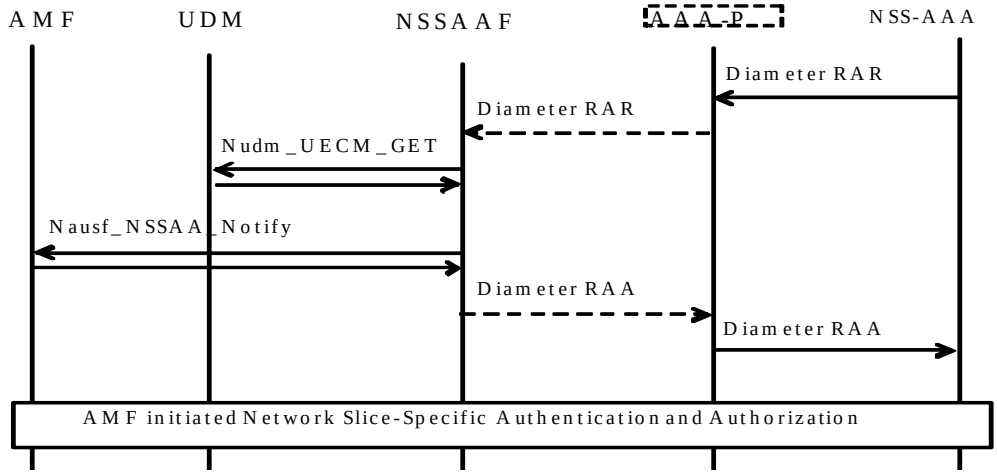

Figure 17.2.3-1: NSS-AAA initiated re-authentication and re-authorization with Diameter

17.3 Specific AVPs

There is no specific AVP defined in the present release.

17.4 re-used AVPs

17.4.1 General

Information defined in clause 12.4.0 are re-used for network slice specific authentication with the following differences:

- NSSAAF replaces SMF.
- IP, Ethernet and PDU session related descriptions and AVPs are not applicable.
- Additional detailed information needed for network slice specific authentication are described below.

Table 17.4-1: Additional information needed for network slice specific authentication

Attribute Name	AVP Code	Section defined	Value Type (NOTE 2)	AVP Flag rules (NOTE 1)				May Encr.	Applicability
				Must	May	Should not	Must not		
3GPP-S-NSSAI	200	16.3.1 (NOTE 3)	UTF8String	V	P		M	Y	

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see IETF RFC 6733 [24].
NOTE 2: The value types are defined in IETF RFC 6733 [24].
NOTE 3: The use of Radius VSA as a Diameter vendor AVP is described in Diameter NASREQ (IETF RFC 7155 [23]) and the P flag may be set.

17.4.2 Use of the Supported-Features AVP

The Supported-Features AVP is used during the network slice specific authentication procedure to inform the destination host about the required and optional features that the origin host supports. The client shall, in the first request in a Diameter session indicate the set of supported features. The server shall, in the first answer within the Diameter session indicate the set of features that it has in common with the client and that the server shall support within the same Diameter session. Any further command messages shall always be compliant with the list of supported features indicated in the Supported-Features AVPs during session establishment. Features that are not advertised as supported shall not be used to construct the command messages for that Diameter session. Unless otherwise stated, the use of the Supported-Features AVP shall be compliant with the requirements for dynamic discovery of supported features and associated error handling on the Cx reference point as defined in clause 7.2.1 of 3GPP TS 29.229 [41].

The base functionality is the 3GPP Rel-16 standard and a feature is an extension to that functionality. If the origin host does not support any features beyond the base functionality, the Supported-Features AVP may be absent in the DER command. As defined in clause 7.1.1 of 3GPP TS 29.229 [41], when extending the application by adding new AVPs for a feature, the new AVPs shall have the M bit cleared and the AVP shall not be defined mandatory in the command ABNF.

As defined in 3GPP TS 29.229 [41], the Supported-Features AVP is of type grouped and contains the Vendor-Id, Feature-List-ID and Feature-List AVPs. The Supported-Features AVP is used to identify features that have been defined by 3GPP and hence, for features defined in this document, the Vendor-Id AVP shall contain the vendor ID of 3GPP (10415). If there are multiple feature lists defined, the Feature-List-ID AVP shall differentiate those lists from one another.

On receiving an initial request application message, the destination host shall act as defined in clause 7.2.1 of 3GPP TS 29.229 [41].

Once the NSSAAF or AAA-P and NSS-AAA have negotiated the set of supported features during session establishment, the set of common features shall be used during the lifetime of the Diameter session.

The table below defines the features applicable for the network slice specific authentication, for the feature lists with a Feature-List-ID of 1.

Table 17.4.2-1: Features of Feature-List-ID 1

Feature bit	Feature	M/O	Description

Feature bit: The order number of the bit within the Feature-List AVP where the least significant bit is assigned number "0".
Feature: A short name that can be used to refer to the bit and to the feature, e.g. "5GC".
M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O") in this 3GPP Release.
Description: A clear textual description of the feature.

