ETSI TS 129 273 V17.6.0 (2023-04)

Universal Mobile Telecommunications System (UMTS);
LTE;
5G;
Evolved Packet System (EPS);
3GPP EPS AAA interfaces
(3GPP TS 29.273 version 17.6.0 Release 17)

Reference
RTS/TSGC-0429273vh60

Keywords
5G,LTE,UMTS

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

The present specification details the stage 3 work related to all 3GPP AAA reference points used by the different non-3GPP accesses included in EPS. It also details the stage 3 work related to the SWa reference point used for Non-seamless WLAN offload (NSWO) in 5GS.

1 Scope

The present document defines the stage-3 protocol description for several reference points for the non-3GPP access in EPS:

- The SWa reference point between an un-trusted non-3GPP IP access and the 3GPP AAA Server/Proxy.
- The STa reference point between a trusted non-3GPP IP access and the 3GPP AAA Server/Proxy.
- The SWd reference point between the 3GPP AAA Proxy and 3GPP AAA Server.
- The SWx reference point between the 3GPP AAA Server and the HSS.
- The S6b reference point between the 3GPP AAA Server/Proxy and the PDN GW.
- The SWm reference point between the 3GPP AAA Server/Proxy and the ePDG.
- The reference point between the 3GPP AAA Server/Proxy and the EIR.

The present document also defines the stage 3 protocol description for the following reference points defined for Non-seamless WLAN offload in 5GS:

- the SWa' reference point between a non-3GPP WLAN access, possibly via a 3GPP AAA Proxy, and the NSWO NF; and
- the SWd' reference point between the 3GPP AAA Proxy, possibly via an intermediate 3GPP AAA Proxy, and the NSWO NF.

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] IETF RFC 5779: "Diameter Proxy Mobile IPv6: Mobility Access Gateway and Local Mobility Anchor Interaction with Diameter Server ".

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

[4] IETF RFC 4005: "Diameter Network Access Server Application"

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

[6] IETF RFC 5447 "Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction".

[7] Void.

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

[9] IETF RFC 5777: "Traffic Classification and Quality of Service (QoS) Attributes for Diameter".

[10] Void

[11] IETF RFC 5778: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction".

[12] Void

[13] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6; Stage 3".

[14] 3GPP TS 23.003: "Numbering, addressing and identification".

[15] IETF RFC 4282: "The Network Access Identifier".

[16] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[17] 3GPP TS 29.230: "Diameter applications; 3GPP specific codes and identifiers".

[18] IETF RFC 4004: "Diameter Mobile IPv4 Application".

[19] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[20] IETF RFC 4006: "Diameter Credit-Control Application".

[21] Void.

[22] 3GPP TS 29.228: "IP multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and Message Elements".

[23] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[24] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol; Protocol details".

[25] 3GPP2 X. S0057-B: "EUTRAN – eHRPD Connectivity and Interworking: Core Network Aspects".

[26] 3GPP TS 24.302: "Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks".

[27] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[28] IETF RFC 6611: "Mobile IPv6 (MIPv6) Bootstrapping for the Integrated Scenario".

[29] 3GPP TS 29.272: "Evolved Packet System; MME and SGSN Related Interfaces Based on Diameter Protocol".

[30] 3GPP TS 32.299: "Charging management; Diameter charging applications".

[31] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[32] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

[33] Void.

[34] 3GPP TS 29.303: "Domain Name System Procedures; Stage 3".

[35] IETF RFC 1035: "Domain Names - Implementation and Specification".

[36] Void.

[37] IETF RFC 5729: "Clarifications on the Routing of Diameter Requests Based on the Username and the Realm".

[38] 3GPP TS 29.274: "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunnelling Protocol for Control plane (GTPv2-C); Stage 3".

[39] 3GPP TS 23.139: "3GPP System-Fixed Broadband Access Network Interworking; Stage 2".

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

[41] Void.

[42] Void.

[43] 3GPP TS 24.139: "3GPP system - fixed broadband access network interworking".

[44] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[45] 3GPP TS 23.203: "Policy and Charging Control Architecture".

[46] IETF RFC 5580: "Carrying Location Objects in RADIUS and Diameter".

[47] IETF RFC 7683: "Diameter Overload Indication Conveyance".

[48] ETSI TS 283 034: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Sub-System (NASS); e4 interface based on the DIAMETER protocol".

[49] 3GPP TS 23.008: "Organization of subscriber data".

[50] Void

[51] Void

[52] 3GPP TS 23.380: "IMS Restoration Procedures".

[53] IETF RFC 7944: "Diameter Routing Message Priority".

[54] IETF RFC 8583: "Diameter Load Information Conveyance".

[55] IETF RFC 6696: "EAP Extensions for the EAP Re-authentication Protocol (ERP)".

[56] IETF RFC 6734: "Diameter Attribute-Value Pairs for Cryptographic Key Transport".

[57] IETF RFC 6942: "Diameter Support for the EAP Re-authentication Protocol (ERP)".

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

[59] 3GPP TS 23.501: "System Architecture for the 5G System".

[60] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

3 Definitions, symbols and abbreviations

3.1 Definitions

3.1.1 General

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].

Multi-connection mode (MCM): see definition in clause 3.1 of 3GPP TS 23.402 [3].

Non-Seamless WLAN offload (NSWO): Non-Seamless Non-3GPP offload when the access network is WLAN.

Single-connection mode (SCM): see definition in clause 3.1 of 3GPP TS 23.402 [3].

Transparent single-connection mode (TSCM): see definition in clause 3.1 of 3GPP TS 23.402 [3].

Trusted WLAN Identifier (TWID): Identifier of a given Trusted WLAN, a combination of, e.g., an SSID and/or an HESSID as defined in IEEE Std 802.11-2012 [40].

3.1.2 Handling of Information Elements

In the tables that describe the Information Elements transported by each Diameter command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional in the Category "Cat." column. For the correct handling of the Information Elements and their precedence to any included ABNF definition of the command as defined according to their category types, see the description detailed in clause 6 of the 3GPP TS 29.228 [22].

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].

AE	Authentication Extension
DRMP	Diameter Routing Message Priority
DSCP	Differentiated Services Code Point
EIR	Equipment Identity Register
EPC	Evolved Packet Core
ER	EAP Re-authentication
ERP	EAP Re-Authentication Protocol
ePDG	Evolved Packet Data Gateway
eHRPD	evolved High Rate Packet Data
FA	Foreign Agent
FACoA	FA Care-of-Address
HA	Home Agent
HBM	Host Based Mobility
HESSID	Homogenous Extended Service Set Identifier
HSGW	eHRPD Serving Gateway
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MIPv4	Mobile IP version 4
MN	Mobile Node
NBM	Network Based Mobility
NAS	Network Access Server
NSWO	Non-Seamless WLAN offload
NSWOF	Non-Seamless WLAN offload Function
PBU	Proxy Binding Update
PDN GW	PDN Gateway
PGW	PDN Gateway, the abbreviation of PDN GW
PMIP/PMIPv6	Proxy Mobile IP version 6
RRP	MIPv4 Registration Reply
RRQ	MIPv4 Registration Request
SA	Security Association
SGW	Serving Gateway
SIPTO	Selected IP Traffic Offload
SSID	Service Set Identifier
TWAN	Trusted WLAN Access Network
WLCP	Wireless LAN Control Plane Protocol

4 SWa and SWa' Description

4.1 Functionality

4.1.1 General

The SWa reference point is defined between the untrusted non-3GPP IP access and the 3GPP AAA Server or Proxy in EPS. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

The SWa reference point is optionally used to authenticate and authorize the UE for the access to the EPS. It is up to the non-3GPP operator's policy whether this interface and the procedures defined in this clause are used.

NOTE: From the EPS operator's view, the tunnel authentication and authorization procedures described in clause 7 (SWm description) and clause 9 are required to ensure the user's authentication and authorization when the UE is attached to an untrusted non-3GPP IP access.

The same procedures as defined for STa reference points are used also in the SWa, but with reduced message content. As an exception, the service authorization information update procedure is not applicable for the SWa reference point.

The SWa' reference point is defined between the non-3GPP WLAN access, possibly via a 3GPP AAA Proxy, and the NSWOF in 5GS. The definition of the reference point and its functionality is given in clause 4.2.15 of 3GPP TS 23.501 [59] and Annex S of 3GPP TS 33.501 [60]. It reuses the same stage 3 protocol definition as defined for SWa in EPC, with specific requirements for NSWO in 5GS specified in clause 4.1.2.5.

4.1.2 Procedure Descriptions

4.1.2.1 SWa Authentication and Authorization procedure

4.1.2.1.1 General

This procedure follows the STa Authentication and Authorization procedure, with the following differences:

- Information elements that would reflect information about the user's service request and about the access network are not included or are optional in the authentication and authorization request.
- The information elements that describe the user's subscription profile are not downloaded to the non-3GPP access network.

NOTE: The information elements related to the IP Mobility Mode Selection function are not supported over this interface.

Table 4.1.2.1/1: SWa Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in the IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
UE Layer-2 address	Calling-Station-ID	M	This IE shall carry the Layer-2 address of the UE.
Access Type	RAT-Type	C	If present, this IE shall contain the untrusted non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	O	If present, this IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values) It shall be included if the non-3GPP access network selects the EAP-AKA' authentication method.
Full Name for Network	Full-Network-Name	O	If present, this IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network
Short Name for Network	Short-Network-Name	O	If present, this IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network
Transport Access Type	Transport-Access-Type	C	For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see clause 5.2.3.19).
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the non-3GPP access network has determined that a previously assigned 3GPP AAA Server is unavailable.
WLAN Location Information	Access-Network-Info	O	If present, this IE shall contain the location information of the WLAN Access Network where the UE is attached.
WLAN Location Timestamp	User-Location-Info-Time	O	This IE may be present if the WLAN Location Information IE is present. When present, this IE shall contain the NTP time at which the UE was last known to be in the location reported in the WLAN Location Information.

Table 4.1.2.1/2: SWa Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP payload	M	This IE shall contain the Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. Result codes are as in Diameter base protocol (see IETF RFC 6733 [58]). Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER _SUCCESS. If present, it shall contain the maximum number of seconds the user session is allowed to remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS.
3GPP AAA Server URI	Redirect-Host	C	This information element shall be present if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Trust Relationship Indicator	AN-Trusted	M	This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted or untrusted. For the SWa case, the value "UNTRUSTED" shall be used.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
Permanent User Identity	Mobile-Node-Identifier	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS and if the Transport Access Type in the request command indicated that the UE is accessing the EPC from a Fixed Broadband access network (i.e., the Transport-Access-Type AVP takes the value "BBF"); it shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used by the non-3GPP access network in subsequent PCC procedure for identifying the user in the EPS network. This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.

4.1.2.1.2 3GPP AAA Server Detailed Behaviour

The detailed behaviour of the 3GPP AAA Server follows the behaviour defined for the STa Authentication and Authorization procedure (refer to clause 5.1.2.1.2), with the following deviations:

- The 3GPP AAA Server shall handle the non-3GPP access network as untrusted.

- The 3GPP AAA Server marks the trust relationship as "untrusted" with the User Identity.

- The authentication method shall be selected based on the presence of the Access Network Identity as specified in 3GPP TS 33.402 [19]: if this information element is present, the EAP-AKA' method as specified in IETF RFC 5448 [27] is used; otherwise, the EAP-AKA method as specified in IETF RFC 4187 [44] is used.

When a WLAN Access Network provides WLAN Location Information to the 3GPP AAA Server that it considers as network provided location, the 3GPP AAA Server should store this information for the duration of the WLAN session of the UE, along with the WLAN Location Timestamp if received from the WLAN Access Network, or with the timestamp at which the WLAN Location Information is received from the WLAN Access Network, and provide it to the ePDG during a subsequent Authentication and Authorization procedure or Authorization procedure over the SWm reference point (see clauses 7.1.2.1.2 and 7.1.2.2.2).

The 3GPP AAA Server shall delete any stored WLAN Location Information and WLAN Location Timestamp associated with the UE when a WLAN Access Network provides WLAN Location Information to the 3GPP AAA Server that it does not consider as network provided location.

NOTE: It is up to local 3GPP AAA Server policies to decide whether the location information received from the WLAN access network can be considered as network provided location.

4.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The detailed behaviour of the 3GPP AAA Proxy follows the behaviour defined for the STa Authentication and Authorization procedure (refer to clause 5.1.2.1.3), with the following exception:

- The 3GPP AAA Proxy shall insert or overwrite Visited-Network-Identifier AVP before forwarding the request to the 3GPP AAA Server.

NOTE: If the untrusted WLAN is operated by the VPLMN's equivalent PLMN, the 3GPP AAA proxy can receive the Visited-Network-Identifier AVP from the Authentication and Authorization Request message.

- The 3GPP AAA Proxy shall handle the non-3GPP access network as untrusted and marks the trust relationship as "untrusted".

On receipt of the authentication and authorization answer that completes a successful authentication, the 3GPP AAA Proxy shall record the authentication state of the user.

4.1.2.2 SWa HSS/AAA Initiated Detach

This procedure equals with the STa HSS/AAA Initiated Detach procedure, refer to clause 5.1.2.2.

The 3GPP AAA Server shall delete any stored WLAN Location Information and WLAN Location Timestamp associated with the UE when it becomes aware that the WLAN session of the UE is terminated.

4.1.2.3 SWa Non-3GPP Access Network Initiated Detach

This procedure equals with the STa Non-3GPP Access Network Initiated Detach procedure, refer to clause 5.1.2.4.

The 3GPP AAA Server shall delete any stored WLAN Location Information and WLAN Location Timestamp associated with the UE when it becomes aware that the WLAN session of the UE is terminated.

4.1.2.4 SWa Re-Authentication and Re-Authorization Procedure

4.1.2.4.1 General

This procedure is optional and it may be invoked by the 3GPP AAA Server, if the operator policies require that the re-authentication of the user for the SWa is to be renewed and the untrusted non-3GPP access network supports the re-authentication.

This procedure shall be performed in two steps:

- The 3GPP AAA server shall issue an unsolicited re-auth request towards the untrusted non-3GPP access, indicating that both re-authentication and re-authorization of the user is needed. Upon receipt of such a

request, the untrusted non-3GPP access shall respond to the request and shall indicate the disposition of the request. This procedure is mapped to the Diameter command codes Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 6733 [58]. Information element contents for these messages shall be as shown in tables 4.1.2.4.1/1 and 4.1.2.4.1/2.

- Upon receiving the re-auth request, the untrusted non-3GPP access shall immediately invoke the SWa authentication and authorization procedure requesting the identity of the user via EAP and using DER/DEA commands, with the same session-ID but the content adapted to the needs of a re-authentication. Information element contents for these messages shall be as shown in tables 4.1.2.4.1/3 and 4.1.2.4.1/4.

  If the re-authentication of the user is not successful, the untrusted non-3GPP access shall detach the user.

Table 4.1.2.4.1/1: SWa Re-auth request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Re-Auth Request Type	Re-Auth–Request-Type	M	This information element shall define whether the user is to be authorized only or authenticated and authorized. AUTHORIZE_AUTHENTICATE shall be used in this case.
Routing Information	Destination-Host	M	This information element shall be obtained from the Origin-Host AVP, which was included in a previous command received from the untrusted non-3GPP access.

Table 4.1.2.4.1/2: SWa Re-auth response

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter Base Protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP and the error code in the Experimental-Result-Code AVP.

Table 4.1.2.4.1/3: SWa Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.

Table 4.1.2.4.1/4: SWa Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP payload	O	If present, this IE shall contain the Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. Result codes are defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	If present, this IE shall contain the maximum number of seconds the user session should remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be sent if Result-Code AVP is set to DIAMETER_SUCCESS.

4.1.2.4.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall trigger this procedure according to the local policies configured by the operator.

The 3GPP AAA Server shall use the same authentication method that was used during the full authentication executed at the UE's attach. If EAP-AKA' is used, the 3GPP AAA Server shall use the ANID parameter received during the authentication and authorization executed at the UE attach (refer to clause 4.1.2.1.1).

4.1.2.4.3 3GPP AAA Proxy Detailed Behaviour

The detailed behaviour of the 3GPP AAA Proxy follows the behaviour defined for the STa Re-Authorization and Re-Authentication Procedures (refer to clause 5.1.2.3.3), with the following addition:

- When forwarding the authorization answer or the authentication and authorization answer, the 3GPP AAA Proxy shall record the authentication state of the user.

4.1.2.5 SWa procedures for NSWO in 5GS

The SWa' interface between the non-3GPP WLAN access, possibly via a 3GPP AAA Proxy, and the NSWOF shall use the same stage 3 protocol definition as for the SWa interface in EPS, with the following modifications:

- SWa' Authentication and Authorization procedure:

  - The User Identity IE in the SWa' Authentication and Authorization Request and in the SWa' Authentication and Authorization Response shall contain the SUCI in NAI form as defined in clause 28.7.3 of 3GPP TS 23.003 [14]. In NSWO roaming scenario with a 3GPP AAA Proxy in the VPLMN (see clause 4.2.15 of 3GPP TS 23.501 [59]), the SUCI in NAI form shall be decorated as defined in clause 28.7.9 of 3GPP TS 23.003 [14] to enable the routing of SWa' signalling towards the 3GPP AAA Proxy in the VPLMN selected by the UE.

NOTE 1: This IE does not contain any leading digit to differentiate between authentication schemes.

NOTE 2: The realm in the SUCI in NAI form (starting by the first label "5gc-nswo") enables to route the signaling towards an NSWOF, as opposed to sending it to a 3GPP AAA Server, if the non-3GPP WLAN access also supports SWa signaling with a 3GPP AAA Server e.g. for a 4G subscriber.

  - EAP-AKA' as specified in RFC 5448 [27] shall be used as the authentication method.

- The NSWOF shall behave as specified in Annex S of 3GPP TS 33.501 [60]. The NSWOF shall send the MSK received from the AUSF in the Pairwise Master Key IE in the SWa' Authentication and Authorization Answer.

- The SWa HSS/AAA Initiated Detach, SWa Non-3GPP Access Network Initiated Detach and SWa Re-authentication and Re-Authorization are not supported.

4.2 Protocol Specification

4.2.1 General

The SWa reference point shall use the same Diameter application as the STa reference point. The first authentication command exchange (DER/DEA) is common between the SWa and STa reference points. During this initial exchange, the 3GPP AAA Server determines the HPLMN's trust relationship with the non-3GPP access network and communicates it to the non-3GPP access network and the UE as described in clause 5.1.2.1.2. The contents of the subsequent commands are dependent on this trust relationship determination and are specific to the SWa or STa reference points.

4.2.2 Commands

4.2.2.1 Commands for SWa authentication and authorization procedures

4.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the 'R' bit set in the Command Flags field, is sent from a trusted non-3GPP access network to a 3GPP AAA Server.

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY >
                             < Session-Id >
                             [ DRMP ]
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             { Auth-Request-Type }
                             { EAP-Payload }
                             [ User-Name ]
                             [ Calling-Station-Id ]
                             [ RAT-Type ]
                             …
                             [ ANID ]
                             [ Full-Network-Name ]
                             [ Short-Network-Name ]
                             *[ Supported-Features ]
                             [ AAA-Failure-Indication ]
                             [ Transport-Access-Type ]
                             [ OC-Supported-Features ]
                             [ Access-Network-Info ]
                             [ User-Location-Info-Time ]
                             …
                             *[ AVP ]
```

4.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the 'R' bit cleared in the Command Flags field, is sent from a 3GPP AAA Server to a trusted non-3GPP access network NAS.

```
< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY >
```

< Session-Id >
[DRMP]
{ Auth-Application-Id }
{ Result-Code }
[Experimental-Result]
{ Origin-Host }
{ Origin-Realm }
{ Auth-Request-Type }
[EAP-Payload]
[User-Name]
[Session-Timeout]
[Accounting-Interim-Interval]
[EAP-Master-Session-Key]
*[Redirect-Host]
[AN-Trusted]
*[Supported-Features]
[Mobile-Node-Identifier]
[OC-Supported-Features]
[OC-OLR]
*[Load]
…
*[AVP]

4.2.2.2 Commands for SWa HSS/AAA Initiated Detach

Refer to clause 5.2.2.2.

4.2.2.3 Commands for Untrusted non-3GPP Access network Initiated Session Termination

Refer to clause 5.2.2.4.

4.2.2.4 Commands for SWa Re-Authentication and Re-Authorization Procedures

4.2.2.4.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command, indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, shall be sent from a 3GPP AAA server to an untrusted non-3GPP access network NAS. ABNF for the RAR command shall be as follows:

< Re-Auth-Request > ::= < Diameter Header: 258, REQ, PXY, 16777250 >
< Session-Id >
[DRMP]
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
{ Re-Auth-Request-Type }
[User-Name]
…
*[AVP]

4.2.2.4.2 Re-Auth-Answer (RAA) Command

The Diameter Re-Auth-Answer (RAA) command, indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field, shall be sent from an untrusted non-3GPP access network NAS to a 3GPP AAA server. ABNF for the RAA command shall be as follows:

```
< Re-Auth-Answer > ::=  < Diameter Header: 258, PXY, 16777250 >
                        < Session-Id >
                        [ DRMP ]
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        …
                        *[ AVP ]
```

4.2.2.4.3 Diameter-EAP-Request (DER) Command

Refer to clause 4.2.2.1.1.

4.2.2.4.4 Diameter-EAP-Answer (DEA) Command

Refer to clause 4.2.2.1.2

4.2.3 Information Elements

The information elements of SWa are the same as the IEs defined for the STa interface described in the clause 5.2.3.

4.2.4 Session Handling

The session handling for the SWa interface is the same as the STa session handling described in the clause 5.2.4.

5 STa Description

5.1 Functionality

5.1.1 General

The STa reference point is defined between a non-3GPP access network and the 3GPP AAA Server or between a non-3GPP access network and the 3GPP AAA Proxy. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

Whether a Non-3GPP access network is Trusted or Untrusted is not a characteristic of the access network; this decision shall be made during the access authentication and authorization procedure executed between the non-3GPP access network and the 3GPP AAA Server. This is implemented by the STa and SWa reference points sharing the same Diameter application and partly sharing the same authentication and authorization procedure. The STa and SWa reference points are clearly distinguished after the exchange of the first authentication and authorization messages, during which trusted/untrusted decision is made by the 3GPP AAA server and this decision is communicated to the non-3GPP access network. The other procedures are specific to the STa and SWa reference points.

The STa reference point shall be used to authenticate and authorize the UE.

The STa reference point may also be used to transport PMIPv6, GTPv2, or MIPv4 FA-CoA mode related mobility parameters in a case the UE attaches to the EPC using the S2a reference point. The procedures specified for EPC access via GTP based S2a are only applicable to trusted WLAN access networks (see clause 16 of 3GPP TS 23.402 [3]).

Additionally the STa reference point may also be used to transport DSMIPv6 related mobility parameters in case the UE attaches to the EPC using the S2c reference point. In particular, in this case the STa reference point may be used for conveying the Home Agent IP address or FQDN from the AAA server to the gateway of the trusted non-3GPP access for Home Agent discovery based on DHCPv6 (see TS 24.303 [13]).

This reference point shall be also used to transport charging-related information and optionally information about IP Mobility Mode Selection.

5.1.2 Procedures Description

5.1.2.1 STa Access Authentication and Authorization

5.1.2.1.1 General

These procedures are transported over Diameter, the Access (Re-)Authentication and Authorization between the trusted non-3GPP access network and the 3GPP AAA Proxy or Server. The STa interface and Diameter application shall be used for authenticating and authorizing the UE for EPC access in PMIPv6, GTPv2, MIPv4 FA-CoA mode or for TWAN access without EPC S2a access (i.e. non-seamless WLAN offload) via trusted non-3GPP accesses and non-3GPP accesses that are decided to be untrusted during the authentication and authorization procedure.

When EAP-AKA' is used in the STa access authentication and either EPC access in NBM (PMIPv6 or GTPv2) or TWAN access without EPC S2a access (i.e. non-seamless WLAN offload) is used, the trusted non-3GPP access network shall support also the role of the NAS. Specifically, in the case where PMIPv6 is used, the network element of the non-3GPP access network acting as a MAG shall have also the role of the NAS. During the STa access authentication the NAS shall serve as pass-through EAP authenticator.

Diameter usage over the STa interface:

- When EAP is used, the trusted non-3GPP access authentication and authorization procedure shall be mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in IETF RFC 4072 [5].

- For (re)authentication procedures, the messaging described below shall be reused.

During the STa Access Authentication and Authorization procedure the non-3GPP access network may provide information on its PMIPv6 or GTPv2 capabilities to the 3GPP AAA Server.

During the STa Access Authentication and Authorization procedure the trusted non-3GPP access network shall provide information on the Access Network Identity (ANID) to the 3GPP AAA Server. Specifically, the TWAN shall set the Access Network Identity as specified in clause 8.1.1.2 of 3GPP TS 24.302 [26] for a WLAN access network.

For a trusted non-3GPP access, the 3GPP AAA Server may perform IP mobility mode selection between NBM and HBM. The 3GPP AAA Server may provide to the trusted non-3GPP access network an indication if either NBM or local IP address assignment (for HBM) shall be used.

For a trusted WLAN access,

- the TWAN should send information on whether it supports TSCM, SCM or MCM or any combination of them to the 3GPP AAA Server as specified in 3GPP TS 23.402 [63]. If it indicates support of the MCM, the TWAN shall also provide the 3GPP AAA Server with the TWAG's control plane IPv4 address, or IPv6 address or both (if it supports both IPv4 and IPv6), to be sent to the UE and used for WLCP if the MCM is selected.

- if the user is successfully authenticated and authorized for this access, the 3GPP AAA Server:

  - shall select either TSCM, SCM or MCM and indicate to the TWAN the selected mode of operation. If the 3GPP AAA Server does not provide such an indication, the TSCM shall be used;

  - may either only authorize the user to access to EPC via S2a (i.e. EPC-routed service only), or only authorize the user to access the TWAN without granting access to EPC via S2a (i.e. non-seamless WLAN offload service only), or authorize both EPC-routed and non-seamless WLAN offload services. If the SCM is selected, the 3GPP AAA Server shall indicate to the TWAN its decision to either authorize access to EPC via S2a or only authorize the user to access the TWAN without granting access to EPC via S2a, i.e. not both;

  - when authorizing the SCM to be used for EPC access, the 3GPP AAA server shall forward the PDN connectivity parameters received from the UE to the TWAN, i.e. the UE requested PDN type (IPv4, IPv6 or IPv4v6), the attach type (initial attach or handover), optionally the requested APN (if received from the UE) and optionally the Protocol Configuration Options (if received from the UE));

  - when authorizing the MCM for EPC access, the 3GPP AAA server shall derive the WLCP key as defined in 3GPP TS 33.402 [19] and shall provide the WLCP key to the TWAN to protect the WLCP signalling.

  if the user is successfully authenticated and authorized for this access, the TWAN:

- shall decide the S2a protocol variant to use if access to EPC is authorized and the TWAN decides to establish S2a.

- if the SCM has been authorized to be used for EPC access, the TWAN shall return an indication to the 3GPP AAA Server on whether the requested connectivity has been granted and, if so, also pass on to the 3GPP AAA Server the connectivity parameters to be provided to the UE, i.e. the selected APN, the selected PDN type (IPv4, IPv6 or IPv4v6), the IPv4 address (for PDN type IPv4 or IPv4v6), the IPv6 interface identifier (for PDN type IPv6 or IPv4v6), optionally the Protocol Configuration Options received from the PDN GW once S2a has been established, and the TWAG user plane MAC address. If the requested connectivity has not been granted, the TWAN should provide the 3GPP AAA Server with a cause indicating why the requested connectivity could not be granted; the TWAN may also provide a Session Management back-off timer to be sent to the UE to instruct the UE to not request new PDN connectivity to the same APN for the indicated time.

When authorizing NBM to be used, the 3GPP AAA server shall return NBM related information back to the trusted non-3GPP access network.

During the STa Access Authentication and Authorization procedure, when DSMIPv6 is used, the 3GPP AAA Server may provide a Home Agent IPv6 address (and optionally IPv4 address) or FQDN to the trusted non-3GPP access network. This is needed if the DHCPv6 option for Home Agent address discovery is chosen (see TS 24.303 [13] and IETF RFC 6611 [28]). If the Home Agent IPv6 address or FQDN is not included in the final Authentication and Authorization Answer by the 3GPP AAA server, the trusted non-3GPP access network shall not assign the Home Agent via DHCPv6.

During the STa Access Authentication and Authorization procedure for MIPv4 FA-CoA mode using trusted non-3GPP access, the 3GPP AAA Server may provide the mobility security parameters FA-RK and FA-RK-SPI to the trusted non-3GPP access network.

The User-Name AVP may contain a decorated NAI (as defined in clause 19.3.3 of 3GPP TS 23.003 [14]). In this case the 3GPP AAA Proxy shall process the decorated NAI and support routing of the Diameter request messages based on the decorated NAI as described in IETF RFC 5729 [37].

Based on local policies, EPC access for emergency services over a trusted non-3GPP access is supported as specified in clause 4.5.7.2.1 of 3GPP TS 23.402 [3] for:

- UEs with a valid EPC subscription that are authenticated and authorized for EPC services;

- UEs that are authenticated only;

- UEs with an unauthenticated IMSI; and/or

- UICC-less UEs.

For PMIPv6, GTPv2 and MIPv4 FA-CoA mode trusted non-3GPP accesses, upon mobility between 3GPP and non-3GPP accesses, for the PDNs the UE is already connected, the PDN GW identity for each of the already allocated PDN GW(s) with the corresponding PDN information is provided to the trusted non-3GPP system. The PDN GW identity is a FQDN and/or IP address of the PDN GW. The non-3GPP access network shall use the received PDN GW identity for mobility with IP address preservation or in case of static PDN GW assignment. If a FQDN is provided, the trusted non-3GPP system shall then derive it to IP address according to the selected mobility management protocol.

NOTE: Mobility with IP address preservation is not supported between TWAN and 3GPP access in TSCM.

During the STa Access Authentication and Authorization procedure, the bootstrapping of an ER server in the TWAN with a given root key may be performed, as described in IETF RFC 6696 [55] and 3GPP TS 33.402 [19]. This procedure is used to provide an ER server with the keying material that will be used for further EAP re-authentication procedures using ERP.

Table 5.1.2.1/1: STa Access Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
UE Layer-2 address	Calling-Station-ID	M	This IE shall contain the Layer-2 address of the UE.
Supported 3GPP QoS profile	QoS-Capability	O	If the non-3GPP access network supports QoS mechanisms, this information element may be included to contain the access network's QoS capabilities as defined in IETF RFC 5777 [9].
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall contain the mobility capabilities of the non-3GPP access network. This information shall be utilized if dynamic mobility mode selection is executed. This information may also be used to decide whether to authorize access to EPC to a user accessing a TWAN. The PMIP6_SUPPORTED flag and/or the GTPv2 SUPPORTED flag shall be set if the non-3GPP access supports PMIPv6 and/or GTPv2. PMIP6_SUPPORTED flag is defined in IETF RFC 5779 [2]. The flag MIP6_INTEGRATED shall be set if DHCPv6 based Home Agent address discovery is supported as defined in IETF RFC 5447 [6]. The MIP4_SUPPORTED flag shall be set if the non-3GPP access supports MIPv4 FA-CoA mode.
Access Type	RAT-Type	M	This IE shall contain the non-3GPP access network technology type that is serving the UE. The TWAN shall set the Access Type value to "WLAN".
Access Network Identity	ANID	M	This IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values)
Full Name for Network	Full-Network-Name	O	If present, this IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
Short Name for Network	Short-Network-Name	O	If present, this IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
Visited Network Identifier	Visited-Network-Identifier	O	If present, this IE shall contain the Identifier that allows the home network to identify the Visited Network. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network.
APN Id	Service-Selection	O	If present, this information element shall contain the Network Identifier part of the APN the user wants to connect to (if available).
Terminal Information	Terminal-Information	O	If present, this information element shall contain information about the user's mobile equipment. The type of identity carried depends on the access technology type. For an HRPD access network, the 3GPP2-MEID AVP shall be included in this grouped AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

Selected Trusted WLAN Identifier	WLAN-Identifier	O	If present, this IE shall contain the WLAN Identifier selected by the UE to access the Trusted WLAN Access Network (see clause 16 of 3GPP TS 23.402 [3]).
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the non-3GPP access network has determined that a previously assigned 3GPP AAA Server is unavailable.
DER Flags	DER-Flags	O	This Information Element contains a bit mask. See 5.2.3.20 for the meaning of the bits.
Transport Access Type	Transport-Access-Type	C	For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see clause 5.2.3.19).
Supported TWAN Connection Modes	TWAN-Connection-Mode	O	The TWAN should include this IE. If present, this information element shall contain the TWAN connection modes supported by the TWAN, i.e. TSCM, SCM and/or MCM.
Provided Connectivity Parameters	TWAN-Connectivity-Parameters	C	This information element shall be present if the 3GPP AAA Server has previously authorized the SCM to be used for EPC access. TWAN-Connectivity-Parameters is a grouped AVP. If the requested connectivity has been granted, the following information elements shall be included: - selected APN - selected PDN type - UE IPv4 Address (for PDN type IPv4 or IPv4v6) - UE IPv6 Interface Identifier (for PDN type IPv6 or IPv4v6) - Protocol Configuration Options (if received from the PGW) - TWAG user plane MAC address The absence of both an IPv4 address and an IPv6 Interface Identifier indicates that the requested connectivity could not be granted. If the requested connectivity has not been granted, the following information elements may be included: - a cause indicating why the requested connectivity has not been granted - a Session Management back-off timer to be sent to the UE
TWAG Control Plane IP Address	TWAG-CP-Address	C	The TWAN shall include this IE if it indicates support of the MCM in the Supported TWAN Connection Modes IE. When present, this IE shall contain the TWAG Control Plane IPv4 Address, or the TWAG Control Plane IPv6 link local address, or both (if the TWAG supports IPv4 and IPv6), to be used for WLCP by the UE if the MCM is used.
IMEI Check in VPLMN Result	IMEI-Check-In-VPLMN-Result	C	The 3GPP AAA Proxy shall include this IE if it has performed an IMEI check in the VPLMN. When present, this IE shall contain the result of the IMEI check.
Domain-Specific Re-authentication Key Request	ERP-RK-Request	O	If present, this IE indicates the willingness of an ER server located in the non-3GPP access network to act as the ER server for this session. When present, this IE shall contain the name of the realm in which the ER server is located.

Table 5.1.2.1/2: Trusted non-3GPP Access Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State.
EAP payload	EAP payload	O	If present, this IE shall contain the Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication. This IE shall not be included if the UE has been authenticated and the 3GPP AAA Server authorizes the SCM for EPC access for the UE and the Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental Result Code	M	This IE shall contain the result of the operation. Result codes are as in Diameter base protocol (see IETF RFC 6733 [58]). Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER _SUCCESS; if present, it contains the maximum number of seconds the session is allowed to remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be present if Result-Code AVP is set to DIAMETER_SUCCESS.
Default APN	Context-Identifier	C	This AVP shall indicate the default APN for the user. If the Access Network Identity received in the Authentication and Authorization Request indicates WLAN (see clause 8.1.1.2 of 3GPP TS 24.302 [26]) and if the TSCM is selected, this AVP shall be set to the Default APN for Trusted WLAN if received from the HSS; otherwise this AVP shall be set to the subscriber's Default APN for 3GPP and other non-3GPP accesses. It shall only be included if NBM is authorized for use, the non-3GPP access network was decided to be trusted, the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Answer and the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1)
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which a DNS resolution needs to be performed. See 3GPP TS 23.003 [3]. It shall only be included if NBM is authorized for use, the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Answer and the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1)

APN and PGW Data	APN-Configuration	C	This information element shall only be sent if EPC Access is authorized, the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Answer and the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1) When NBM is authorized for use, this AVP shall contain the default APN, the list of authorized APNs, including the wildcard APN if configured in the user's subscription, user profile information and PDN GW information. When local IP address assignment is used (for HBM), this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes. The trusted non-3gpp access network knows if NBM is authorized for use or if a local IP address (for HBM) is assigned based on the flags in the MIP6-Feature-Vector. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is authorized for use, the following information elements per APN may be included: - APN - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN types - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - APN-AMBR - Visited Network Identifier (see clause 5.1.2.1.4) - SIPTO permission When DSMIPv6 is used, the following information elements per Home Agent may be included: - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14]) - Authorized 3GPP QoS profile - PDN GW identity When MIPv4 FACoA is used, the following information elements per APN may be included: - APN - Allowed PDN types
Serving GW Address	MIP6-Agent-Info	O	This AVP shall be used only in chained S2a-S8 cases and it shall be sent only if the Result-Code AVP is set to DIAMETER_SUCCESS.

Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall only be sent if EPC Access is authorized and if the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1) It shall contain a AAA/HSS authorized set of mobility capabilities to the trusted non-3GPP access network, if dynamic mobility mode selection between NBM and HBM is done. It shall also be sent when authorizing access to EPC to a user accessing a TWAN. The PMIP6_SUPPORTED and/or the GTPv2_SUPPORTED shall be set to indicate that NBM (PMIPv6 or GTPv2) is authorized for use. Otherwise, ASSIGN_LOCAL_IP or MIP4_SUPPORTED flag shall be set by the 3GPP AAA Server to mandate which HBM mobility protocol is used. The MIP6_INTEGRATED flag shall be set if a Home Agent address is provided for DHCPv6 based Home Agent address discovery. In the latter case HA information for DHCPv6 discovery is provided via the APN-Configuration AVP.

Permanent User Identity	Mobile-Node-Identifier	C	This information element shall only be sent if the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1) This information element shall only be sent if NBM or MIPv4 is authorized for use, or when authorizing the user to access the TWAN without granting access to EPC S2a (i.e. non-seamless WLAN offload). If the user is authenticated, it shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used: - by the MAG in subsequent PBUs as the MN-ID identifying the user in the EPS network, or - by the trusted non-3GPP access network in subsequent MIPv4 RRQs as the MN-NAI identifying the user in the EPS network, or - by the trusted non-3GPP access network to derive the IMSI to be sent in subsequent Create Session Request on GTP S2a. For an Emergency Attach, if the UE is UICC-less (i.e. the User Identity IE in the request contains an IMEI) or if the IMSI is not authenticated, the Permanent User Identity shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14]. This information element shall also be sent if HBM is authorized for use, or to access a Fixed Broadband access network without granting access to EPC S2a (i.e. non-seamless WLAN offload), and the Result-Code AVP is set to DIAMETER_SUCCESS and if the Transport Access Type in the request command indicated that the UE is accessing the EPC from a Fixed Broadband access network (i.e., the Transport-Access-Type AVP takes the value "BBF"); it shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used: - by the trusted non-3GPP access network in subsequent PCC procedure for identifying the user in the EPS network. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
3GPP AAA Server URI	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
UE AMBR	AMBR	C	This Information Element shall contain the UE AMBR of the user. It shall be present only if the non-3GPP access network was decided to be trusted, the Result-Code AVP is set to DIAMETER_SUCCESS and ANID is "HRPD".

Trust Relationship Indicator	AN-Trusted	C	This AVP shall be included only in the first authentication and authorization response. If present, it shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network trusted or untrusted. For the STa case, the value "TRUSTED" shall be used.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
FA-RK	MIP-FA-RK	C	This AVP shall be present if MIPv4 FACoA mode is used, the MN-FA authentication extension is supported and the Result-Code AVP is set to DIAMETER_SUCCESS.
FA-RK-SPI	MIP-FA-RK-SPI	C	This AVP shall be present if MIP-FA-RK is present
Trace information	Trace-Info	C	This information element shall only be sent if the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1) This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the non-3GPP access network. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth-List - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent if it is available and the non-3GPP access network is trusted and the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1)
DEA Flags	DEA-Flags	O	This Information Element contains a bit mask. See 5.2.3.21 for the meaning of the bits.
Selected TWAN Connection Mode	TWAN-Connection-Mode	C	The 3GPP AAA Server shall include this IE if it selects either the SCM or MCM and the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1) When present, this IE shall indicate the selected mode of operation (either SCM or MCM). If this IE is not present, the TWAN shall use TSCM.
Requested Connectivity Parameters	TWAN-Connectivity-Parameters	C	This IE shall contain the requested connectivity parameters received from the UE if the 3GPP AAA Server authorizes the SCM for TWAN and the Result-Code AVP is set to DIAMETER_MULTI_ROUND_AUTH, and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. When present, the following information elements shall be included: - attach type (initial attach or handover) - requested APN (if received from the UE, see NOTE 3) if the UE did not request an Emergency Attach. - requested PDN type - Protocol Configuration Options (if received from the UE)

WLCP Key	WLCP-Key	C	This IE shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS and the selected TWAN Connection Mode is MCM. If present, it shall contain the key for protecting WLCP signalling (see 3GPP TS 33.402 [19]).
Terminal Information	Terminal-Information	C	This information element enables to convey the user's Mobile Equipment Identity to the non-3GPP access network in scenarios where the UE signals its Mobile Equipment Identity directly to the 3GPP AAA Server, i.e. when the Terminal-Information AVP is not received in the Authentication and Authorization Request. For a trusted WLAN access, the 3GPP AAA Server shall include this IE if the user's Mobile Equipment Identity is available. When present, this grouped AVP shall contain the IMEI AVP and, if available, the Software Version AVP. (see NOTE 2)
Emergency Services	Emergency-Services	C	If the 3GPP AAA Server supports IMS emergency sessions over TWAN (see clause 4.5.7 of 3GPP TS 23.402 [3]), it shall include this IE and set the Emergency-Indication bit when the UE indicates an Emergency Attach in EAP-AKA' signalling.
Emergency Info	Emergency-Info	C	When present, this IE shall contain the identity of the PDN GW dynamically allocated for emergency services. It shall be present for a non-roaming authenticated user, if this information was received from the HSS, the TWAN indicated support of IMS Emergency sessions and the Result-Code AVP is set to either: - DIAMETER_SUCCESS or - DIAMETER_MULTI_ROUND_AUTH and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags. (see NOTE 1)
ERP Keying Material	Key	C	If the 3GPP AAA Server supports ERP, this IE shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS, the domain-specific re-authentication key was requested and the use of ERP is authorized for this user (see clause 8.2.3.27). In that case, this IE shall contain the Domain-Specific Root Key (DSRK) and the Extended Master Session Key name (EMSKname), and it may contain the DSRK lifetime.
ERP Realm	ERP-Realm	C	This IE shall be present if the ERP Keying Material is present. This IE indicates the realm where the ER server is located; it also indicates the domain name to use as the realm part of the KeyName-NAI used during ERP-based re-authentication.
UE Usage Type	UE-Usage-Type	C	This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the UE Usage Type of the subscriber.

NOTE 1: The 3GPP AAA Server may decide to not include the AVP if the Result-Code AVP is set to DIAMETER_SUCESS and the AVP has already been sent in a previous message with the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH and the TWAN-S2a-Connectivity-Indicator set in DEA-Flags. In that case, the TWAN shall consider the information received in the previous message as still applicable.

NOTE 2: For a trusted WLAN access, the UE signals its Mobile Equipment Identity to the 3GPP AAA Server via EAP-AKA' and the 3GPP AAA Server forwards this information to the TWAN in the Terminal-Information AVP in the Authentication and Authorization Answer.

NOTE 3: The Service-Selection AVP in the Requested Connectivity Parameters IE shall contain the APN requested by the UE, regardless of whether this APN is authorized by a matching APN or by the wildcard APN in the user's subscription.

5.1.2.1.2 3GPP AAA Server Detailed Behaviour

On receipt of the first DER message, the 3GPP AAA Server shall check the validity of the ANID AVP and whether the non-3GPP access network is entitled to use the included value. The correct syntax of the ANID is checked as follows:

- In a non-roaming case, i.e. when the 3GPP AAA Server receives the request directly and not via the 3GPP AAA Proxy, checking ANID is mandatory;

- In a roaming case when the request is received via an 3GPP AAA proxy, checking ANID is optional. The 3GPP AAA Server may decide to check ANID based on local configuration, e.g. depending on the received visited network identifier.

- If the checking result shows that the included ANID value is not valid (not defined by 3GPP) or that the requesting entity is not entitled to use the received ANID value, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY.

The 3GPP AAA Server shall check if user data exists in the 3GPP AAA Server (containing valid authentication information for the current access network identity). If not, the 3GPP AAA Server shall use the procedures defined in SWx interface to obtain access authentication and authorization data.

If IMEI check is required by operator policy and the TWAN is in the HPLMN, the 3GPP AAA Server shall:

- retrieve the IMEI(SV) from the UE as specified in 3GPP TS 23.402 [26];
- if the IMEI(SV) is available, check the Mobile Equipment's identity status towards the EIR, using the ME Identity Check procedure (see clause 11);
    - upon getting the IMEI check result from the EIR, determine whether to continue or stop the authentication and authorization procedure;
- if the IMEI(SV) is not available, determine whether to continue or stop the authentication and authorization procedure based on operator policy;
- if the 3GPP AAA Server determines that the authentication and authorization procedure shall be stopped, it shall:
    - notify the UE that the Mobile Equipment used is not acceptable to the network (e.g. the Mobile Equipment is on the prohibited list of the EIR), as specified in 3GPP TS 24.302 [26];
    - respond to the TWAN with the Experimental-Result-Code DIAMETER_ERROR_ILLEGAL_EQUIPMENT.

Specific operator policies may be configured for emergency services, regarding whether to check the IMEI and, if the IMEI needs to be checked, whether to continue or stop the authentication and authorization procedure upon getting the IMEI check result or when the IMEI(SV) is not available.

If the IMEI-Check-Required-In-VPLMN bit is set in the DER-Flags AVP of the first Authentication and Authorization Request message and the TWAN is in the VPLMN, the 3GPP AAA Server shall:

- retrieve the IMEI(SV) from the UE as specified in 3GPP TS 23.402 [26];
- request the VPLMN to check the IMEI, by setting the IMEI-Check-Request-In-VPLMN bit in the DEA-Flags AVP and including the IMEI(SV) if available in the DEA message;
- upon getting the IMEI-Check-In-VPLMN-Result AVP in the subsequent DER message, if the IMEI check failed in the VPLMN:
    - notify the UE that the Mobile Equipment used is not acceptable to the network (e.g. the Mobile Equipment is on the prohibited list of the EIR), as specified in 3GPP TS 24.302 [26];
    - respond to the TWAN with the Experimental-Result-Code DIAMETER_ERROR_ILLEGAL_EQUIPMENT.

See Annex A.2.3 and A.3.2.

If the 3GPP AAA Server receives a request message not related to any existing session and is able to recognize that the non-3GPP access network included the AAA-Failure-Indication AVP in the request, the 3GPP AAA Server shall also include the AAA-Failure-Indication AVP over the SWx interface, while retrieving the access authentication and authorization data from the HSS.

If SWx authentication response indicates that:

- The user does not exist, then the 3GPP AAA Server shall respond the non-3GPP access network with Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN.
- The user does not have non-3GPP access subscription, then 3GPP AAA Server shall respond the non-3GPP access network with Experimental-Result-Code DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION.
- The user is not allowed to roam in the visited network, then 3GPP AAA Server shall respond the non-3GPP access network with Experimental-Result-Code DIAMETER_ERROR_ROAMING_NOT_ALLOWED.

- The user is currently being served by a different 3GPP AAA Server, then the 3GPP AAA Server shall respond to the non-3GPP access network with the Result-Code set to DIAMETER_REDIRECT_INDICATION and the Redirect-Host set to the Diameter URI of the 3GPP AAA Server currently serving the user (this Diameter URI shall be constructed based on the Diameter Identity included in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

- The user is not allowed to use the current access type, then the 3GPP AAA Server shall respond to the non-3GPP access network with Experimental-Result-Code DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED.

- Any other error occurred, then the error code DIAMETER_UNABLE_TO_COMPLY shall be returned to the non-3GPP access network.

When SWx authentication response includes the requested authentication information, the 3GPP AAA Server shall proceed with the authentication and authorization procedure. The 3GPP AAA Server shall use the procedures defined in SWx interface to obtain the user's subscription profile from HSS.

Before sending out the authentication challenge, the 3GPP AAA Server shall decide, whether the access network is handled as Trusted or Untrusted. The 3GPP AAA Server shall make the decision based on the Access Network Identifier and Visited Network Identity information elements, according to its local policies. The local policies of the 3GPP AAA Server shall be based on the security criteria described in 3GPP TS 33.402 [19].

NOTE 1: The network operator can configure this e.g. according to the roaming agreements with the non-3GPP AN operator or with VPLMN operator.

In a roaming case, if the 3GPP AAA Server has received the trust relationship indicator from the VPLMN (AN-Trusted AVP), the 3GPP AAA Server may use this information as input parameter to the trusted/untrusted evaluation.

The VPLMN trust relationship indicator may be utilized only if the appropriate trust relationship exists between the HPLMN and VPLMN operators.

Based on the trusted/untrusted decision, the 3GPP AAA Server may send a trust relationship indication to the UE, as described in 3GPP TS 24.302 [26].

The 3GPP AAA Server shall indicate the trust relationship assessment of the non-3GPP access network to the UE in the AT_TRUST_IND attribute (in the EAP-Request/AKA'-Challenge) as defined in 3GPP TS 24.302 [26]. The 3GPP AAA Server shall also indicate the trust relationship assessment to the non-3GPP access network using AN-Trusted AVP in the DEA command.

If the decision is "Trusted", the STa authentication and authorization procedure is executed as described here, in clause 5.1.2.1 and it clauses. Otherwise, the SWa authentication and authorization procedure is executed as described in clause 4.1.2.1.

The 3GPP AAA Server marks the trust relationship as "trusted" with the User Identity. If the 3GPP AAA Server detects that an S6b session already exists for the corresponding UE and the S6b session was established as a result of an authentication request for DSMIPv6, the 3GPP AAA Server shall send the trust relationship to the PDN GW as specified in clause 9.1.2.5.

The 3GPP AAA Server shall run EAP-AKA' authentication as specified in 3GPP TS 33.402 [19]. Exceptions shall be treated as error situations and the result code shall be set to DIAMETER_UNABLE_TO_COMPLY.

Once authentication is successfully completed, the 3GPP AAA Server shall perform the following authorization checking (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error):

1) Check if the user is barred to use the non 3GPP Access. If it is so, then the Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED

2) Check the access type. If the received access type is listed in the user's disallowed RAT-Types,

   this shall be treated as error and the Experimental-Result-Code DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED shall be returned.

The following steps are only executed if the non-3GPP access network was decided to be Trusted.

3) If the APN Id IE is present in the request, check if the user has a subscription for the requested APN or for the wildcard APN. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION

4) for a trusted WLAN access (i.e. ANID in the request indicates WLAN, see clause 8.1.1.2 of 3GPP TS 24.302 [26]), check if the user is authorized to access to EPC via S2a and/or non-seamless WLAN offload via the selected WLAN:

   - if no TWAN-Access-Info AVP was received from the HSS in the user's subscription, the 3GPP AAA Server shall consider that access to EPC and non-seamless WLAN Offload is authorized;

   - if one or more TWAN-Access-Info AVP(s) was received from the HSS in the user's subscription:

     - if the TWAN has signalled the selected Trusted WLAN in the request and the selected Trusted WLAN identifier contains only the SSID of the selected WLAN, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the selected trusted WLAN (i.e. including a WLAN-Identifier AVP with the same SSID and without HESSID information) if any;

NOTE 2: When the TWAN does not include the HESSID in the request, the authorization information in the 3GPP AAA Server containing both SSID and HESSID is not applicable; therefore, in order to get specific authorization of the UE in this case, the operator needs to define authorization information for the SSID in question (without HESSID), or to rely on the "wildcard" authorization (i.e., a TWAN-Access-Info AVP not including a WLAN-Identifier AVP).

     - if the TWAN has signalled the selected Trusted WLAN in the request and the selected Trusted WLAN identifier contains both the SSID and the HESSID of the selected WLAN, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the selected trusted WLAN (i.e. including a WLAN-Identifier AVP with the same SSID and same HESSID);

       Else, if no match is found, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the HESSID of the selected Trusted WLAN identifier (i.e. TWAN-Access-Info including a WLAN-Identifier AVP with the same HESSID and without SSID information);

       Else, if no match is found, the 3GPP AAA Server shall authorize the access methods allowed by the TWAN-Access-Info AVP explicitly matching the SSID of the selected Trusted WLAN identifier (i.e. TWAN-Access-Info including a WLAN-Identifier AVP with the same SSID and without HESSID information) ;

     - otherwise, if the selected Trusted WLAN does not match explicitly any of the TWAN-Access-Info or if TWAN has not signalled the selected Trusted WLAN Identifier, the 3GPP AAA Server shall apply the access methods allowed by the "wildcard" TWAN-Access-Info AVP (i.e. TWAN-Access-Info AVP not including a WLAN-Identifier AVP) if any;

     - otherwise, if the "wildcard" TWAN-Access-Info is not present, the 3GPP AAA Server shall consider that access to EPC and non-seamless WLAN Offload is not authorized.

5) Check if the user is not authorized to perform non-seamless WLAN Offload and, if the user is also barred from using the subscribed APNs, then the Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

6) If present, check the flags of the received MIP6-Feature-Vector AVP:

   - If the MIP6-INTEGRATED flag is set and the 3GPP AAA Server has authorized DHCP Home Agent assignment, the 3GPP AAA Server shall include the Home Agent addresses in the APN-Configuration AVP in the response and the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag set. If the HA assignment via DHCPv6 is not used, the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag not set shall be sent.

   - The PMIP6_SUPPORTED and/or GTPv2 SUPPORTED flag indicates to the 3GPP AAA Server whether the trusted non-3GPP access network supports NBM or not.

     As specified in 3GPP TS 23.402 [3], based on the information it has regarding the UE (see 3GPP TS 24.302 [26]), local/home network capabilities and local/home network policies, the 3GPP AAA Server may perform mobility mode selection between NBM and HBM.
     For a trusted WLAN access, if the user is successfully authenticated and authorized for this access, the 3GPP

AAA Server may either only authorize the user to access to EPC via S2a (i.e. EPC-routed service only), or only authorize the user to access the TWAN without granting access to EPC via S2a (i.e. non-seamless WLAN offload service only), or authorize both EPC-routed and non-seamless WLAN offload services, taking also into account the subscriber profile, access network, the selected WLAN identifier if present, and the TWAN's non-seamless WLAN offload capability if present, and the authorized mode of operation (TSCM, SCM or MCM). The 3GPP AAA Server may authorize both EPC-routed and non-seamless WLAN offload services only if the MCM is selected, or in non-roaming scenarios if the TSCM is selected; the 3GPP AAA Server shall not authorize both EPC-routed and non-seamless WLAN offload services if the SCM is selected or in roaming scenarios if the TSCM is selected.

If the 3GPP AAA Server decides that access to EPC is authorized and NBM should be used for such access, the PMIP6_SUPPORTED and GTPv2_SUPPORTED flags shall be set in the response to indicate that NBM is authorized for use for the UE by the trusted non 3GPP access network. If only the PMIPv6_SUPPORTED or the GTPv2_SUPPORTED flag is present in the response, the trusted non-3GPP access network shall assume that this also indicates that NBM is authorized for use. In addition, for a trusted WLAN access, the Non-seamlesss WLAN offload Authorization flag shall be set in the DEA-Flags AVP in the response if the non-seamless WLAN offload is authorized.

If the 3GPP AAA Server decides to only authorize the user to access the TWAN without granting access to EPC S2a (i.e. non-seamless WLAN offload service only), none of the flags (PMIP6_SUPPORTED, GTPv2_SUPPORTED, MIP4_SUPPORTED, MIP6-INTEGRATED, ASSIGN_LOCAL_IP) shall be set in the response, i.e. the Mobility Capabilities IE is not sent in the response, and the Non-seamlesss WLAN offload Authorization flag shall be set in the DEA-Flags AVP in the response.

If the 3GPP AAA Server decides that a local IP address should be assigned for HBM, the ASSIGN_LOCAL_IP flag shall be set in the response to indicate to the trusted non 3GPP access network that a local IP address (for HBM) should be assigned.

The 3GPP AAA Server shall not set the PMIP6_SUPPORTED/GTPv2_SUPPORTED and ASSIGN_LOCAL_IP flags both at the same time in the response.

- The MIP4_SUPPORTED flag indicates to the 3GPP AAA Server whether the trusted non-3GPP access network supports MIPv4 FA-CoA mode or not. As specified in 3GPP TS 23.402 [3], based on the information it has regarding the UE (see 3GPP TS 24.302 [26]), local/home network capabilities and local/home network policies, the 3GPP AAA Server may perform mobility mode selection. If the 3GPP AAA Server decides that MIPv4 FA-CoA mode should be used, the MIP4_SUPPORTED flag shall be set in the response.

NOTE 3: When selecting DSMIPv6 the AAA server assumes that the trusted non 3GPP access gateway has the capability to assign a local IP address to the UE.

For Trusted WLAN access, the 3GPP AAA Server shall select the TWAN connection mode, i.e. either TSCM, SCM or MCM, taking into account the modes supported by the TWAN (as reported in the first DER message), those supported by the UE (as reported in the EAP payload, see 3GPP TS 24.302 [26]) and operator policy. The 3GPP AAA Server shall then indicate to the TWAN the TWAN connection mode it has selected, either explicitly using the Selected TWAN Connection Mode IE if it has selected SCM or MCM, or implicitly by not including the Selected TWAN Connection Mode IE if it has selected TSCM.

For Trusted WLAN access, if the 3GPP AAA Server has determined that the EAP-AKA' authentication is correct (i.e., the UE has sent a valid EAP-AKA' challenge response) and if the 3GPP AAA Server authorizes the SCM to be used for EPC access, the 3GPP AAA Server shall reply to the first DER message it receives with a result code set to DIAMETER_MULTI_ROUND_AUTH, leave the EAP-Payload AVP absent in the reply, and set the TWAN-S2a-Connectivity-Indicator bit to 1 in the DEA-Flags AVP; it shall also include in the response command all subscription-related parameters for the user, so the TWAN is able to proceed with the setup of the required S2a network connectivity (e.g., establishment of the GTP tunnel). After receiving a subsequent DER command from the TWAN, the 3GPP AAA Server shall check if the TWAN-S2a-Connectivity-Indicator is set, and if so, it may disregard the received EAP-Payload, since the EAP-AKA' challenge response has been already successfully checked. If the TWAN could not provide the requested S2a network connectivity and included a Session Management back-off timer in the DER command, the 3GPP AAA Server shall instruct the UE to not request new PDN connectivity to the same APN for the indicated time as specified in 3GPP TS 24.302 [26]. See Annex A.

Once the Authentication and Authorization procedure successfully finishes, the 3GPP AAA Server shall download, the authentication data, the list of authorized APN's if the UE did not indicate an Emergency Attach in EAP-AKA' signalling (see 3GPP TS 24.302 [26]), and the authorized mobility protocols in the authentication and authorization response from the HSS (see SWx procedure in Clause 8.1.2.1). If the Access Network Identity received in the Authentication and Authorization Request indicates WLAN (see clause 8.1.1.2 of 3GPP TS 24.302 [26]) and if the TSCM is selected, the 3GPP AAA Server shall set the Default APN in the Authentication and Authorization Answer to the Default APN for Trusted WLAN if received from the HSS, otherwise to the subscriber's Default APN for 3GPP and other non-3GPP accesses.

For a trusted WLAN access, if the user is authorized to access to EPC via S2a, and/or non-seamless WLAN offload via the selected WLAN, the 3GPP AAA Server shall send the user's Mobile Equipment Identity to the TWAN, if this information is available.

Once the Authentication and Authorization procedures successfully finish and if MIPv4 FACoA mode is used the 3GPP AAA Server shall calculate the MIPv4 FACoA mobility security parameters as defined in 3GPP TS 33.402 [19] and include these in the authentication and authorization response to the trusted non 3GPP access network.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and, therefore, no authorization information shall be returned.

For Fixed Broadband access network, the 3GPP AAA Server shall determine if the UE is connected via a BBF-defined WLAN access according to the Transport-Access-type AVP. If the UE is connected via a BBF-defined WLAN access, the 3GPP AAA Server shall perform the enabling of the UE reflective QoS function as specified in 3GPP TS 24.139 [43].

NOTE 4: This behaviour is applicable for both fixed broadband access interworking and the fixed broadband access convergence. The architecture of fixed broadband access interworking is specified in 3GPP TS 23.139 [39]. The architecture of the fixed broadband access convergence is specified in 3GPP TS 23.203 [45].

If the 3GPP AAA Server supports IMS Emergency sessions over WLAN (see clause 4.5.7.2 of 3GPP TS 23.402 [3]), the 3GPP AAA Server shall proceed as specified above, but with the following modifications, for an Emergency Attach:

1) The 3GPP AAA Server shall reject the Authentication and Authorization Request and set the result code to DIAMETER_UNABLE_TO_COMPLY if the TWAN does not indicate support of IMS Emergency sessions in the DER-Flags AVP in the request.

2) If the UE does not have an IMSI:

   - if local policies allow emergency sessions for all UEs, the 3GPP AAA Server shall skip the procedures defined for the SWx interface to obtain access authentication and authorization data, shall skip the authorization checkings and shall authorize the UE to access to EPC for emergency services. The Permanent User Identity IE in the answer shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14];

   - otherwise the 3GPP AAA Server shall reject the request with the Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN.

3) If the UE has an IMSI but the IMSI is not authenticated:

   - if local policies allow emergency sessions for unauthenticated UEs with an IMSI, the 3GPP AAA Server shall skip the procedures defined for the SWx interface to obtain access authorization data, shall skip the authorization checkings, shall request the UE to provide its IMEI as specified in clause 13.4 of 3GPP TS 33.402 [19] and shall authorize the UE to access to EPC for emergency services. The Permanent User Identity IE in the answer shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14];

   - otherwise the 3GPP AAA Server shall reject the request with the Experimental-Result-Code set as specified for authentication failures in this clause.

4) If the UE has an authenticated IMSI but the UE is not authorized to access the EPC:

   - if local policies allow emergency sessions for any authenticated UE, the 3GPP AAA Server shall authorize the UE to access to EPC for emergency services;

- otherwise the 3GPP AAA Server shall reject the request with the Experimental-Result-Code set as specified for authorization failures in this clause.

5) When authorizing a UE to access to EPC for emergency services, the 3GPP AAA Server:

- shall set the Emergency-Indication bit of the Emergency-Services IE in the answer;

- shall not allow the use of non-seamless WLAN offload services.

In addition, if the 3GPP AAA Server supports IMS Emergency sessions over WLAN (see clause 4.5.7.2 of 3GPP TS 23.402 [3]), the 3GPP AAA Server shall also include the Emergency Info IE in the Authentication and Authorization Answer, for emergency and non-emergency Attach, if this information was received from the HSS, the user is not roaming, the TWAN indicated support of IMS Emergency sessions and the Result-Code AVP is set to either:

- DIAMETER_SUCCESS or

- DIAMETER_MULTI_ROUND_AUTH and TWAN-S2a-Connectivity-Indicator is set in DEA-Flags.

Once the Authentication and Authorization procedures successfully finish, if a domain-specific re-authentication key was requested and the use of ERP is authorized for this user based on subscription parameter, the 3GPP AAA Server which support ERP shall derive the DSRK from the EMSK and the domain name received in the request as specified in IETF RFC 6696[55] and shall include the DSRK, the EMSKname, and optionally the DSRK lifetime in the authentication and authorization response to the non-3GPP access network.

Otherwise, when the 3GPP AAA Server does not support ERP, the domain-specific re-authentication key request is ignored if present in the authentication and authorization request.

5.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the non-3GPP access network is connected to a VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy, with the following additions.

If IMEI check is required by operator policy and the TWAN is in the VPLMN, the 3GPP AAA Proxy shall:

- set the IMEI-Check-Required-In-VPLMN bit in the first Authentication and Authorization Request message sent to the 3GPP AAA Server;

- upon receipt of a subsequent DER message with the IMEI-Check-Request-in-VPLMN bit set to 1 in the DER-Flags AVP,

  - if the IMEI(SV) is available, check the Mobile Equipment's identity status towards the EIR, using the ME Identity Check procedure (see clause 11);

    - upon getting the IMEI check result from the EIR, determine whether to continue or stop the authentication and authorization procedure;

  - if the IMEI(SV) is not available, determine whether to continue or stop the authentication and authorization procedure based on operator policy;

  - send the result of the IMEI check to the 3GPP Server in the IMEI-Check-In- VPLMN-Result AVP.

Specific operator policies may be configured for emergency services, regarding whether to check the IMEI and, if the IMEI needs to be checked, whether to continue or stop the authentication and authorization procedure upon getting the IMEI check result or when the IMEI(SV) is not available.

See Annex A.2.3 and A.3.2.

On receipt of an authentication and authorization request, the 3GPP AAA Proxy

- shall check the Visited-Network-Identifier AVP,

  - If the AVP is not present, the 3GPP AAA Proxy shall insert it before forwarding the request to the 3GPP AAA Server.

- If the AVP is present, the 3GPP AAA Proxy may check and overwrite its value, depending on its local policy, e.g. the trusted non-3GPP access network is being operated by the VPLMN operator or by a third party.

- shall check the ANID AVP. If the result of the checking shows that the included ANID value is not valid (not defined by 3GPP) or that the requesting entity is not entitled to use the received value, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and the authentication response shall be sent to the trusted non-3GPP access network.

- may take a decision about the trustworthiness of the non-3GPP access from VPLMN's point of view. If such decision is taken, it shall be based on the Access Network Identifier and optionally, on further information about the non-3GPP access network, according to the 3GPP AAA Proxy's local policies. These local policies shall reflect the security criteria described in 3GPP TS 33.402 [19], with the assumption that the PDN GW will be allocated in the VPLMN.

NOTE 1: For example, if hop-by-hop security relationship exists between the NAS and the 3GPP AAA Proxy, the 3GPP AAA Proxy may use the Origin-Host AVP to uniquely identify the NAS and the access network.

The decision about the trustworthiness of the non-3GPP access network is encoded to the VPLMN trust relationship indicator that is inserted to the authentication and authorization request.

On receipt of the first authentication and authorization request, the 3GPP AAA Proxy shall check locally configured information whether users from the HPLMN are allowed to activate a PDN connection from the non-3GPP access network via this (V)PLMN. If not, the Experimental-Result-Code shall be set to DIAMETER_ERROR_ROAMING_NOT_ALLOWED and the authentication and authorization response shall be sent to the non-3GPP access network.

NOTE 2: It is assumed that there is a roaming agreement between the non-3GPP access network and the VPLMN.

On receipt of the first authentication and authorization request, a 3GPP AAA Proxy which supports ERP may check whether ERP is supported by the non-3GPP access network. If the non-3GPP access network supports ERP and there is an ER server requesting a domain-specific re-authentication key in the authentication and authorization request, the 3GPP AAA Proxy may not authorize it based on locally configured information, remove the domain-specific key request before forwarding the request. If the non-3GPP access network supports ERP and there is no ER server in the non-3GPP access network or if the ER server in the non-3GPP access network was not authorized based on locally configured information, the 3GPP AAA Proxy may act as ER server and include the domain-specific re-authentication key request into the first authentication and authorization request forwarded to the 3GPP AAA server.

On receipt of the authentication and authorization answer that completes a successful authentication, the 3GPP AAA Proxy

- may check locally configured information about using the chained S8-S2a option towards the given HPLMN. If chaining is required, the 3GPP AAA Proxy shall select a Serving GW from its network configuration database and shall include the Serving GW address in the answer.

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.

- shall record the state of the connection (i.e. Authentication and Authorization Successful).

- may check if ERP keying material is provided in the answer in response to the domain-specific re-authentication key requested by the 3GPP AAA Proxy acting as an ER server. If it is, the 3GPP AAA Proxy shall remove the ERP keying material from the answer forwarded to the non-3GPP access network and store the DSRK, the EMSKname and the DSRK lifetime. If there is no ERP keying material and the DEA-Flag does not indicate that ERP is supported by the 3GPP AAA Server, the 3GPP AAA Proxy shall not forward any ERP related messages to the 3GPP AAA Server.

- shall forward the ERP keying material to the TWAN if received from the 3GPP AAA Server and the ER server is located in the TWAN.

5.1.2.1.4 Trusted non-3GPP access network Detailed Behaviour

The Trusted non-3GPP access network shall initiate the Trusted non-3GPP Access Authentication and Authorization procedure when the user attaches to the access network. During the authentication, it shall act as a pass-through EAP authenticator.

If the IMEI-Check-Request-In-VPLMN bit is set in the DEA-Flags AVP of the DEA message, the TWAN shall request the 3GPP AAA Proxy to check the IMEI, by setting the IMEI-Check-Request-In-VPLMN bit in the DER-Flags AVP and including the IMEI(SV) in the DER message. See Annex A.2.3 and A.3.2.

If PMIPv6, GTPv2 or MIPv4 FACoA is used, at successful completion of the procedure, the trusted non-3GPP access network shall store the non-3GPP user data received from the 3GPP AAA Server. The trusted non-3GPP access network shall utilize these data

- To authorize the APNs received in PDN connection creation request from the UE;
- To authorize the requested home address types: IPv4 home address and/or IPv6 home network prefix;
- To check if the UE requested APN is authorized as such or based on the wildcard APN.

NOTE: The user will be allowed to create PDN connections only to the subscribed APNs and use the address types that are allowed by the subscribed PDN types.

If DSMIPv6 is used and if the trusted non-3GPP access network has received the PGW identity in form of the FQDN from the 3GPP AAA Server, then the trusted non-3GPP access network may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

If MIPv4 FACoA is used and if the non-3GPP access network has received FA-RK-SPI and FA-RK from the 3GPP AAA Server , the trusted non-3GPPaccess network will use FA-RK key and FA-RK-SPI to further derive MN-FA shared key and MN-FA-SPI, as defined in 3GPP TS 33.402 [19]. These are used to process the MN-FA Authentication Extension in the RRQ/RRP messages if the extension is present.

If the subscriber is not roaming and the SIPTO-Permission information for an APN is present, the HSGW shall allow SIPTO for that APN only if the SIPTO-Permission information indicates so. If the subscriber is not roaming and the SIPTO-Permission information for an APN is not present, the HSGW may allow SIPTO for that APN. If the subscriber is roaming and the SIPTO-Permission information for an APN is present, the HSGW shall allow SIPTO for that APN only if the SIPTO-Permission information indicates so and the VPLMN Dynamic Address is allowed and the HSGW selects a PDN GW in the VPLMN. For the requested APN allowed for SIPTO, the trusted non-3GPP access network may use the 3GPP DNS mechanism to select a PGW which is close to the HSGW. Detailed behaviour is specified in 3GPP2 X.S0057 [25], 3GPP TS 23.402 [3] and 3GPP TS 29.303 [34].

For optimized handover of an emergency session from E-UTRAN to an S2a based cdma2000® HRPD access network, if the trusted non-3GPP access network supports Emergency services for users in limited service state, then the trusted non-3GPP access network shall skip the authentication procedure (for users without an IMSI or with an IMSI marked as unauthenticated); or if the trusted non-3GPP access network accepts that the authentication may fail (for users with an IMSI), it shall continue with the procedure. For these cases, the Trusted non-3GPP access network shall release any non-emergency PDN connections.

The TWAN decides the S2a protocol variant to use if access to EPC is authorized and the TWAN decides to establish S2a. The TWAN may be configured with the S2a protocol variant(s) on a per PLMN granularity, or may retrieve information regarding the S2a protocol variants supported by the PDN GW (PMIPv6 or/and GTPv2) from the Domain Name Service Function as described in 3GPP TS 29.303[34]. For static PDN GW assignment, in order to determine the PLMN of the PDN GW, the TWAN may use the Visited Network Identifier, if received from the 3GPP AAA Server, or the FQDN of the PDN GW, if included in the MIP6-Agent-Info AVP of the APN in use; if none of them are available, it may use the PLMN where the 3GPP AAA Server is located. If the TWAN supports Dedicated Core Networks and receives the UE-Usage-Type from the 3GPP AAA Server, the TWAN shall select the PGW as specified in clause 5.8 of 3GPP TS 29.303 [34].

For Trusted WLAN access, the TWAN should attempt the establishment of the S2a connectivity if the 3GPP AAA Server authorizes the SCM to be used for EPC access and the 3GPP AAA Server answers the authentication request with a result code of DIAMETER_MULTI_ROUND_AUTH and with the TWAN-S2a-Connectivity-Indicator bit set to 1 in the DEA-Flags AVP. After completing the S2a network connectivity actions, the TWAN shall re-issue a new DER command including the last EAP-Payload sent in a former request, and setting the TWAN-S2a-Connectivity-Indicator bit to 1 in the DER-Flags AVP. If the requested connectivity has been granted, the TWAN shall also provide the 3GPP

AAA Server with the connectivity parameters provided to the UE; otherwise, the TWAN should also provide a cause indicating why the requested connectivity could not be granted and may provide a Session Management back-off timer to be sent to the UE to instruct the UE to not request new PDN connectivity to the same APN for the indicated time.

If GTPv2 is used on S2a and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the trusted non-3GPP access network shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user.

If the Trusted non-3GPP access networkdetermines that a previously assigned 3GPP AAA Sever is unavailable, it may attempt to send a new authentication and authorization request to an alternate 3GPP AAA Server. If the Trusted non-3GPP access network receives from this new server a redirect indication towards the former server (due to the HSS having stored the former 3GPP AAA Server identity), it shall terminate all previously existing sessions and PDN connections for that user, and it shall re-send again the request towards the new server, but it shall include the AAA-Failure-Indication AVP in the new request.

If the TWAN supports IMS Emergency sessions over WLAN (see clause 4.5.7.2 of 3GPP TS 23.402 [3]), the TWAN shall:

- set the Emergency-Capability-Indication bit in the DER-Flags AVP to indicate support of IMS emergency sessions to the 3GPP AAA Server (to be forwarded to the UE via EAP-AKA' signalling).
- interpret the receipt of an Emergency NAI for Limited Service State or an IMSI-based Emergency NAI from the UE, or the Emergency-Services AVP from the 3GPP AAA Server, with the Emergency-Indication bit set, as an indication that the UE requests to access the EPC for emergency services;
- give preferential treatment to UEs which access the EPC for emergency services, e.g. in scenarios including network overload;
- use its Emergency Configuration Data to determine the APN to be associated with the emergency PDN connection and possibly the PGW to use;
- use the PGW identified in the Emergency PGW Identity IE, during a handover of an emergency PDN connection to a trusted WLAN access, if this information is received from the 3GPP AAA Server, the user is a non-roaming authenticated user and the TWAN is configured to use a dynamic PGW for emergency services for such users;
- proceed during an Emergency Attach for a UE without a UICC or with an authenticated IMSI as specified above with the following modifications, if local policies (related with local regulations) in the TWAN allows unauthenticated emergency sessions:
  - if the UE is UICC-less, the User Identity IE in the Authentication and Authorization Request shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14];
  - if the Permanent User Identity IE in the answer contains an IMEI based NAI but the User Identity IE in the request did not contain an IMEI based NAI, the TWAN shall determine that the IMSI was not authenticated and proceed accordingly with the setup of the Emergency PDN connection over S2b (see 3GPP TS 29.274 [38]).

5.1.2.2 HSS/AAA Initiated Detach on STa

5.1.2.2.1 General

This procedure is used between the 3GPP AAA/HSS and the trusted non-3GPP access network to instruct the non-3GPP access network to detach a specific user from the access network. The procedure is based on Diameter session abort messages.

Diameter usage over the STa interface:

- This procedure is mapped to the Diameter command codes Diameter-Abort-Session-Request (ASR), Diameter-Abort-Session-Answer (ASA), Diameter-Session-Termination-Request (STR) and Diameter-Session-Termination-Answer (STA) specified in IETF RFC 6733 [58]. Information element contents for these messages are shown in tables 5.1.2.2.1/1 and 5.1.2.2.1/2.
- The STa application id value of 16777250 shall be used as the Application Id in ASR/ASA/STR/STA commands.

Table 5.1.2.2.1/1: Information Elements passed in ASR message

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Auth-Session-State	Auth-Session-State	O	If present this information element shall indicate to the Non-3GPP access network whether the 3GPP AAA Server requires an STR message.

Table 5.1.2.2.1/2: Information Elements passed in ASA message

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall indicate the result of the operation.

Table 5.1.2.2.1/3: Information Elements passed in STR message

Information element name	Mapping to Diameter AVP	Cat.	Description
Termination-Cause	Termination-Cause	M	This information element shall contain the reason why the session was terminated. It shall be set to "DIAMETER_ADMINISTRATIVE" to indicate that the session was terminated in response to an ASR message.

Table 5.1.2.2.1/4: Information Elements passed in STA message

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall contain the result of the operation.

5.1.2.2.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to instruct the Non-3GPP access network to detach a specific user from the access network.

In the DSMIPv6 case, the 3GPP AAA Server shall initiate first the detach procedure over the S6b reference point towards the PDN GW. When this process has finalized, the 3GPP AAA Server can initiate the detach procedure of the UE from the non-3GPP access network.

The 3GPP AAA Server shall include the Auth-Session-State AVP in the ASR command with a value of NO_STATE_MAINTAINED if it does not require a STR from the Non-3GPP access network. If it does require a STR from the Non-3GPP access network, the 3GPP AAA Server shall either omit the Auth-Session-State AVP from the ASR command or include the Auth-Session-State AVP in the ASR command with a value of STATE_MAINTAINED.

On receipt of the ASR command, the Non-3GPP access network shall check if the user is known in the Non-3GPP access network. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

If the user is known, the Non-3GPP access network shall perform the disconnection of all the PDN connections active for this user and remove any stored user information, except for emergency PDN connections which shall remain active, if the trusted Non-3GPP access supports Emergency services for users in limited service state.

The Non-3GPP access network shall set the Result-Code to DIAMETER_SUCCESS and send back the ASA command to the 3GPP AAA Server, which shall update the status of the subscriber on the detached access network.

If required by the 3GPP AAA Server, the Non-3GPP access network shall send an STR with the Termination-Cause set to DIAMETER_ADMINISTRATIVE. The 3GPP AAA Server shall set the Result-Code to DIAMETER_SUCCESS and return the STA command to the Non-3GPP access network.

5.1.2.2.3 3GPP AAA Proxy Detailed Behaviour

When the 3GPP AAA Proxy receives the ASR from the 3GPP AAA Server it shall route the request to the non-3GPP access network.

If the 3GPP AAA Proxy requires an STR but the 3GPP AAA Server does not, the 3GPP AAA Proxy may override the value of the Auth-Session-State AVP in the ASR and set it to STATE_MAINTAINED. In this case, the 3GPP AAA Proxy shall not forward the STR received from the non-3GPP access network onto the 3GPP AAA Server and shall return an STA command to the non-3GPP access network with the Result-Code set to DIAMETER_SUCCESS. The 3GPP AAA Proxy shall not override the value of the Auth-Session-State AVP under any other circumstances.

On receipt of the ASA message with Diameter Result Code set to DIAMETER_SUCCESS, the 3GPP AAA Proxy shall route the successful response to the 3GPP AAA Server and shall release the resources associated with the session.

When the 3GPP AAA Proxy receives the STR from the Non-3GPP access network, it shall route the request to the 3GPP AAA Server. On receipt of the STA message, the 3GPP AAA Proxy shall route the response to the Non-3GPP access network.

5.1.2.3 STa Re-Authorization and Re-Authentication Procedures

5.1.2.3.1 General

The STa Re-Authorization procedure shall be used between the 3GPP AAA Server and the trusted non-3GPP access network for enabling:

- the 3GPP AAA Server to modify the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example, removal of a specific APN associated with the subscriber, or change of the identity of a dynamically allocated PDN GW, or change of the identity of a dynamically allocated PDN GW for emergency services, see clause 8.1.2.3). In this case, this procedure is performed in two steps:

  - The 3GPP AAA server shall issue an STa Re-Auth request towards the trusted non-3GPP access network. Upon receipt of such a request, the trusted non-3GPP access network shall respond to the request and shall indicate the disposition of the request. This procedure is mapped to the Diameter command Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 6733 [58]. Information element contents for these messages are shown in tables 5.1.2.3.1/1 and 5.1.2.3.1/2.

  - Upon receiving the STa Re-Auth request, the non-3GPP access network shall immediately invoke the STa access authorization procedure, based on the reuse of the Diameter command codes AA-Request and AA-Answer commands specified in IETF RFC 4005 [4]. Information element contents for these messages are shown in tables 5.1.2.3.1/3 and 5.1.2.3.1/4.

- the trusted non-3GPP access network to retrieve the subscriber profile from the HSS. This procedure may be initiated at any time by the Trusted non-3GPP access network for check if there is any modification in the user authorization parameters previously provided by the 3GPP AAA Server. In this one-step procedure, the trusted non-3GPP access network shall invoke the STa access authorization procedure, based on the reuse of the Diameter commands AA-Request and AA-Answer commands IETF RFC 4005 [4]. Information element contents for these messages are shown in tables 5.1.2.3.1/3 and 5.1.2.3.1/4.

After receiving the authorization answer, the trusted non-3GPP access network will release the active PDN connections, for which the authorization has been revoked. If the authorization was rejected by the 3GPP AAA server (e.g. because the user's subscription for non-3GPP accesses has been terminated), the non-3GPP access network shall detach the user from the non-3GPP access network and release all resources. If an emergency PDN connection is active and the trusted non-3GPP access supports emergency services for users in limited service state, the non-3GPP access network shall keep the user attached in the non-3GPP access and the emergency PDN connection active. The non-emergency resources shall be released.

The STa Re-Authentication procedure shall be used between the 3GPP AAA Server and the trusted non-3GPP access network for re-authenticating the user. This procedure may be initiated at any time by the 3GPP AAA Server based on HPLMN operator policies configured in the 3GPP AAA server. This procedure is performed in two steps:

- The 3GPP AAA server issues an STa Re-Auth request towards the trusted non-3GPP access. Upon receipt of such a request, the trusted non-3GPP access network shall respond to the request and indicate the disposition of the request. This procedure is mapped to the Diameter command Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 6733 [58]. Information element contents for these messages are shown in tables 5.1.2.3.1/1 and 5.1.2.3.1/2.

- Upon receiving the STa Re-Auth request, the trusted non-3GPP access network shall immediately invoke the STa Access Authentication and Authorization procedure, based on the Re-Auth Request Type provided by the 3GPP AAA server. This procedure is mapped to the Diameter command codes based on the reuse of the Diameter commands Diameter-EAP-Request and Diameter-EAP-Answer specified in IETF RFC 4072 [5]. Information element contents for these messages are shown in tables 5.1.2.3.1/5 and 5.1.2.3.1/6.

If the re-authentication of the user is not successful, the trusted non-3GPP access network will release all the active PDN connections of the user, except for emergency PDN connections which shall remain active if the trusted non-3GPP access network supports Emergency services for users in limited service state. After a successful authentication and authorization procedure, the trusted non-3GPP access network shall release the active PDN connections for which the authorization has been revoked.

Table 5.1.2.3.1/1: STa Re-Auth request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Re-Auth Request Type	Re-Auth–Request-Type	M	T This IE shall define whether the user is to be authorized only or authenticated and authorized. In this case, the following values shall be used: AUTHORIZE_AUTHENTICATE if the re-authentication of the user is requested; AUTHORIZE_ONLY if the update of the previously provided user authorization parameters is requested.
Routing Information	Destination-Host	M	This information element shall be obtained from the Origin-Host AVP, which was included in a previous command received from the trusted non-3GPP access.

Table 5.1.2.3.1/2: STa Re-Auth response

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 5.1.2.3.1/3: STa Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14] If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request-Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. In this case, it shall have the value: AUTHORIZE_ONLY
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall contain the mobility capabilities of the non-3GPP access network. This AVP shall be included only if optimized idle mode mobility from E-UTRAN to HRPD access is executed. When included, the PMIP_SUPPORTED and the OPTIMIZED_IDLE_MODE_MOBILITY flags shall be set.
Routing Information	Destination-Host	M	The 3GPP AAA Server name shall be obtained from the Origin-Host AVP of a previously received message.
Access Network Information	Access-Network-Info	O	If present, this IE shall contain the identity and location information of the access network where the UE is attached.
Local Time Zone	Local-Time-Zone	O	If present, this IE shall contain the time zone of the location in the access network where the UE is attached.

Table 5.1.2.3.1/4: STa Authorization response

Information element name	Mapping to Diameter AVP	Cat.	Description
Registration Result	Result Code/ Experimental Result Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP
Request-Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER _SUCCESS; if present, it shall contain the maximum number of seconds the user session is allowed to remain active. This AVP is defined in IETF RFC 6733 [58].
Accounting Interim Interval	Acct-Interim-Interval	O	If present, this IE shall contain the Charging duration.
Default APN	Context-Identifier	C	This AVP shall indicate the default APN for the user. It shall only be included if NBM is authorized for use, the Emergency-Indication AVP was not present in the initial Authentication and Authorization Answer and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is authorized for use, the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Answer and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Answer and the Result-Code AVP is set to DIAMETER_SUCCESS. When NBM is authorized for use, this AVP shall contain the default APN, the list of authorized APNs, user profile information and PDN GW information. When local IP address assignment is used (for HBM), this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes. The Trusted Non-3GPP access network knows if NBM is authorized for use or if a local IP address (for HBM) is assigned based on the flags in the MIP6-Feature-Vector received during the STa access authentication and authorization procedure. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is authorized for use, the following information elements per APN may be included: - APN - APN-AMBR - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - Visited Network Identifier (see clause 5.1.2.1.4) When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included: - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14]) - Authorized 3GPP QoS profile - PDN GW identity
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
UE AMBR	AMBR	C	This Information Element shall contain the modified UE AMBR of the user. It shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS and ANID is "HRPD".

Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall only be sent if it has been received in the corresponding authorization request and the Result-Code AVP is set to DIAMETER_SUCCESS. When included, the PMIP_SUPPORTED and the OPTIMIZED_IDLE_MODE_MOBILITY flags shall be set.
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the trusted non-3GPP access network. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth-List - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent if it is available and the Result-Code AVP is set to DIAMETER_SUCCESS.
Emergency Info	Emergency-Info	C	This IE shall contain the identity of the PDN GW dynamically allocated for emergency services. It shall be present for a non-roaming authenticated user, if this information was received from the HSS, the TWAN indicated support of IMS Emergency Sessions and the Result-Code AVP is set to DIAMETER_SUCCESS.
UE Usage Type	UE-Usage-Type	C	This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the UE Usage Type of the subscriber.

Table 5.1.2.3.1/5: STa Access Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and it shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. In this case, it shall have the value AUTHORIZE_AUTHENTICATE.

Table 5.1.2.3.1/6: Trusted non-3GPP Access Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and it shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State.
EAP payload	EAP payload	M	This IE shall contain the Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental Result Code	M	This IE shall contain the result of the operation. Result codes are as in Diameter base protocol (see IETF RFC 6733 [58]). Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Session Alive Time	Session-Timeout	O	This AVP may be present if the Result-Code AVP is set to DIAMETER _SUCCESS; if present, it contains the maximum number of seconds the user session is allowed to remain active. This AVP is defined in IETF RFC 6733 [58].
Accounting Interim Interval	Accounting Interim-Interval	O	If present, this IE shall contain the Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	This IE shall be sent if Result-Code AVP is set to DIAMETER_SUCCESS.
Default APN	Context-Identifier	C	This AVP shall indicate the default APN for the user. It shall only be included if NBM is authorized for use, the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Answer and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is authorized for use, the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Answer and the Result-Code AVP is set to DIAMETER_SUCCESS.

APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the non-3GPP access network was decided to be trusted, the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Answer and the Result-Code AVP is set to DIAMETER_SUCCESS. When NBM is authorized for use this AVP shall contain the default APN, the list of authorized APNs, user profile information and PDN GW information. When local IP address assignment is used (for HBM), this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes. The trusted non-3GPP access network knows if NBM is authorized for use or if a local IP address (for HBM) is assigned based on the flags in the MIP6-Feature-Vector. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is authorized for use, the following information elements per APN may be included: - APN - APN-AMBR - Authorized 3GPP QoS profile - User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - APN-AMBR - Visited Network Identifier (see clause 5.1.2.1.4) When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included: - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14]) - Authorized 3GPP QoS profile - PDN GW identity
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
UE AMBR	AMBR	C	This Information Element shall contain the UE AMBR of the user. It shall be present only if the non-3GPP access network was decided to be trusted, the Result-Code AVP is set to DIAMETER_SUCCESS and ANID is "HRPD".
FA-RK	MIP-FA-RK	C	This AVP shall be present if MIPv4 is used, MN-FA authentication extension is supported and the Result-Code AVP is set to DIAMETER_SUCCESS.
FA-RK-SPI	MIP-FA-RK-SPI	C	This AVP shall be present if MIP-FA-RK is present
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the trusted non-3GPP access network. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth-List - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent if it is available and the Result-Code AVP is set to DIAMETER_SUCCESS.

WLCP Key	WLCP-Key	C	This IE shall be present if the Result-Code AVP is set to DIAMETER_SUCCESS and the TWAN Connection Mode previously selected is MCM. If present, it shall contain the key for protecting WLCP signalling (see 3GPP TS 33.402 [19]).
Emergency Info	Emergency-Info	C	This IE shall contain the identity of the PDN GW dynamically allocated for emergency services. It shall be present for a non-roaming authenticated user, if this information was received from the HSS, the TWAN indicated support of IMS Emergency Sessions and the Result-Code AVP is set to DIAMETER_SUCCESS.
UE Usage Type	UE-Usage-Type	C	This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the UE Usage Type of the subscriber.

5.1.2.3.2 3GPP AAA Server Detailed Behaviour

Handling of Re-Auth Request:

The 3GPP AAA Server shall make use of this procedure to indicate the following:

- If the relevant service authorization information shall be updated in the Trusted non-3GPP access network, the Re-Auth-Request-Type shall be set to AUTHORIZE_ONLY. This procedure may be triggered by the HSS sending a subscription data update (refer to clause 8.1.2.3) or by local policies, e.g. periodic re-authorization configured by the operator. As for the STa reference point, only a single Diameter authorization session is used for a user, this procedure is initiated for all the PDN connections of this user, i.e. a single instance of Re-authorization Request shall be used per user.

- If the re-authentication and re-authorization of the user shall be executed, the Re-Auth-Request-Type shall be set to AUTHORIZE_AUTHENTICATE. This procedure may be triggered e.g. by the expiration of a timer started at the successful completion of the last (re-)authentication of the user, depending on the local policies configured in the 3GPP AAA Server.

Handling of Authorization Request:

The 3GPP AAA Server shall check that the user exists in the 3GPP AAA Server. The check shall be based on Diameter Session-Id. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN. If the user exists, the 3GPP AAA Server shall perform the authorization checking described in clause 5.1.2.1.2.

If the Authorization request contained the MIP6-Feature-Vector with the OPTIMIZED_IDLE_MODE_MOBILITY flag set, the 3GPP AAA server shall request the user data from the HSS, in order to retrieve up-to-date PDN GW information.

Handling of Authentication and Authorization Requests:

The 3GPP AAA Server shall execute the re-authentication of the user, using a full authentication or fast re-authentication, as described in 3GPP TS 33.402 [19], clause 6.2 and 6.3. If full authentication is executed and there are no valid authentication vectors for the given non-3GPP access network available in the 3GPP AAA Server, it shall fetch authentication vectors from the HSS. A combined authentication and authorization shall be executed, with reduced message content described in Tables 5.1.2.3.1/5 and 5.1.2.3.1/6. The QoS-Capability, Access Network Identity, Access Type, Visited Network Identifier, Terminal Information elements received during the initial authentication and authorization procedure as well as the trustworthiness of the non-3GPP AN and the IP mobility mode selected during that procedure shall be considered as valid. If re-authentication of the user is successful and MIPv4 FACoA mode is used the 3GPP AAA Server shall create the MIPv4 FACoA security parameters as defined in 3GPP TS 33.402 [19].

If the re-authentication of the user is unsuccessful, the 3GPP AAA Server shall:

- Terminate all S6b authorization sessions connected to the user, as described in clause 9.1.2.4

- Remove all APN-PDN GW bindings from the HSS, as described in clauses 8.1.2.2.2.1 and 8.1.2.2.2.2.

- De-register the user from the HSS, as described in clauses 8.1.2.2.2.1 and 8.1.2.2.2.2. Depending on the cause of the re-authentication being unsuccessful, the Server Assignment Type shall be set to AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT.

- Release all resources connected to the user.

5.1.2.3.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the Non-3GPP access network is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy, with the following additions.

When forwarding the authorization answer or the authentication and authorization answer, the 3GPP AAA Proxy

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authentication and Authorization Successful).

5.1.2.3.4 Trusted Non-3GPP Access Network Detailed Behaviour

Upon receiving the re-auth request, the Trusted non-3GPP access network shall perform the following checks and if an error is detected, the non-3GPP access network shall stop processing the request and return the corresponding error code.

Check the Re-Auth–Request-Type AVP:

1) If it indicates AUTHENTICATE_ONLY, Result-Code shall be set to DIAMETER_INVALID_AVP_VALUE.
2) If it indicates AUTHORIZE_AUTHENTICATE, the authentication and authorization of the user is initiated, as defined in 3GPP TS 33.402, with the Diameter message contents described by Tables 5.1.2.3.1/5 and 5.1.2.3.1/6.
3) If it indicates AUTHORIZE_ONLY, the non-3GPP access network shall just perform an authorization procedure as described by Tables 5.1.2.3.1/3 and 5.1.2.3.1/4.

After successful authorization or authentication and authorization procedure, the trusted non-3GPP access network shall overwrite, for the subscriber identity indicated in the request and the received session, the current authorization information with the information received from the 3GPP AAA Server.

For the TWAN access, if the TWAN receives the PDN GW Identity from 3GPP AAA Server which is different from the currently selected PDN GW for the same APN, the TWAN shall not tear down the existing PDN connection.

If the TWAN supports Dedicated Core Networks and receives the UE-Usage-Type from the 3GPP AAA Server, the TWAN shall select the PGW as specified in clause 5.8 of 3GPP TS 29.303 [34] for new PDN connections.

The release of a PDN connection shall be initiated if the user's subscription for the APN belonging to an active PDN connection has been terminated.

If the authorization or authentication and authorization procedure was unsuccessful, the non-3GPP access network shall detach the user from the non-3GPP access and release all resources. If the trusted non-3GPP access supports emergency services for users in limited service state, and there is an emergency PDN connection active for such user, the non-3GPP access network shall keep the user attached in the non-3GPP access and the emergency PDN connection active. The non-emergency resources shall be released.

The Trusted Non-3GPP access network shall initiate the re-authorization of the user in a one-step procedure (i.e. without receiving a re-authorization request from the AAA Server) if the PDN GW information needs to be updated for optimized idle mode mobility from E-UTRAN to HRPD access.

If GTPv2 is used on S2a and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the trusted non-3GPP access network shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user. If the Trace-Info AVP including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the trusted non-3GPP access network shall send a GTPv2 Trace Session Deactivation message to the PGW to stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

For the TWAN access, the TWAN shall send the identification, location information of the Access Point where the UE is attached, and the local time zone of the UE, in the authorization request towards the 3GPP AAA Server that follows a re-authorization request issued by the 3GPP AAA Server to the TWAN.

5.1.2.4 Non-3GPP Access Network Initiated Session Termination

5.1.2.4.1 General

The STa reference point allows the non-3GPP access network to inform the 3GPP AAA server that the session resources of the non-3GPP access network assigned to a given user are being released.

The procedure shall be initiated by the non-3GPP access network and removes non-3GPP access information from the 3GPP AAA Server. These procedures are based on the reuse of Diameter STR and STA commands as specified in IETF RFC 6733 [58].

Table 5.1.2.4.1/1: STa Session Termination Request

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user in NAI format as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Termination Cause	Termination-Cause	M	This IE shall contain the reason for the disconnection.

Table 5.1.2.4.1/2: STa Session Termination Answer

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors as defined in the Diameter base protocol (see IETF RFC 6733 [58]). Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

5.1.2.4.2 3GPP AAA Server Detailed Behaviour

Upon reception of the Session Termination Request message from the non-3GPP access network, the 3GPP AAA Server shall check that there is an ongoing session associated to the two parameters received (Session-Id and User-Name).

If an active session is found and it belongs to the user identified by the User-Name parameter, the 3GPP AAA Server shall deregister itself as the managing 3GPP AAA Server for the subscriber following the procedures listed in 8.1.2.2.2. In case of a deregistration success, the 3GPP AAA Server shall release the session resources associated to the specified session and a Session Termination Response shall be sent to the non-3GPP access network, indicating DIAMETER_SUCCESS. If deregistration from the HSS fails, the 3GPP AAA Server shall return a Session-Termination Response with the Diameter Error DIAMETER_UNABLE_TO_COMPLY.

Otherwise, the 3GPP AAA Server returns a Session Termination Response with the Diameter Error DIAMETER_UNKNOWN_SESSION_ID

5.1.2.4.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the non-3GPP access network is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Session Termination Request message from the non-3GPP access network, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server.

On receipt of the Session Termination Answer message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the non-3GPP access network and it shall release any local resources associated to the specified session only if the result code is set to DIAMETER_SUCCESS.

5.1.2.5 ERP Re-Authentication in Non-3GPP Access

5.1.2.5.1 General

The STa reference point allows the non-3GPP access network to perform re-authentication using ERP.

ERP allows the UE and the ER server to mutually verify proof of possession of key material derived from a previous successful EAP authentication and to establish a security association between the UE and the non-3GPP access network.

When this procedure is used, the ER server is collocated either with a TWAP or the 3GPP AAA Proxy or the 3GPP AAA Server. When the ER is located in the TWAP, ERP re-authentication procedures are out of the scope of this specification.

When ERP is used, the ERP re-authentication procedure shall be mapped to the Diameter-EAP-Request and Diameter-EAP-Answer command codes specified in IETF RFC 4072 [5].

Table 5.1.2.5.1/1: STa ERP Re-authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
KeyName-NAI	User-Name	M	This information element shall contain the KeyName-NAI (as defined in clause 19.3.8 of 3GPP TS 23.003 [14]) in the context of EAP re-authentication using ERP as described in IETF RFC 6696 [55] and 3GPP TS 33.402 [19].
EAP-Initiate	EAP-payload	M	This IE shall contain the EAP-Initiate/Re-auth message used for the UE – ER Server mutual authentication.
Authentication Request Type	Auth-Request-Type	M	This IE defines whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
DER-Flags	DER-Flags	M	This Information Element contains a bit mask. See clause 5.2.3.20.

Table 5.1.2.5.1/2: STa ERP Re-authentication Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
KeyName-NAI	User-Name	M	This information element shall contain the KeyName-NAI (as defined in clause 19.3.8 of 3GPP TS 23.003 [14]) in the context of EAP re-authentication using ERP as described in IETF RFC 6696 [55] and 3GPP TS 33.402 [19].
EAP-Finish	EAP payload	O	If present, this IE shall contain the EAP-Finish as described in IETF RFC 6942 [57].
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental Result Code	M	This IE shall contain the result of the operation. Result codes are as in Diameter Base Protocol (IETF RFC 3588 [7]). Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
ERP Keying Material	Key	C	This IE shall be present if the ERP re-authentication is successful. In that case, this IE shall contain the Re-authentication MSK (rMSK) derived by ERP and may contain the rMSK lifetime.

5.1.2.5.2 ER server located in 3GPP AAA Proxy or 3GPP AAA Server Detailed Behaviour

Upon reception of the ERP re-authentication request from the non-3GPP access network, the 3GPP AAA Proxy or the 3GPP AAA Server acting as ER server shall search in its local database for a valid, unexpired root key matching the keyName part of the KeyName-NAI.

If the root key is not found, the 3GPP AAA Proxy or 3GPP AAA Server shall set the Result-Code to DIAMETER_UNABLE_TO_COMPLY and the answer shall include an EAP-Payload AVP encapsulating an EAP Failure indicating that the ERP re-authentication has failed.

If such root key is found, the 3GPP AAA Server shall generate the ERP keying material as described in IETF RFC 6696 [55], shall include the requested ERP keying material in the answer and the result code shall be set to DIAMETER_SUCCESS.

NOTE: Only the ERP Implicit Bootstrapping mode defined in IETF RFC 6696 [55] is supported in this release.

5.1.2.5.3 3GPP AAA Proxy Detailed Behaviour

Upon reception of the ERP authentication request from the non-3GPP access network, the 3GPP AAA Proxy shall check if the realm part of the KeyName-NAI is its own domain name. If not, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY.

If the keyName part of the KeyName-NAI is its own domain name, the 3GPP AAA Proxy shall behave as described in clause 5.1.2.5.2.

NOTE: In roaming case, the location of the ER server in the home 3GPP AAA Server is not supported in this release.

5.2 Protocol Specification

5.2.1 General

The STa reference point shall be based on Diameter, as defined in IETF RFC 6733 [58], and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 4072 [5], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [8]) frames over Diameter.
- IETF RFC 5779 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5447 [6], which defines Diameter extensions for Mobile IPv6 NAS to AAA interface.

In the case of a trusted non-3GPP IP access where PMIPv6 is used as mobility protocol, the MAG to 3GPP AAA server or the MAG to 3GPP AAA proxy communication shall use the MAG to AAA interface functionality defined in IETF RFC 5779 [2] and the NAS to AAA interface functionality defined in IETF RFC 5447 [6].

The trusted non-3GPP access network to AAA interface functionality over the STa reference defines a new Application Id:

- "STa" with value 16777250.

The STa application reuses existing EAP (IETF RFC 4072 [5]) application commands, command ABNFs, and application logic and procedures.

5.2.2 Commands

5.2.2.1 Commands for STa PMIPv6 or GTPv2 or ERP (re-)authentication and authorization procedures

5.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a non-3GPP access network NAS to a 3GPP AAA server. The ABNF is re-used from the IETF RFC 5779 [2].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777250 >
                             < Session-Id >
                             [ DRMP ]
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             [ Destination-Host ]
                             { Auth-Request-Type }
                             { EAP-Payload }
                             [ User-Name ]
                             [ Calling-Station-Id ]
                             …
                             [ RAT-Type ]
                             [ ANID ]
                             [ Full-Network-Name ]
                             [ Short-Network-Name ]
                             [ QoS-Capability ]
                             [ MIP6-Feature-Vector ]
                             [ Visited-Network-Identifier ]
                             [ Service-Selection ]
                             [ Terminal-Information ]
                             [ OC-Supported-Features ]
                             *[ Supported-Features ]
                             [ AAA-Failure-Indication ]
                             [ WLAN-Identifier ]
                             [ DER-Flags ]
                             [ TWAN-Connection-Mode ]
                             [ TWAN-Connectivity-Parameters ]
                             * 2 [ TWAG-CP-Address ]
                             [ ERP-RK-Request ]
                             …
                             *[ AVP ]
```