17.5 Specific Experimental-Result-Code AVP

There is no specific experimental result code AVP defined in the present release.

17.6 Diameter messages

17.6.1 General

Diameter messages as defined in subclause 12.6 are re-used for network slice specific authentication with the following differences:

- NSSAAF or AAA-P replaces SMF.
- IP, Ethernet and PDU session related descriptions and AVPs are not applicable.
- Diameter commands for accounting function (ACR and ACA) are not applicable.
- AAR and AAA commands are not applicable.
- 3GPP-S-NSSAI is included in the DER command.
- the address of NSS-AAA server is included in the Origin-Host AVP in the ASR and RAR command

NOTE: The presence of 3GPP-S-NSSAI in the DER command is optional but it is mandatory for the NSSAAF or AAA-P to include it for the network slice specific authentication.

18 Interworking with DN (L2TP tunnel)

18.1 Support L2TP for CUPS across N6

L2TP (described in IETF RFC 2661 [57]) is a standard method for tunneling encapsulated Point-to-Point Protocol (PPP) frames over an IP network. L2TP operates between two L2TP endpoints (LAC and LNS), and tunnels PPP-encapsulated IP traffic between these endpoints. L2TP runs over UDP/IP and was originally defined for systems where PPP is used by an end-device to connect to a network (e.g. via DSL connections, or 2G/3G PPP PDP context). In these cases, a LAC could be deployed in the network (e.g. in a BNG or GGSN/PGW) to tunnel the PPP traffic to a server (LNS) over an IP network.

For 5GC with the UE using IP PDU Session, the PPP functionality that is required to use L2TP is instead supported by the UPF or UPF+PGW-U, as illustrated in below figure. Upon receiving a PDU Session/PDN Connection establishment request from the UE via AMF or MME, SMF or SMF+PGW-C may depend on local L2TP configuration per DNN or the received L2TP information from a DN AAA server in Access-Accept message, request the UPF or UPF+PGW-U to setup L2TP tunnel towards an L2TP network server (LNS) in the external DN and tunnel the PDU Session user plane traffic in this L2TP tunnel. In this case the UPF or UPF+PGW-U acts as a L2TP access concentrator (LAC).

To enable this, the SMF or SMF+PGW-C may provide L2TP information to the UPF or UPF+PGW-U as LAC, such as LNS IP address or FQDN, as described in 3GPP TS 29.244 [58]. This L2TP information may be configured on the SMF or SMF+PGW-C as part of the DNN configuration or received from the DN-AAA server. Alternatively, the L2TP

tunnel parameters may be configured in the UPF or UPF+PGW-U. The L2TP tunnel parameters include necessary parameters for setting up L2TP tunnel towards the LNS (e.g. LNS address, tunnel password).

In addition, the SMF or SMF+PGW-C may provide PAP/CHAP authentication information to the UPF or UPF+PGW-U, for use in L2TP session establishment, in case it was received from the UE in the ePCO IE of the PDU Session Establishment Request.

When L2TP is to be used for a PDU Session, the SMF or SMF+PGW-C may select a UPF or UPF+PGW-U and requests the UE IP address to be allocated by LNS according to 3GPP TS 29.244 [58], the UPF (LAC) may retrieve this IP address from the LNS.

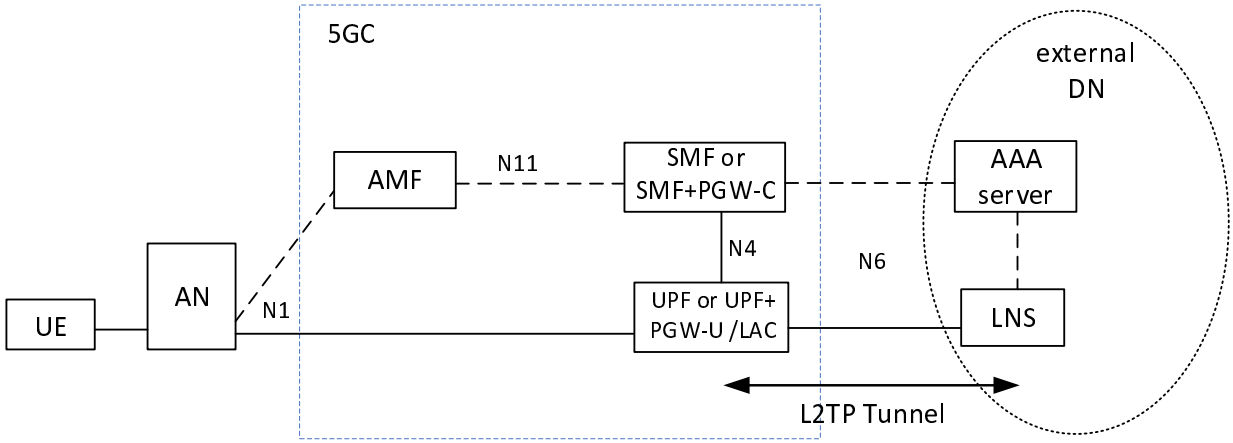

Figure 18.1-1: L2TP Tunnel between 5GC and external DN

Below figure describes the L2TP connection procedures between 5GC and external DN, upon the UE is accessed in 5GC and the SMF or SMF+PGW-C and UPF or UPF+PGW-U has been negotiated supporting L2TP feature.