5.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server to a non-3GPP access network NAS. The ABNF is re-used from the IETF RFC 5779 [2]. The ABNF also contains AVPs that are reused from IETF RFC 4072 [5].

```
< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >
                            < Session-Id >
                            [ DRMP ]
                            { Auth-Application-Id }
                            { Result-Code }
                            [ Experimental-Result ]
                            { Origin-Host }
                            { Origin-Realm }
                            { Auth-Request-Type }
```

[EAP-Payload]
[User-Name]
[Session-Timeout]
[Accounting-Interim-Interval]
[EAP-Master-Session-Key]
[Context-Identifier]
[APN-OI-Replacement]
*[APN-Configuration]
[MIP6-Agent-Info]
[MIP6-Feature-Vector]
[Mobile-Node-Identifier]
[3GPP-Charging-Characteristics]
[AMBR]
*[Redirect-Host]
[AN-Trusted]
[Trace-Info]
[Subscription-ID]
[OC-Supported-Features]
[OC-OLR]
*[Load]
*[Supported-Features]
[MIP-FA-RK]
[MIP-FA-RK-SPI]
[NSWO-Authorization]
[DEA-Flags]
[TWAN-Connection-Mode]
[TWAN-Connectivity-Parameters]
[WLCP-Key]
[Terminal-Information]
[UE-Usage-Type]
[Emergency-Services]
[Emergency-Info]
[Key]
[ERP-Realm]
…
*[AVP]