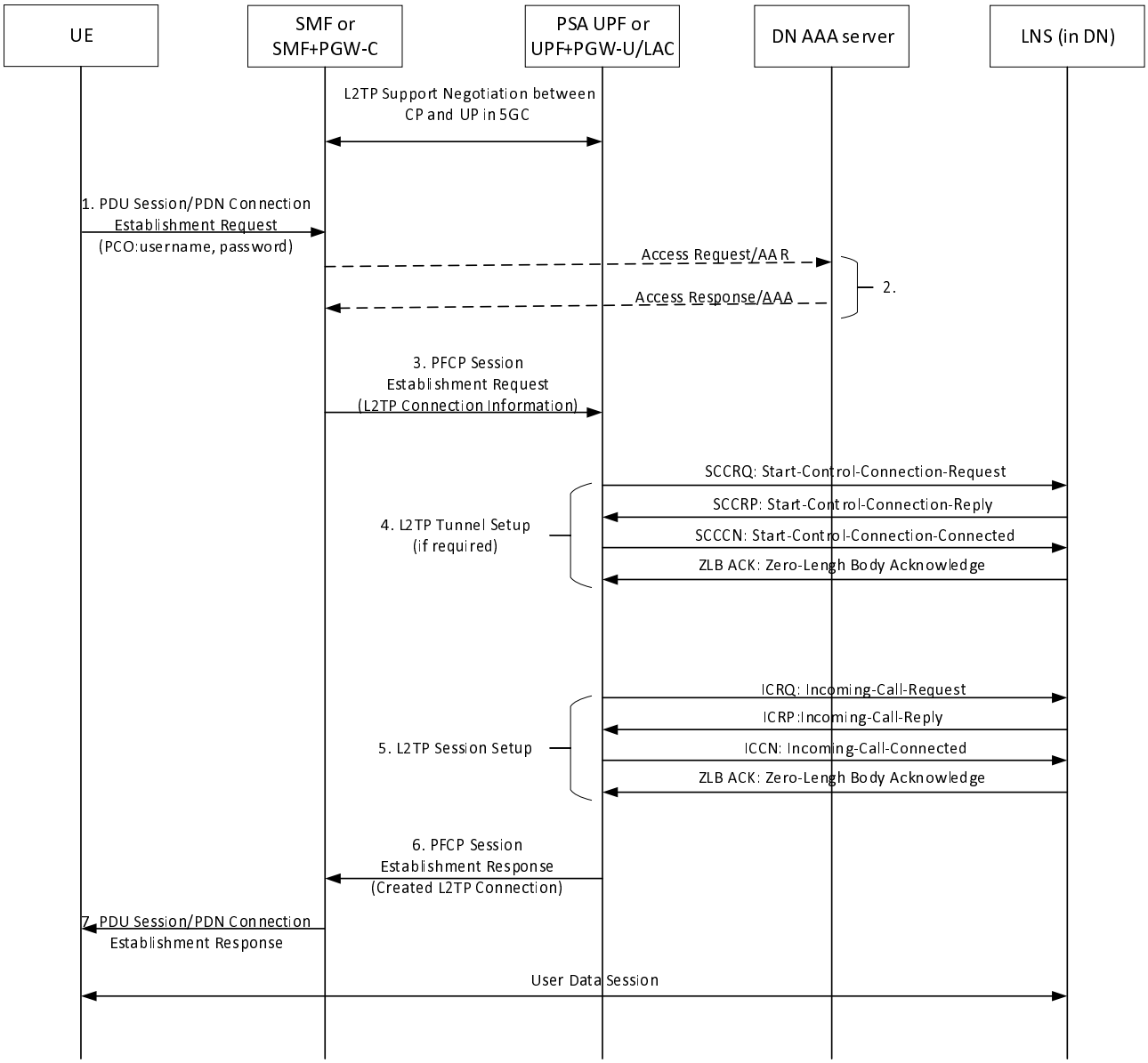

Figure 18.1-2: L2TP connection procedures between 5GC and external DN

0. The SMF or SMF+PGW-C and the UPF or UPF+PGW-U negotiated supporting L2TP feature as specified in 3GPP TS 29.244 [114].

1. The SMF or SMF+PGW-C receives a PDU Session or PDN Connection establishment request from the UE via AMF or MME and SGW.

   The UE may include the authentication information for PAP and/or CHAP in ePCO IE. The SMF or SMF+PGW-C may locally configure the UE authentication information for a given DNN.

   The SMF or SMF+PGW-C may determine that an L2TP session is required for the PDU Session based on local configured L2TP parameters per DNN.

2. The SMF or SMF+PGW-C may receive the L2TP Tunnel parameters (e.g. LNS IP address or FQDN, tunnel password) from the DN-AAA server in Access-Accept message or Diameter AAA message, or local configured.

NOTE: If EAP based secondary authentication is used (e.g. DER/DEA), L2TP Proxy Authenticate Extensions for EAP is not supported in this release of the specification.

3. If L2TP protocol is determined to support the PDU Session, the SMF or SMF+PGW-C selects a UPF or UPF+PGW-U supporting L2TP and be configured with the LAC name/addresses and then requests the UPF or UPF+PGW-U to setup an L2TP tunnel if needed and/or L2TP session towards the L2TP network server (LNS).

The SMF or SMF+PGW-C sends PFCP Session Establishment Request to the UPF or UPF+PGW-U, which may include L2TP Tunnel Information for setting up a L2TP tunnel and L2TP session information to setup a L2TP session, together with the information for authentication used during L2TP Tunnel setup, as well as for L2TP session.

The L2TP Tunnel Information includes LNS IPv4 address or IPv6 address of LNS, Tunnel Password.

The L2TP Session Information includes specific information related to the PDU Session, e.g. a Calling Number which may be set to UE's GPSI, an indication to instruct that the UPF or UPF+PGW-U shall request the LNS to allocate an IP address for the PDU Session, indications to instruct that the UPF or UPF+PGW-U shall request the LNS to provide DNS server addresses or NBNS server addresses etc. as specified in 3GPP TS 29.244 [114].

4. The UPF or UPF+PGW-U checks if any existing L2TP tunnel can be used to serve the PDU Session according to the information provided in the L2TP Tunnel Information.

   If the UPF or UPF+PGW-U decides to setup a new L2TP tunnel, it initiates L2TP Tunnel establishment by sending an SCCRQ (Start-Control-Connection-Request) message towards the LNS, the UPF or UPF+PGW-U will allocate a Tunnel ID, and it may include a CHAP Challenge to authenticate the LNS. The Challenge and Challenge Response (to be included in SCCCN) is produced by the UPF or UPF+PGW-U using the Tunnel Password received from the SMF or SMF+PGW-C.

   The LNS responds with an SCCRP (Start-Control-Connection-Reply) message, containing its allocated Tunnel ID and a CHAP Challenge Response to the Challenge in SCCRQ.

   The UPF or UPF+PGW-U then responds with a Challenge response for tunnel authentication in the SCCCN (Start-Control-Connection-Connected) message. An L2TP tunnel is established after the tunnel authentication is successful, with the reception of the SCCCN message sent by the LAC to the LNS.

   If the UPF or UPF+PGW-U decides to use an already existing L2TP tunnel for the requested PDU Session from the UPF or UPF+PGW-C, it proceeds with step 5 below directly without current step.

5. Once the L2TP Tunnel is established (or already present) between the LAC and the LNS for the PDU Session/PDN Connection requested by the UE, the UPF or UPF+PGW-U proceeds with L2TP session setup towards the LNS.

   The UPF or UPF+PGW-U sends an ICRQ (Incoming-Call-Request) message towards the LNS, which contains the Tunnel ID assigned by the LNS, its assigned Session ID, and optionally, the Calling Number and Called Number. The LNS responds with an ICRP (Incoming-Call-Reply) message and provides the Session ID assigned by it to the LAC.

   The LAC then sends an ICCN (Incoming-Call-Connected) message. If proxy LCP and authentication are employed, the ICCN message includes link control parameters (e.g. MRU) and the UE authentication information sent from the SMF or SMF+PGW-C which was received via ePCO IE in step 1. In addition, the UPF or UPF+PGW-U (LAC) will act as a PPP endpoint to use IPCP to request UE IP Address, DNS server address and/or NBNS server address(es).

   The LCP renegotiation may by triggered by the LNS after receiving the ICCN message. If so, the LAC and LNS will use PPP LCP to communicate link specific control parameter, and indicate authentication type, then either PPP PAP/CHAP takes place. The PPP IPCP transactions takes places to retrieve UE IP Address, DNS server address and/or NBNS server address.

6. The status of the L2TP session setup is sent by the UPF or UPF+PGW-U to the SMF or SMF+PGW-C in a PFCP Session Establishment Response.

7. The SMF or SMF+PGW-C sends a PDU Session Establishment Response to the UE and the user data session is initiated, which may contain the DNS and NBNS Server information.

19 Interworking with Credentials Hoder using AAA server

19.1 Credentials Holder using AAA server for primary authentication and authorization

The AUSF and the UDM in SNPN may support primary authentication and authorization of UEs using credentials from an AAA Server in a Credentials Holder (CH).

- Upon the UDM decides that the primary authentication is performed by AAA Server with credentials hoder and inform the AUSF that primary authentication by a AAA server in a CH is required, the AUSF shall discover and select the NSSAAF, and then forward EAP messages to the NSSAAF.
- The NSSAAF selects AAA Server based on the domain name corresponds to the realm part of the SUPI, relays EAP messages between AUSF and AAA Server (or AAA proxy) and performs related protocol conversion. The AAA server acts as the EAP Server for the purpose of primary authentication.