5.2.2.2 Commands for STa HSS/AAA Initiated Detach for Trusted non-3GPP Access

5.2.2.2.1 Abort-Session-Request (ASR) Command

The Abort-Session-Request (ASR) command, indicated by the Command-Code field set to 274 and the "R" bit set in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a non-3GPP access network NAS. ABNF for the ASR commands is as follows:

< Abort-Session-Request > ::= < Diameter Header: 274, REQ, PXY, 16777250 >
< Session-Id >
[DRMP]
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Destination-Host }
{ Auth-Application-Id }
[User-Name]
[Auth-Session-State]
…
*[AVP]

5.2.2.2.2 Abort-Session-Answer (ASA) Command

The Abort-Session-Answer (ASA) command, indicated by the Command-Code field set to 274 and the "R" bit cleared in the Command Flags field, is sent from a non-3GPP access network NAS to a 3GPP AAA Server/Proxy. ABNF for the ASA commands is as follows:

```
< Abort-Session-Answer >  ::= < Diameter Header: 274, PXY, 16777250 >
                              < Session-Id >
                              [ DRMP ]
                              { Result-Code }
                              { Origin-Host }
                              { Origin-Realm }
                              …
                              *[ AVP ]
```

5.2.2.2.3 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a trusted non-3GPP access network to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58], Session-Termination-Request command.

```
<Session-Termination-Request> ::=  < Diameter Header: 275, REQ, PXY, 16777250 >
                                   < Session-Id >
                                   [ DRMP ]
                                   { Origin-Host }
                                   { Origin-Realm }
                                   { Destination-Realm }
                                   [ Destination-Host ]
                                   { Auth-Application-Id }
                                   { Termination-Cause }
                                   [ User-Name ]
                                   [ OC-Supported-Features ]
                                   …
                                   *[ AVP ]
```

5.2.2.2.4 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a trusted non-3GPP access network. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58], Session-Termination-Answer command.

```
<Session-Termination-Answer> ::=  < Diameter Header: 275, PXY, 16777250 >
                                  < Session-Id >
                                  [ DRMP ]
                                  { Result-Code }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  [ OC-Supported-Features ]
                                  [ OC-OLR ]
                                  *[ Load ]
                                  *[ AVP ]
```

5.2.2.3 Commands for Re-Authentication and Re-Authorization Procedure

5.2.2.3.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command, indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, is sent from a 3GPP AAA Server to a Trusted Non-3GPP access network. ABNF for the RAR command is as follows:

```
< Re-Auth-Request > ::=  < Diameter Header: 258, REQ, PXY, 16777250 >
                         < Session-Id >
                         [ DRMP ]
                         { Origin-Host }
                         { Origin-Realm }
                         { Destination-Realm }
                         { Destination-Host }
                         { Auth-Application-Id }
                         { Re-Auth-Request-Type }
                         [ User-Name ]
                         …
                         *[ AVP ]
```

5.2.2.3.2 Re-Auth-Answer (RAA) Command

The Diameter Re-Auth-Answer (ASA) command, indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field, is sent from a Trusted Non-3GPP access network to a 3GPP AAA Server/Proxy. ABNF for the RAA commands is as follows:

```
< Re-Auth-Answer > ::=  < Diameter Header: 258, PXY, 16777250 >
                        < Session-Id >
                        [ DRMP ]
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        …
                        *[ AVP ]
```

5.2.2.3.3 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a Trusted Non-3GPP access network to a 3GPP AAA Server/Proxy. The ABNF is re-used from IETF RFC 4005 [4], adding AVPs from IETF RFC 5779 [2].

```
< AA-Request > ::= < Diameter Header: 265, REQ, PXY, 16777250 >
                   < Session-Id >
                   [ DRMP ]
                   { Auth-Application-Id }
                   { Origin-Host }
                   { Origin-Realm }
                   { Destination-Realm }
                   { Auth-Request-Type }
                   [ Destination-Host ]
                   [ User-Name ]
                   [ MIP6-Feature-Vector ]
                   [ Access-Network-Info ]
                   [ Local-Time-Zone ]

                   [ OC-Supported-Features ]
                   …
                   *[ AVP ]
```

5.2.2.3.4 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a Trusted Non-3GPP access network. The ABNF is re-used from IETF RFC 4005 [4], adding AVPs from IETF RFC 5779 [2].

```
< AA-Answer > ::=  < Diameter Header: 265, PXY, 16777250 >
                   < Session-Id >
```

[DRMP]
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
[Experimental-Result]
{ Origin-Host }
{ Origin-Realm }
[Session-Timeout]
[Accounting-Interim-Interval]
[Context-Identifier]
[APN-OI-Replacement]
*[APN-Configuration]
[3GPP-Charging-Characteristics]
[Trace-Info]
[Subscription-ID]
[OC-Supported-Features]
[OC-OLR]
[UE-Usage-Type]
[Emergency-Info]
*[Load]
…
*[AVP]

5.2.2.3.5 Diameter-EAP-Request (DER) Command

Refer to clause 5.2.2.1.1

5.2.2.3.6 Diameter-EAP-Answer (DEA) Command

Refer to clause 5.2.2.1.2

5.2.2.4 Commands for Trusted non-3GPP Access network Initiated Session Termination

5.2.2.4.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a non-3GPP access network to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58], Session-Termination-Request command.

<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777250 >
< Session-Id >
[DRMP]
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ Auth-Application-Id }
{ Termination-Cause }
[User-Name]
[OC-Supported-Features]
…
*[AVP]

5.2.2.4.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a non-3GPP access network. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58], Session-Termination-Answer command.