NOTE: The UDM in SNPN, based on SLA between Credentials Holder and SNPN, is pre-configured with information indicating whether the UE needs primary authentication from AAA server.

5G System architecture with access to SNPN using credentials from Credentials Holder using AAA Server and related functions are defined in clause 5.30.2.9 of 3GPP TS 23.501 [2].

19.2 Credentials Holder using AAA server for primary authentication procedure

The procedures described in this clause enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN.

In this scenario the authentication server role is taken by the AAA Server. The AUSF acts as EAP authenticator and interacts with the AAA Server to execute the primary authentication procedure.

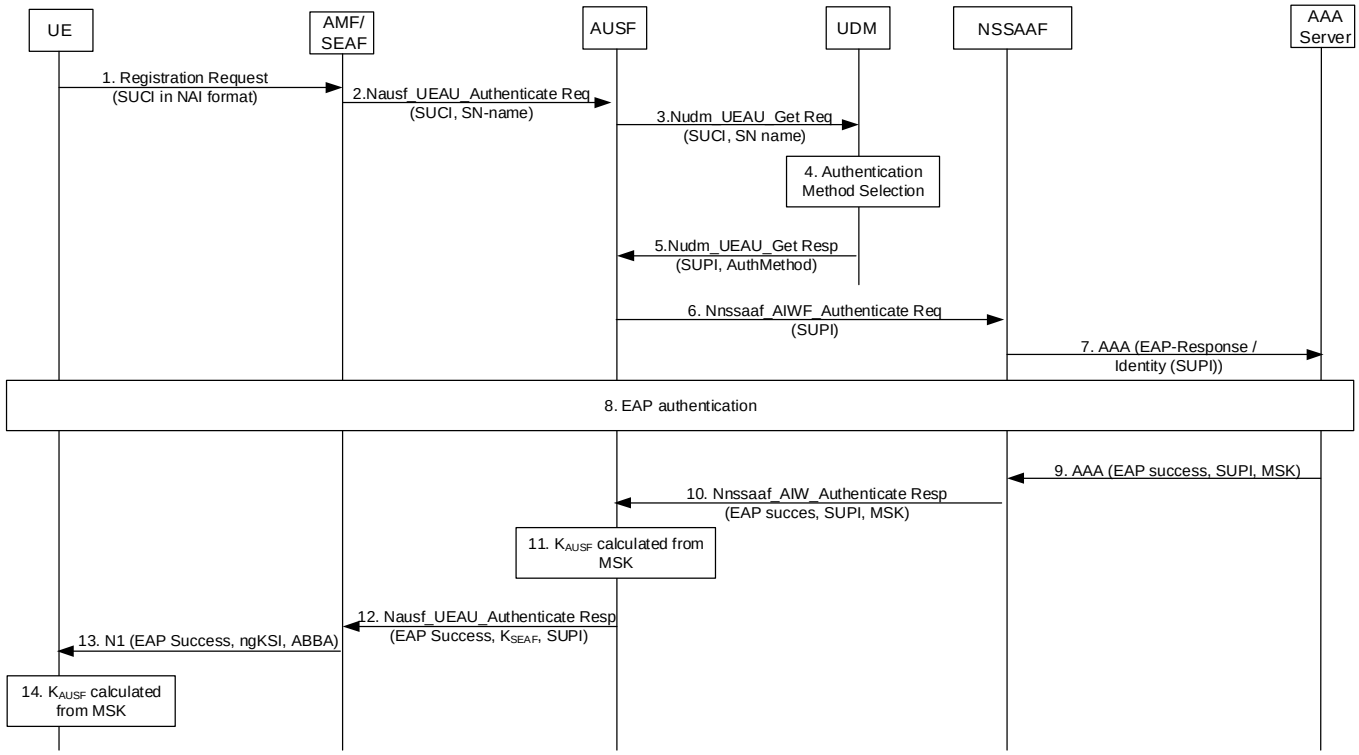

Figure 19.2-1: Primary authentication with external domain

The detail procedures description is defined in clause I.2.2.2 of 3GPP TS 33.501 [59].

Annex A (normative): Rate control related to 5G Cellular Internet of Things (CIoT) optimisations

A.1 General

The present annex defines specific requirements for rate control related to 5G CIoT optimisations.

A.2 Support of rate control of user data

A.2.1 General

The rate of user data sent to and from a UE (e.g. a UE using 5G CIoT Optimizations) can be controlled in two different ways:

- Serving PLMN rate control
- Small data rate control

Serving PLMN rate control is further described in 3GPP TS 23.501 [2].

Small data rate control allows HPLMN operators on per user to control the amount of user data sent DL and UL. This is done with help of policing user data on a maximum number of user data packets per time unit both DL and UL. Small data DL rate control policing is done in the UPF or the NEF and the small data UL rate control policing is done in the UE. The UPF or NEF can also do small data UL rate control policing.

For further information on small data rate control in the UE, see 3GPP TS 24.501 [42].

NOTE 1: Existing Session-AMBR mechanisms are not suitable for such a service since, for radio efficiency and UE battery life reasons, an AMBR of e.g. > 100kbit/s is desirable and such an AMBR translates to a potentially large daily data volume.

NOTE 2: For serving PLMN rate control and small data rate control, whether the UPF or the NEF is used for data policing depends on the CIoT Optimizations mode that UE and network support (CP or UP Optimizations) and the UE subscription data.

A.2.2 Small Data Rate Control

The small data rate control is configured in the (H-)SMF.

The small data rate control parameters, if configured, shall consist of:

- the maximum number of DL user data packets per time unit,
- the maximum number of UL user data packets per time unit, and
- the maximum number of additional UL exception reports per time unit.

Possible time units shall be, minute, hour, day or week.

If the small data rate control is supported by the UE as indicated in the Extended Protocol Configuration Options (ePCO) IE included in the PDU session establishment request and if the (H-)SMF is configured to use small data rate control, the (H-)SMF shall include the configured small data UL rate control parameters in the ePCO IE of the PDU session establishment reply, and send the configured small data DL rate control parameters and optionally the UL rate control parameters to the UPF or the NEF. The small data rate control parameters sent to UE, UPF or NEF may include

a remaining small data rate control with validity time information that shall be applied first before applying the configured small data rate control parameters.

NOTE 1: The (H-)SMF can receive small data rate control parameters from the AMF.

See 3GPP TS 24.501 [42] for ePCO IE definition.

If the small data UL rate control parameters are modified, the (H-)SMF shall initiate a PDU session modification procedure and include the small data UL rate control parameters in the ePCO IE. The (H-)SMF may also send the updated small data UL rate control parameters to the UPF or the NEF.

If the small data DL rate control parameters are modified, the (H-)SMF shall send the updated small data DL rate control parameters to the UPF or the NEF.

The UPF or the NEF shall enforce the small data DL rate control and may enforce the small data UL rate control per UE.

NOTE 2: The UE locally enforces this uplink small data rate control instruction. The UE considers this small data rate control instruction as valid until it receives a new one from the (H-)SMF.

A.2.3 Serving PLMN Rate Control information handling

The serving PLMN rate control is configured in the (V-)SMF and it applies per PDU session.

This rate control is operator configurable and expressed as "X NAS Data PDUs per deci hour" where X is an integer that shall not be less than 10. There are separate limits for uplink and downlink NAS Data PDUs:

If serving PLMN rate control information is received from the SMF, the UPF or the NEF shall store this information and use that for DL rate control enforcement for this UE.

The UE shall enforce the serving PLMN UL rate control based on the rate control information received from the (V-)SMF.

The (V-)SMF may also enforce the serving PLMN UL and/or DL rate control.

If the UPF or the NEF previously have received Serving PLMN rate control information, it shall behave as follows:

- If the UPF or the NEF receives new Serving PLMN rate control information from the SMF, it shall replace the old Serving PLMN rate control information with the new Serving PLMN rate control information and use that for DL rate control enforcement for this UE.
- If the UPF or the NEF receives no Serving PLMN rate control information from the SMF, it shall still consider the latest received Serving PLMN rate control information from the SMF as valid.
- If UPF or the NEF receives an indication that Serving PLMN rate control does not apply from the SMF, it shall remove the rate control information based on Serving PLMN rate control information.

Small data rate control, if configured, also applies for the same PDU session, see subclause A.2.2.