<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777250 >
< Session-Id >

[DRMP]
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[OC-Supported-Features]
[OC-OLR]
*[Load]
*[AVP]

5.2.3 Information Elements

5.2.3.1 General

The following table describes the Diameter AVPs defined for the STa interface protocol in NBM mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

Table 5.2.3.1/1: Diameter STa AVPs

	AVP Flag rules

Attribute Name	AVP Code	Clause defined	Value Type	Must	May	Should not	Must not
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V,P
QoS-Capability	578	5.2.3.4	Grouped	M			V,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
RAT-Type	1032	5.2.3.6	Enumerated	M,V			P
ANID	1504	5.2.3.7	UTF8String	M,V			P
AN-Trusted	1503	5.2.3.9	Enumerated	M,V			P
MIP-FA-RK	1506	5.2.3.12	OctetString	M,V			P
MIP-FA-RK-SPI	1507	5.2.3.13	Unsigned32	M,V			P
Full-Network-Name	1516	5.2.3.14	OctetString	V			M,P
Short-Network-Name	1517	5.2.3.15	OctetString	V			M,P
WLAN-Identifier	1509	5.2.3.18	Grouped	V			M,P
Mobile-Node-Identifier	506	5.2.3.2	UTF8String	M			V,P
AAA-Failure-Indication	1518	8.2.3.21	Unsigned32	V			M,P
Transport-Access-Type	1519	5.2.3.19	Enumerated	V			M,P
APN-Configuration	1430	8.2.3.7	Grouped	M,V			P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
DER-Flags	1520	5.2.3.20	Unsigned32	V			M,P
DEA-Flags	1521	5.2.3.21	Unsigned32	V			M,P
SSID	1524	5.2.3.22	UTF8String	V			M,P
HESSID	1525	5.2.3.23	UTF8String	V			M,P
Access-Network-Info	1526	5.2.3.24	Grouped	V			M,P
TWAN-Connection-Mode	1527	5.2.3.25	Unsigned32	V			M,P
TWAN-Connectivity-Parameters	1528	5.2.3.26	Grouped	V			M,P
Connectivity-Flags	1529	5.2.3.27	Unsigned32	V			M,P
TWAN-PCO	1530	5.2.3.28	OctetString	V			M,P
TWAG-CP-Address	1531	5.2.3.29	Address	V			M,P
TWAG-UP-Address	1532	5.2.3.30	UTF8String	V			M,P
TWAN-S2a-Failure-Cause	1533	5.2.3.31	Unsigned32	V			M,P
SM-Back-Off-Timer	1534	5.2.3.32	Unsigned32	V			M,P
WLCP-Key	1535	5.2.3.33	OctetString	V			M,P
Emergency-Services	1538	7.2.3.4	Unsigned32	V			M,P
IMEI-Check-In-VPLMN-Result	1540	5.2.3.35	Unsigned32	V			M,P

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 [58],.

NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.

The following table describes the Diameter AVPs re-used by the STa interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within STa. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol defined in IETF RFC 6733 [58], do not need to be supported.

Table 5.2.3.1/2: STa re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
Accounting-Interim-Interval	IETF RFC 6733 [58]		
Auth-Request-Type	IETF RFC 6733 [58]		
Calling-Station-Id	IETF RFC 4005 [4]		
Subscription-ID	IETF RFC 4006 [20]		Must not set
EAP-Master-Session-Key	IETF RFC 4072 [5]		
EAP-Payload	IETF RFC 4072 [5]		
RAT-Type	3GPP TS 29.212 [23]		
Re-Auth-Request-Type	IETF RFC 6733 [58]		
Session-Timeout	IETF RFC 6733 [58]		
User-Name	IETF RFC 6733 [58]		
Terminal-Information	3GPP TS 29.272 [29]		
MIP6-Agent-Info	IETF RFC 5447 [6]		
APN-OI-Replacement	3GPP TS 29.272 [29]		
Supported-Features	3GPP TS 29.229 [24]		
Feature-List-ID	3GPP TS 29.229 [24]	See clause 5.2.3.10	
Feature-List	3GPP TS 29.229 [24]	See clause 5.2.3.11	
BSSID	3GPP TS 32.299 [30]		
Location-Information	IETF RFC 5580 [46]		
Location-Data	IETF RFC 5580 [46]		
Operator-Name	IETF RFC 5580 [46]		
Logical-Access-ID	ETSI TS 283 034 [48]		
Local-Time-Zone	3GPP TS 29.272 [29]		
PDN-Type	3GPP TS 29.272 [29]		
Served-Party-IP-Address	3GPP TS 32.299 [30]		
OC-Supported-Features	IETF RFC 7683 [47]	See clause 8.2.3.22	
OC-OLR	IETF RFC 7683 [47]	See clause 8.2.3.23	
DRMP	IETF RFC 7944 [53]	See clause 8.2.3.25	Must not set
Emergency-Info	3GPP TS 29.272 [29]		
Load	IETF RFC 8583 [54]	See clause 8.2.3.26	Must not set
ERP-RK-Request	IETF RFC 6942 [57]		Must not set
Key	IETF RFC 6734 [56]	This is a grouped AVP containing Key-Type, Keying-Material and, optionally, Key-Lifetime.	Must not set
ERP-Realm	IETF RFC 6942 [57]		Must not set
UE-Usage-Type	3GPP TS 29.272 [29]		

NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.

NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.

Only those AVP initially defined in this reference point or AVP with values initially defined in this reference point and for this procedure are described in the following clause.

5.2.3.2 Mobile-Node-Identifier

The Mobile-Node-Identifier AVP (AVP Code 506) is of type UTF8String.

The Mobile-Node-Identifier AVP is returned in an answer message that ends a successful authentication (and possibly an authorization) exchange between the AAA client and the AAA server. The returned Mobile Node Identifier may be used as the PMIPv6 MN-ID or as the MIPv4 MN-NAI or to derive the IMSI to be sent in GTPv2 signalling.

The Mobile-Node-Identifier is defined on IETF RFC 5779 [2].

5.2.3.3 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP (AVP Code 124) is of type Unsigned64 and contains a 64 bit flags field of supported mobile IP capabilities of the non-3GPP access network (when this AVP is used in the request commands) and the mobile IP capabilities the 3GPP AAA Server has authorized (when this AVP is used in the response commands).

The following capabilities are defined for STa interface:

- MIP6_INTEGRATED (0x0000000000000001)
  This flag is set by the non-3GPP access network and the 3GPP AAA Server. It means that the Mobile IPv6 integrated scenario bootstrapping functionality is supported.

- PMIP6_SUPPORTED (0x0000010000000000)
  When this flag is set by the non-3GPP access network it indicates to the 3GPP AAA Server that it supports PMIPv6.
  When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that NBM shall be used.

- ASSIGN_LOCAL_IP (0x0000080000000000)
  This flag is set by the 3GPP AAA Server.
  When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that the non-3GPP access network shall assign to the user a local IP address (for HBM).

- MIP4_SUPPORTED (0x0000100000000000)
  This flag is set by the non-3GPP access network, the PDN GW and the 3GPP AAA Server. When this flag is set by the non-3GPP access network it indicates to the 3GPP AAA Server that it supports MIPv4 FA-CoA mode. When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that MIPv4 FA-CoA mode shall be used. When this flag is set by the PDN GW and 3GPP AAA Server over the S6b interface, it shows that MIPv4 mobility protocol is used on the S2a interface.

- OPTIMIZED_IDLE_MODE_MOBILITY (0x0000200000000000)
  This flag is set by the Trusted Non-3GPP access network if the PDN GW information needs to be updated for the case of idle mode mobility from E-UTRAN to HRPD access.

- GTPv2_SUPPORTED (0x0000400000000000)
  When this flag is set by the non-3GPP access network it indicates to the 3GPP AAA Server that it supports GTPv2.
  When this flag is set by the 3GPP AAA Server it indicates to the non-3GPP access network that NBM shall be used.

5.2.3.4 QoS Capability

This AVP is FFS

5.2.3.5 Service-Selection

The Service-Selection AVP is of type of UTF8String. This AVP contains an APN Network Identifier (i.e., an APN without the Operator Identifier), and it shall consist of one or more labels according to DNS naming conventions (IETF RFC 1035 [35]) describing the access point to the packet data network.

The contents of the Service-Selection AVP shall be formatted as a character string composed of one or more labels separated by dots (".").

The Service-Selection AVP is defined in IETF RFC 5778 [11].

5.2.3.6 RAT-Type

The RAT-Type AVP (AVP code 1032) is of type Enumerated and is used to identify the radio access technology that is serving the UE. It follows the specification described in TS 29.212 [23].

5.2.3.7 ANID

The ANID AVP is of type UTF8String; this AVP contains the Access Network Identity; see 3GPP TS 24.302 [26] for defined values.

5.2.3.8 AMBR

Please refer to 3GPP TS 29.272 [29] for the encoding of this AVP.

5.2.3.9 AN-Trusted

The AN-Trusted AVP (AVP Code 1503) is of type Enumerated.

The AN-Trusted AVP sent from the 3GPP AAA Server to the Non-3GPP access network conveys the decision about the access network being trusted or untrusted by the HPLMN.

The following values are defined:

TRUSTED (0)

This value is used when the non-3GPP access network is to be handled as trusted.

UNTRUSTED (1)

This value is used when the non-3GPP access network is to be handled as untrusted.

5.2.3.10 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the STa/SWa application.

5.2.3.11 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the STa/SWa application.

NOTE: There are no STa/SWa features defined for this release.

5.2.3.12 MIP-FA-RK

The MIP-FA-RK AVP is of type OctetString; this AVP contains the FA-RK used to calculate the security parameters needed for the MN-FA authentication extension as defined by 3GPP TS 33.402 [19].

5.2.3.13 MIP-FA-RK-SPI

The MIP-FA-RK-SPI AVP is of type Unsigned32; this AVP contains the security index used in identifying the security context for the FA-RK as defined by 3GPP TS 33.402 [19].

5.2.3.14 Full-Network-Name

The Full-Network-Name AVP is of type OctetString; this AVP shall contain the Full Network Name and be encoded as the Full name value field of the AT_FULL_NAME_FOR_NETWORK attribute specified in clause 8.2.5.1 of 3GPP TS 24.302 [26].

5.2.3.15 Short-Network-Name

The Short-Network-Name AVP is of type OctetString; this AVP shall contain the Short Network Name and be encoded as the Short name value field of the AT_SHORT_NAME_FOR_NETWORK attribute specified in clause 8.2.5.2 of 3GPP TS 24.302 [26].

5.2.3.16 Void

5.2.3.17 Void

5.2.3.18 WLAN-Identifier

The WLAN-Identifier AVP is of type Grouped. It contains the type and value of an IEEE 802.11 identifier of a Trusted WLAN.

AVP Format:

```
WLAN-Identifier ::= < AVP Header: 1509 10415 >
                    [SSID ]
                    [HESSID ]
                    *[ AVP ]
```

5.2.3.19 Transport-Access-Type

The Transport-Acess-Type AVP (AVP code 1519) is of type Enumerated and is used to identify the transport access technology that is serving the UE.

The following values are defined:

BBF (0)

This value shall be used to indicate a BBF transport access network.

5.2.3.20 DER-Flags

The DER-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 5.2.3.20/1:

Table 5.2.3.20/1: DER-Flags

Bit	Name	Description
0	NSWO-Capability-Indication	This bit, when set, indicates to the 3GPP AAA proxy/server that the TWAN supports non-seamless WLAN offload service (see clause 16 of 3GPP TS 23.402 [3]).
1	TWAN-S2a-Connectivity-Indicator	This bit is only applicable to the TWAN authentication and authorization procedure, when authorizing the SCM for EPC access. When set, it indicates to the 3GPP AAA Server that the TWAN has completed the necessary S2a network connectivity actions, and the 3GPP AAA Sever can finalize the EAP conversation by sending a final EAP 'Success' or 'Failure' response to the TWAN.
2	IMEI-Check-Required-In-VPLMN	This bit is only applicable to the TWAN authentication and authorization procedure, when the UE and the network support Mobile Equipment Identity signalling over trusted WLAN. When set, it indicates to the 3GPP AAA Server that the 3GPP AAA Server shall retrieve the IMEI(SV) from the UE and return it to the VPLMN with the IMEI-Check-Request-In-VPLMN bit set in the DEA-Flags.
3	IMEI-Check-Request-In-VPLMN	This bit is only applicable to the TWAN authentication and authorization procedure, when the UE and the network support Mobile Equipment Identity signalling over trusted WLAN. When set, it indicates that the 3GPP AAA Proxy shall perform the IMEI(SV) check in the VPLMN and send the IMEI check result to the 3GPP AAA Server.
4	Emergency-Capability-Indication	This bit, when set, indicates to the 3GPP AAA Server that the TWAN supports IMS emergency sessions (see clause 4.5.7 of 3GPP TS 23.402 [3]).
5	ERP-Support-Indication	This bit, when set, indicates to the 3GPP AAA proxy/server that the non-3GPP access network supports EAP extensions for the EAP Re-authentication Protocol (ERP).
6	ERP-Re-Authentication	This bit, when set, indicates to the 3GPP AAA proxy/server that the authentication request is sent for EAP re-authentication based on ERP.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

5.2.3.21 DEA-Flags

The DEA-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 5.2.3.21/1:

Table 5.2.3.21/1: DEA-Flags

Bit	Name	Description
0	NSWO-Authorization	This bit, when set, indicates to the TWAN that the non-seamless WLAN offload service is authorized (see clause 16 of 3GPP TS 23.402 [3]).
1	TWAN-S2a-Connectivity-Indicator	This bit is only applicable to the TWAN authentication and authorization procedure, when authorizing the SCM for EPC access; when set, it indicates to the TWAN that the EAP-AKA' authentication has been successful (i.e., the 3GPP AAA Server has checked the validity of the challenge response sent by the UE), and the network connectivity set up may proceed at the TWAN.
2	IMEI-Check-Request-In-VPLMN	This bit is only applicable to the TWAN authentication and authorization procedure, when the UE and the network support Mobile Equipment Identity signalling over trusted WLAN. When set, it indicates that the VPLMN shall perform the IMEI check and return the outcomes to the 3GPP AAA Server.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the recever of the command.		

5.2.3.22 SSID

The SSID AVP is of type UTF8String and it shall contain the Service Set Identifier which identifies a specific 802.11 extended service set (see IEEE Std 802.11-2012 [40]). It shall contain a string of 1 to 32 octets.

5.2.3.23 HESSID

The HESSID AVP is of type UTF8String and it shall contain a 6-octet MAC address that identifies the Homogenous Extended Service Set (see IEEE Std 802.11-2012 [40]). It shall be encoded in upper-case ASCII characters with the octet values separated by dash characters. It shall contain a string of 17 octets. Example: "00-10-A4-23-19-C0".

5.2.3.24 Access-Network-Info

The Access-Network-Info AVP is of type Grouped.

For a Trusted WLAN, it shall contain the SSID of the WLAN and, unless otherwise determined by the TWAN operator's policies, it shall contain at least one of the following elements:

- the BSSID,
- the civic address of the access point to which the UE is attached,
- the Logical Access ID (see ETSI ES 283 034 [48]) associated to the access point to which the UE is attached.

It may also contain the name of the TWAN operator (either a PLMN-ID or an operator name in realm format).

For an untrusted WLAN, it shall contain the same information as specified above for a trusted WLAN, where the operator name indicates the WLAN operator name.

AVP Format:

```
Access-Network-Info ::=     < AVP Header: 1526 10415 >
                                [ SSID ]
                                [ BSSID ]
                                [ Location-Information ]
                                [ Location-Data ]
                                [ Operator-Name ]
                                [ Logical-Access-ID ]
                                *[ AVP ]
```

The Location-Data and Location-Information AVPs are defined in IETF RFC 5580 [46]; the content of Location-Information shall indicate that the encoding follows a civic location profile, by setting the "Code" field to 0.

The Operator-Name AVP is defined in IETF RFC 5580 [46]; the first 8 bits contain the Namespace ID field, whose values are managed by IANA, and are encoded as a single ASCII character. Only values "1" (Realm) and "2" (E212, containing MCC and MNC values) shall be used in this specification.

5.2.3.25 TWAN-Connection-Mode

The TWAN-Connection-Mode AVP (AVP Code 1527) is of type Unsigned32 and it shall contain a 32 bit flags field which is used to indicate the connection modes supported by the TWAN (when this AVP is used in the request commands) and the selected TWAN connection mode the 3GPP AAA Server has authorized (when this AVP is used in the response commands).

Table 5.2.3.25/1: TWAN-Connection-Mode

Bit	Name	Description
0	TSC-MODE	This bit, when set by the TWAN, indicates to the 3GPP AAA Server that the TWAN supports the TSCM.
1	SC-MODE	This bit, when set by the TWAN, indicates to the 3GPP AAA Server that the TWAN supports the SCM. This bit, when set by the 3GPP AAA Server, indicates to the TWAN that the SCM shall be used.
2	MC-MODE	This bit, when set by the TWAN, indicates to the 3GPP AAA Server that the TWAN supports the MCM. This bit, when set by the 3GPP AAA Server, indicates to the TWAN that the MCM shall be used.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

5.2.3.26 TWAN-Connectivity-Parameters

The TWAN-Connectivity-Parameters AVP is of type Grouped.

AVP Format:

```
TWAN-Connectivity-Parameters ::=    < AVP Header: 1528 10415 >
                                    [ Connectivity-Flags ]
                                    [ Service-Selection ]
                                    [ PDN-Type ]
                                    * 2 [ Served-Party-IP-Address ]
                                    [ TWAN-PCO ]
                                    [ TWAG-UP-Address ]
                                    [ TWAN-S2a-Failure-Cause ]
                                    [ SM-Back-Off-Timer ]
                                    *[ AVP ]
```

The Service-Selection AVP indicates the APN requested by the UE (requested connectivity parameters) or the APN selected by the TWAN (provided connectivity parameters). It shall contain both the network identifier part and the operator identifier part of the Access Point Name.

The PDN-Type AVP indicates the PDN type requested by the UE (requested connectivity parameters) or the PDN type allocated by the network (provided connectivity parameter). It may be set to IPv4, IPv6 or IPv4v6.

The UE's Served-Party-IP-Address AVP may be present 0, 1 or 2 times. These AVPs shall be present if the S2a connection was successfully established, and they shall contain either of:

- an IPv4 address, or
- an IPv6 interface identifier, or
- both, an IPv4 address and an IPv6 interface identifier.

For the IPv6 interface identifier, the higher 64 bits of the address shall be set to zero.

The TWAN-S2a-Failure-Cause AVP may be present to indicate the cause of S2a connectivity establishment failure.

The SM-Back-Off-Timer AVP may be present to provide a Session Management back-off timer to be sent to the UE. The exact value of the SM-Back-Off-Timer is operator dependant.

5.2.3.27 Connectivity-Flags

The Connectivity-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 5.2.3.26/1:

Table 5.2.3.26/1: Connectivity-Flags

Bit	Name	Description
0	Initial-Attach-Indicator	This bit may be set by the 3GPP AAA Server. This bit, when set, indicates that a UE performs the Initial Attach procedure from non-3GPP access network. When not set, it indicates that a UE performs the Handover procedure.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.		

5.2.3.28 TWAN-PCO

The TWAN-PCO AVP is of type OctetString and shall contain the Protocol Configuration Options for the UE.