Annex B (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2017-10						TS skeleton of interworking between 5G Network and external Data Networks	0.0.0
2017-11	CT3#92	C3-175380				Update after CT3#92; inclusion of C3-175241, C3-175286, C3-175287, C3-175288, C3-175289.	0.1.0
2017-12	CT3#93	C3-176400				Update after CT3#93; TS number changed to 29.561 and inclusion of C3-176265, C3-176266.	0.2.0
2018-01	CT3#94	C3-180365				Update after CT3#94; inclusion of C3-180264, C3-180126, C3-180348, C3-180129, C3-180130.	0.3.0
2018-03	CT3#95	C3-181371				Update after CT3#95; inclusion of C3-181043, C3-181044, C3-181261, C3-181047, C3-181099.	0.4.0
2018-04	CT3#96	C3-182519				Update after CT3#96; inclusion of C3-182183, C3-182381, C3-182382, C3-182383.	0.5.0
2018-06	CT3#97	C3-183917				Update after CT3#97; inclusion of C3-183308, C3-183309, C3-183310, C3-183318, C3-183319, C3-183717, C3-183321, C3-183325, C3-183326, C3-183327, C3-183729.	0.6.0
2018-06	CT#80	CP-181027				TS sent to plenary for approval	1.0.0
2018-06	CT#80	CP-181027				TS approved by plenary	15.0.0
2018-09	CT#81	CP-182015	0001	2	F	Add multihoming support in IPv6 stateless address autoconfiguration	15.1.0
2018-09	CT#81	CP-182015	0002	1	F	IP address change	15.1.0
2018-09	CT#81	CP-182015	0003	1	F	MAC address change	15.1.0
2018-09	CT#81	CP-182015	0004	-	F	Final result of authentication/authorization from the DN-AAA – Receiving entity	15.1.0
2019-06	CT#84	CP-191188	0006	4	F	Correct session AMBR	15.2.0
2019-06	CT#84	CP-191070	0005	-	B	Rate control for 5G CIoT	16.0.0
2019-09	CT#85	CP-192150	0008		A	3GPP VSA presence for RADIUS	16.1.0
2019-09	CT#85	CP-192169	0010	1	B	Add DN-AAA re-authentication	16.1.0
2019-09	CT#85	CP-192150	0012		A	Correct DN-AAA authentication	16.1.0
2019-09	CT#85	CP-192150	0014	2	A	Correct DN-AAA authorization	16.1.0
2019-09	CT#85	CP-192137	0017	1	F	Correct small data rate control status	16.1.0
2019-09	CT#85	CP-192159	0018	2	B	IP address allocation via DHCP/AAA Server	16.1.0
2019-09	CT#85	CP-192152	0019	1	B	DN interworking of UPF for PIM	16.1.0
2019-12	CT#86	CP-193200	0022	1	B	Support Slice Specific authentication	16.2.0
2020-03	CT#87e	CP-200210	0023	2	B	Call flows of NSSAA procedures	16.3.0
2020-03	CT#87e	CP-200198	0024	-	F	Resolve editor note for PLMN rate control	16.3.0
2020-03	CT#87e	CP-200211	0025	-	F	IP address pool id encoding	16.3.0
2020-06	CT#88e	CP-201226	0027	1	A	Correct access challenge	16.4.0
2020-06	CT#88e	CP-201247	0028	-	B	Support secondary RAT data usage report	16.4.0
2020-06	CT#88e	CP-201236	0030	-	F	Replacing AUSF by NSSAAF to support NSSAA	16.4.0
2020-06	CT#88e	CP-201237	0031	-	F	IP address pool id in accounting and its IP version	16.4.0
2020-06	CT#88e	CP-201247	0033	1	F	Correct AMF and SMF address	16.4.0
2020-06	CT#88e	CP-201274	0034	1	B	Subscription trigger request UE IP address from DN-AAA server	16.4.0
2020-06	CT#88e	CP-201228	0035	1	B	Ipv6 Prefix Delegation via DHCPv6	16.4.0
2020-06	CT#88e	CP-201331	0036	1	F	Remove the feature for ip address pool	16.4.0
2020-09	CT#89e	CP-202057	0040	1	A	Correction to 3GPP-UE-MAC-Address	16.5.0
2020-09	CT#89e	CP-202057	0042	1	A	Correction on the authentication and authorization procedure	16.5.0
2020-09	CT#89e	CP-202057	0046	-	A	Correction to the Sesson-AMBR	16.5.0
2020-09	CT#89e	CP-202067	0049	-	F	Add missing applicable messages for IP pool info	16.5.0
2020-09	CT#89e	CP-202081	0048	1	F	List of allowed VLAN Ids within DN authorization data	16.5.0
2020-09	CT#89e	CP-202057	0054	-	A	Correction on the authorization data	16.5.0
2020-09	CT#89e	CP-202060	0055	-	F	RAT Type extension for 5WWC	16.5.0
2020-09	CT#89e	CP-202059	0056	-	F	User Location extension for 5WWC	16.5.0
2020-12	CT#90e	CP-203121	0060	-	A	Correction on the Acct-Session-Id	16.6.0
2020-12	CT#90e	CP-203143	0064	1	F	Correct SGSN address	16.6.0
2020-12	CT#90e	CP-203123	0066	1	F	Correct applicability for User Location extension	16.6.0
2020-12	CT#90e	CP-203150	0067	-	F	Correct network identifier for SNPN	16.6.0
2020-12	CT#90e	CP-203123	0069	-	F	Updates to IPv6 Prefix Delegation	16.6.0
2020-12	CT#90e	CP-203099	0072	2	A	Correction on PAP/CHAP supporting Rel-15 N1 mode UE	16.6.0
2020-12	CT#90e	CP-203134	0058	1	B	Adding a note for IPv4/IPv6 Non-transparent access to DN using PAP/CHAP	17.0.0
2020-12	CT#90e	CP-203134	0061	1	B	Adding PAP/CHAP in RADIUS message flow(successful case)	17.0.0
2020-12	CT#90e	CP-203134	0062	1	B	Adding PAP/CHAP in Diameter message flow(successful case)	17.0.0
2020-12	CT#90e	CP-203144	0068	-	F	Corrections to IPv6	17.0.0
2020-12	CT#90e	CP-203147	0070	1	F	Corrections on SMF directly connecting DN-AAA server	17.0.0

2021-03	CT#91e	CP-210226	0076	1	B	Interworking scenario support	17.1.0
2021-03	CT#91e	CP-210226	0077	1	B	Reporting Session S-NSSAI to RADIUS DN-AAA server	17.1.0
2021-03	CT#91e	CP-210226	0078	1	B	Reporting Session S-NSSAI to Diameter DN-AAA server	17.1.0
2021-03	CT#91e	CP-210227	0079	3	B	Reporting FQDN of CHF to RADIUS DN-AAA server	17.1.0
2021-03	CT#91e	CP-210227	0080	1	B	Reporting FQDN of CHF to Diameter DN-AAA server	17.1.0
2021-03	CT#91e	CP-210226	0081	1	B	Reporting FQDN of Serving NF to RADIUS DN-AAA server	17.1.0
2021-03	CT#91e	CP-210226	0082	-	B	Report FQDN of Serving NF to Diameter DN-AAA server	17.1.0
2021-03	CT#91e	CP-210214	0083	2	F	Update descriptions for PAP/CHAP in RADIUS message flow	17.1.0
2021-03	CT#91e	CP-210214	0084	2	F	Update descriptions for PAP/CHAP in Diameter message flow	17.1.0
2021-03	CT#91e	CP-210214	0085	1	B	5GS interworking with EPS for IPv4IPv6 Non-transparent access using PAPCHAP	17.1.0
2021-03	CT#91e	CP-210241	0088	1	B	5GS interworking with EPS for EAP based secondary AUTH in RADIUS message flow	17.1.0
2021-03	CT#91e	CP-210241	0089	1	B	5GS interworking with EPS for EAP based secondary AUTH in Diameter message flow	17.1.0
2021-03	CT#91e	CP-210214	0090	1	F	Update clarification for PAP/CHAP in RADIUS message flow	17.1.0
2021-03	CT#91e	CP-210214	0091	1	F	Update clarification for PAP/CHAP in Diameter message flow	17.1.0
2021-03	CT#91e	CP-210228	0092	1	B	5GC Support of DHCP signalling for RG	17.1.0
2021-03	CT#91e	CP-210202	0093	1	A	Reporting GCI to RADIUS DN-AAA server	17.1.0
2021-03	CT#91e	CP-210202	0094	1	A	Reporting GCI to Diameter DN-AAA server	17.1.0
2021-06	CT#92e	CP-211211	0097	1	F	Clarification of accounting for the interworking scenario	17.2.0
2021-06	CT#92e	CP-211211	0102	1	B	Updates 5GS interwroking with EPS for EAP based re-auth in Diameter message flow	17.2.0
2021-06	CT#92e	CP-211209	0105	1	A	Correction to Framed IP	17.2.0
2021-06	CT#92e	CP-211211	0106	1	F	Complete AAA triggered re-authentication flow for Diameter	17.2.0
2021-06	CT#92e	CP-211280	0107	3	B	Updates to support L2TP for CUPS	17.2.0
2021-06	CT#92e	CP-211280	0108	2	B	Updates to support L2TP in RADIUS message flow	17.2.0
2021-06	CT#92e	CP-211280	0109	2	B	Updates to support L2TP in Diameter message flow	17.2.0
2021-06	CT#92e	CP-211211	0110	1	F	Correction to Framed Route information	17.2.0
2021-06	CT#92e	CP-211281	0111	1	B	Adding support for providing L2TP information through N6 interface	17.2.0
2021-06	CT#92e	CP-211244	0112	1	B	Reporting UE local IP to RADIUS DN-AAA server	17.2.0
2021-06	CT#92e	CP-211244	0113	1	B	Reporting UE local IP to Diameter DN-AAA server	17.2.0
2021-09	CT#93e	CP- 212197	0116	1	B	L2TP information provision	17.3.0
2021-09	CT#93e	CP-212197	0119		F	Fix L2TP procedure	17.3.0
2021-09	CT#93e	CP-212216	0121	-	F	Correct PAP/CHAP description	17.3.0
2021-09	CT#93e	CP-212224	0122	-	F	Fix DN-AAA initiated re-authentication	17.3.0
2021-09	CT#93e	CP-212224	0123	1	F	Addressing impersonate attack from AAA-S	17.3.0
2021-09	CT#93e					Notes and editor notes formatting issues fixed	17.3.1
2021-12	CT#94e	CP-213243	0124	1	B	Reporting DNAI to RADIUS DN-AAA server	17.4.0
2021-12	CT#94e	CP-213243	0125	1	B	Reporting DNAI to Diameter DN-AAA server	17.4.0
2022-03	CT#95e	CP-220206	0127		B	Accounting correlation for redundant transmission	17.5.0
2022-03	CT#95e	CP-220196	0128		F	Correct 3GPP-Session-Id	17.5.0
2022-03	CT#95e	CP-220208	0129		B	Update the 3GPP-RAT-Type AVP to support NR RedCap access type	17.5.0
2022-03	CT#95e	CP-220182	0130		B	Interworking with CH using AAA server	17.5.0

History

Document history		
V17.5.0	May 2022	Publication