5.2.3.29 TWAG-CP-Address

The TWAG-CP-Address AVP is of type Address and shall contain the TWAG control-plane IPv4 and/or IPv6 address that the TWAG supports, to be used for WLCP by the UE if MCM is selected.

5.2.3.30 TWAG-UP-Address

The TWAG-UP-Address AVP is of type UTF8String and shall contain a 6-octet MAC address that identifies the TWAG user-plane MAC address to be used for encapsulating user plane packets between the UE and the TWAN, when SCM is used.

It shall be encoded in upper-case ASCII characters with the octet values separated by dash characters. It shall contain a string of 17 octets. Example: "00-10-A4-23-19-C0".

5.2.3.31 TWAN-S2a-Failure-Cause

The TWAN-S2a-Failure-Cause AVP (AVP Code 1533) is of type Unsigned32 and it shall contain a 32 bit cause value field which is used to indicate the cause of S2a connectivity establishment failure to the 3GPP AAA Server by the TWAN. The description of the TWAN-S2a-Failure-Cause value is specified as in Table 5.2.3.30/1:

Table 5.2.3.30/1: TWAN-S2a-Failure-Cause value description

Cause value (decimal)	Cause Value	Meaning
26	Insufficient resources	This cause is used to indicate that the requested service cannot be provided due to insufficient resources.
27	Unknown APN	This cause is used to indicate that the requested service was rejected because the access point name could not be resolved.
29	User authentication failed	This cause is used to indicate that the requested service was rejected by the external packet data network due to a failed user authentication
30	Request rejected by TWAN or PDN GW	This cause is used to indicate that the requested service or operation was rejected by the TWAN or PDN GW.
31	Request rejected, unspecified	This cause is used to indicate that the requested service or operation was rejected due to unspecified reasons.
32	Service option not supported	This cause is used to indicate that the UE requests a service which is not supported by the PLMN.
33	Requested service option not subscribed	This cause is used to indicate that the UE requests a service option which it has no subscription.
34	Service option temporarily out of order	This cause is used to indicate that the network cannot serve the request because of temporary outage of one or more functions required for supporting the service.
38	Network failure	This cause is used to indicate that the requested service was rejected due to an error situation in the network.
50	PDN type IPv4 only allowed	This value is used to indicate that only PDN type IPv4 is allowed for the requested PDN connectivity.
51	PDN type IPv6 only allowed	This value is used to indicate that only PDN type IPv6 is allowed for the requested PDN connectivity.
54	PDN connection does not exist	This value is used at handover from a 3GPP access network to indicate that the network does not have any information about the requested PDN connection.
113	Multiple accesses to a PDN connection not allowed	This value is used to indicate that the request for the additional access to a PDN connection was rejected by the PDN GW.

5.2.3.32 SM-Back-Off-Timer

The SM-Back-Off-Timer AVP is of type Unsigned32 and it shall contain the session management back-off timer value in seconds. The session management back-off timer is provided to the UE as specified in clause 8.1.4.16 of 3GPP TS 24.302 [26].

5.2.3.33 WLCP-Key

The WLCP-Key AVP (AVP Code 1535) is of type OctetString and it shall contain the WLCP Key used for protecting the WLCP signalling between the UE and the TWAN, as specified in 3GPP TS 33.402 [19].

5.2.3.34 Void

5.2.3.35 IMEI-Check-In-VPLMN-Result

The IMEI-Check-In-VPLMN-Result AVP (AVP Code 1540) is of type Unsigned32 and it shall contain a 32 bit cause value field which is used to indicate the result of the IMEI check performed in the VPLMN. The description of the IMEI-Check-In-VPLMN-Result value is specified as in Table 5.2.3.35/1:

Table 5.2.3.35/1: IMEI-Check-In-VPLMN-Result value description

Cause value (decimal)	Cause Value	Meaning
0	Successful	This cause is used to indicate that the IMEI check has been performed successfully in the VPLMN.
1	Illegal_ME	This cause is used to indicate that the IMEI check has failed in the VPLMN due to an illegal Mobile Equipment.

5.2.4 Session Handling

The Diameter protocol between the non-3GPP access network and the 3GPP AAA Server or 3GPP AAA Proxy, shall always keep the session state, and use the same Session-Id parameter for the lifetime of each Diameter session.

A Diameter session shall identify a given user. In order to indicate that the session state is to be maintained, the Diameter client and server shall not include the Auth-Session-State AVP, either in the request or in the response messages (see IETF RFC 6733 [58]).

6 SWd and SWd' Description

6.1 Functionality

6.1.1 General

The SWd reference point connects the 3GPP AAA Proxy and the 3GPP AAA Server in EPS. The functionality of the SWd reference point is to transport authentication, authorization and related information in AAA messages including:

- Carrying data for authentication signalling between 3GPP AAA Proxy and 3GPP AAA Server;
- Carrying data for authorization signalling between 3GPP AAA Proxy and 3GPP AAA Server
- Carrying charging signalling per user;
- Carrying keying data for the purpose of radio interface integrity protection and encryption;
- Carrying authentication data for the purpose of tunnel establishment, tunnel data authentication and encryption, for the case in which the ePDG is in the VPLMN;
- Carrying mapping of a user identifier and a tunnel identifier sent from the ePDG to the 3GPP AAA Proxy through the 3GPP AAA Server;
- Used for purging a user from the access network for immediate service termination;
- Enabling the identification of the operator networks amongst which the roaming occurs;
- If QoS mechanisms are applied: carrying data for AN QoS capabilities/policies (e.g. the supported 3GPP QoS profiles) within authentication request from 3GPP AAA Proxy to 3GPP AAA Server.
- Carrying the IP Mobility Capabilities between 3GPP AAA Proxy and 3GPP AAA Server.

The SWd' reference point is defined between the 3GPP AAA Proxy, possibly via an intermediate 3GPP AAA Proxy, and the NSWOF in 5GS. The definition of the reference point and its functionality is given in clause 4.2.15 of 3GPP TS 23.501 [59] and Annex S of 3GPP TS 33.501 [60]. It reuses the same stage 3 protocol definition as defined for SWd in EPC, with specific requirements for NSWO in 5GS specified in clause 6.1.2.4.

6.1.2 Procedures Description

6.1.2.1 Trusted non-3GPP Access / Access Gateway related procedures

6.1.2.1.1 Trusted Non-3GPP Access Authentication and Authorization

When used in connection with the STa interface, the SWd interface shall support the trusted non-3GPP access authentication and authorization procedure defined in clause 5.1.2.1. For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the trusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication and authorization request, if roaming is not allowed for the users of the given HPLMN.
- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall check the presence and value of the visited network identifier. If the AVP was missing, it shall insert it, if the AVP was present, it may overwrite the AVP value before forwarding the request.
- The 3GPP AAA Proxy may modify the service authorization information in the authentication and authorization answer that it forwards to the trusted non-3GPP access network, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.
- The 3GPP AAA Proxy may decide about the trustworthiness of the non-3GPP access from the VPLMN point of view and insert a trust relationship indicator to the authentication and authorization request.
- If it supports the ER server functionality, the 3GPP AAA Proxy may decide about the use of ERP for re-authentication and indicate its willingness to act as the ER server for this session into the first authentication and authorization request forwarded to the 3GPP AAA server.

The 3GPP AAA Proxy shall decide about using the S2a-PMIP based S8 chaining and in case it has selected that option, it shall select the Serving GW to be invoked and it shall add the Serving GW address to the authentication and authorization answer that is sent upon successful completion of the authentication.

Table 6.1.2.1.1/1 describes the trusted non-3GPP access authentication and authorization request forwarded on the SWd interface.

Table 6.1.2.1.1-1: Trusted non-3GPP Access Authentication and Authorization Request on SWd

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP payload	EAP-payload	M	This IE shall contain the Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
UE Layer-2 address	Calling-Station-ID	M	This IE shall contain the Layer-2 address of the UE.
Supported 3GPP QoS profile	QoS-Capability	O	If the trusted non-3GPP Access supports QoS mechanisms, this information element may be included to contain the access network's QoS capabilities as defined in IETF RFC 5777 [9].
Mobility Capabilities	MIP6-Feature-Vector	C	This information element shall contain the mobility capabilities of the trusted non-3GPP access network, if dynamic mobility mode selection is done. This information may also be used to decide whether to authorize access to EPC to a user accessing a TWAN. The PMIP6_SUPPORTED flag and/or the GTPv2_SUPPORTED flag shall be set if the trusted non-3GPP access network supports PMIPv6 and/or GTPv2. PMIP6_SUPPORTED flag is defined in IETF RFC 5779 [2]. The flag MIP6_INTEGRATED shall be set if DHCPv6 based Home Agent address discovery is supported as defined in IETF RFC 5447 [6]. The MIP4_SUPPORTED flag shall be set if the trusted non-3GPP access supports MIPv4 FA-CoA mode.
Access Type	RAT-Type	M	This IE shall contain the trusted non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	M	This IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values)
Visited Network Identifier	Visited-Network-Identifier	M	This IE shall contain the Identifier that allows the home network to identify the Visited Network.
Full Name for Network	Full-Network-Name	O	This IE shall contain the full name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
Short Name for Network	Short-Network-Name	O	This IE shall contain the short name for network as specified in 3GPP TS 24.302 [26]. This AVP may be inserted by the non-3GPP access network depending on its local policy and only when it is not connected to the UE's Home Network. If the Visited Network Identifier is present, this AVP shall be set.
APN Id	Service-Selection	O	If present, this information element shall contain the Network Identifier part of the APN the user wants to connect to (if available).
Terminal Information	Terminal-Information	O	If present, this information element shall contain information about the user's mobile equipment. The type of identity carried depends on the access technology type. For HRPD access network, the 3GPP2-MEID AVP shall be included in this grouped AVP.
Trust Relationship Indicator	AN-Trusted	O	If present, This AVP shall express the trusted/untrusted decision about the non-3GPP IP access, from the VPLMN's point of view. The value "TRUSTED" shall be used in this case.
Selected Trusted WLAN Identifier	WLAN-Identifier	O	If present, this IE shall contain the Trusted WLAN Identifier selected by the UE to access the Trusted WLAN Access Network (see clause 16 of 3GPP TS 23.402 [3]).
DER Flags	DER-Flags	O	This Information Element contains a bit mask. See 5.2.3.20 for the meaning of the bits.

Transport Access Type	Transport-Access-Type	C	For interworking with Fixed Broadband access networks (see 3GPP TS 23.139 [39]), if the access network needs to receive the IMSI of the UE in the authentication response, then this information element shall be present, and it shall contain the value "BBF" (see clause 5.2.3.19).
Supported TWAN Connection Modes	TWAN-Connection-Mode	O	The TWAN should include this IE. If present, this information element shall contain the TWAN connection modes supported by the TWAN, i.e.TSCM, SCM and/or MCM.
Provided Connectivity Parameters	TWAN-Connectivity-Parameters	C	This information element shall be present if the 3GPP AAA Server has previously authorized the SCM to be used for EPC access. TWAN-Connectivity-Parameters is a grouped AVP. If the requested connectivity has been granted, the following information elements shall be included: - selected APN - selected PDN type - UE IPv4 Address (for PDN type IPv4 or IPv4v6) - UE IPv6 Interface Identifier (for PDN type IPv6 or IPv4v6) - Protocol Configuration Options (if received from the PGW) - TWAG user plane MAC address The absence of both an IPv4 address and an IPv6 Interface Identifier indicates that the requested connectivity could not be granted. If the requested connectivity has not been granted, the following information elements may be included: - a cause indicating why the requested connectivity has not been granted
TWAG Control Plane IP Address	TWAG-CP-Address	C	The TWAN shall include this IE if it indicates support of the MCM in the Supported TWAN Connection Modes IE. When present, this IE shall contain the TWAG Control Plane IPv4 Address, or the TWAG Control Plane IPv6 link local address, or both (if the TWAG supports IPv4 and IPv6), to be used for WLCP by the UE if the MCM is used.
Domain-Specific Re-authentication Key Request	ERP-RK-Request	O	If present, this IE indicates the willingness of an ER server in the non-3GPP access network or the 3GPP AAA proxy to act as the ER server for this session. When present, this IE shall contain the name of the realm in which the ER server is located.

NOTE: For more details on the 3GPP AAA Proxy behaviour, refer to clause 5.1.2.1.3.

6.1.2.1.2 HSS/AAA Initiated Detach for Trusted non-3GPP Access

When used in connection with the STa interface, the SWd interface shall support the HSS initiated detach procedure defined in clause 5.1.2.2.

For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the access network GW as a stateful Diameter proxy.

6.1.2.1.3 Access and Service Authorization information update

When used in connection with the STa interface, the SWd interface shall support the trusted non-3GPP access and service authorization information update procedure defined in clause 5.1.2.3. For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the trusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall check the presence and value of the visited network identifier. If the AVP was missing, it shall insert it, if the AVP was present, it may overwrite the AVP value before forwarding the request.

- The 3GPP AAA Proxy may modify the service authorization information in the authentication and authorization answer that it forwards to the trusted non-3GPP access network, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.

Table 6.1.2.1.3/1 describes the trusted non-3GPP access authorization request forwarded on the SWd interface. As the content is very similar to that of the request received on the STa interface, only those AVPs are listed that are handled differently on the two interfaces.

Table 6.1.2.1.3/1: Trusted Non-3GPP Access Authorization Request on SWd interface

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request-Type	Auth-Req-Type	M	This IE shall contain the Authorization Request Type. The following values only shall be used: AUTHORIZE_ONLY This value shall indicate the initial request for authorization of the user to the APN.
Visited Network Identifier	Visited-Network-Identifier	M	This IE shall contain an identifier that allows the home network to identify the Visited Network.
Routing Information	Destination-Host	M	This IE shall contain the 3GPP AAA Server name that is obtained from the Origin-Host AVP of a previously received message.
Supported 3GPP QoS profile	QoS-Capability	O	If the trusted non-3GPP Access supports QoS mechanisms, this information element may be included to contain the access network's QoS capabilities as defined in IETF RFC 5777 [9].
Access Type	RAT-Type	O	If present, this IE contain the trusted non-3GPP access network access technology type that is serving the UE.

NOTE: For more details on the 3GPP AAA Proxy behaviour, refer to clause 5.1.2.3.3.

6.1.2.1.4 Trusted non-3GPP Access Network Initiated Session Termination

When used in connection with the STa reference point, the SWd reference point shall support the access network initiated session termination procedures as defined in clause 5.1.2.4

For this procedure, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the access network gateway as a stateful Diameter proxy.

6.1.2.2 Untrusted non-3GPP Access / ePDG related procedures

When used in connection with the SWm reference point, the SWd reference point shall support the following procedures:

- Authentication procedures as defined in clause 7.1.2.1
- Authorization procedures as defined in clause 7.1.2.2
- Access network/ePDG initiated session termination procedures as defined in clause 7.1.2.3
- HSS/AAA initiated detach procedures as defined in clause 7.1.2.4
- Service authorization information update procedures as defined in clause 7.1.2.5

For all these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the ePDG as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication or an authorization request, if roaming is not allowed for the users of the given HPLMN.

- The 3GPP AAA Proxy may modify the service authorization information in the authorization answer that it forwards to the ePDG, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.
- The 3GPP AAA Proxy shall decide about using the S8-S2b chaining and in case it has selected that option, it shall select the Serving GW to be invoked and it shall add the Serving GW address to the authentication answer that is sent upon successful completion of the authentication.

NOTE: For more detailed behavior of the 3GPP AAA Proxy, refer to clauses 7.1.2.1.3 and 7.1.2.2.3 respectively.

When used in connection with the SWa interface point, the SWd reference point shall support the following procedures:

- Authentication and authorization procedure as defined in clause 4.1.2.1
- HSS/AAA initiated detach procedures as defined in clause 4.1.2.2
- Untrusted non-3GPP access network initiated detach procedures as defined in clause 4.1.2.3
- Re-Authentication and Re-Authorization Procedure as defined in clause 4.1.2.4

For all these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the untrusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication and authorization request, if roaming is not allowed for the users of the given HPLMN.
- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall insert the visited network identifier.

6.1.2.3 PDN GW related procedures

When used in connection with the S6b reference point, the SWd reference point shall support the following procedures:

- Authentication and authorization procedures when using DSMIP as defined in clause 9.1.2.1
- Authorization procedures when using NBM as defined in clause 9.1.2.2
- PDN GW initiated session termination procedures as defined in clause 9.1.2.3
- HSS/AAA initiated detach procedures as defined in clause 9.1.2.4
- Service authorization information update procedures as defined in clause 9.1.2.5

For all these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the 3GPP AAA Server and the PDN GW as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication or authorization request, if roaming is not allowed for the users of the given HPLMN
- The 3GPP AAA Proxy may modify the service authorization information in the authorization answers that it forwards to the PDN GW, in order to enforce the QoS limitations according to the local policies and the roaming agreement with the home operator.

NOTE: For more detailed behavior of the 3GPP AAA Proxy, refer to clauses 9.1.2.1.4, 9.1.2.2.4, 9.1.2.3.4, and 9.1.2.4.4, respectively.

6.1.2.4 SWd' procedures for NSWO in 5GS

The SWd' interface between the 3GPP AAA Proxy, possibly via an intermediate 3GPP AAA Proxy, and the NSWOF shall support the same procedures as defined for SWa' in clause 4.1.2.5.

For these procedures, the 3GPP AAA Proxy shall forward the Diameter commands received from the NSWOF and the untrusted non-3GPP access network as a stateful Diameter proxy, with the following exceptions:

- The 3GPP AAA Proxy may reject an authentication and authorization request, if roaming is not allowed for the users of the given HPLMN.

- When forwarding an authentication and authorization request, the 3GPP AAA Proxy shall insert the visited network identifier.

6.2 Protocol Specification

6.2.1 General

The SWd reference point shall be based on Diameter, as defined in IETF RFC 6733 [58] and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 4072 [5], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [8]) frames over Diameter.
- IETF RFC 5779 [2], which defines Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5447 [6], which defines Diameter extensions for Mobile IPv6 NAS to AAA interface.

There is no separate application ID defined for the SWd interface. The application ID used by the 3GPP AAA Proxy depends on the command sent over SWd.

NOTE: Even though the 3GPP AAA Proxy may add new AVPs to the Diameter commands forwarded to/from the 3GPP AAA Server, there is no AVP present in the SWd reference point that would not be present in the interface that is used in connection with it. Therefore, the same Application ID can be used.

6.2.2 Commands

6.2.2.1 Commands used in connection with the STa interface

6.2.2.1.1 Commands for STa PMIPv6 or GTPv2 authentication and authorization procedures

6.2.2.1.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a trusted non-3GPP access network NAS to a 3GPP AAA server. The ABNF is re-used from the IETF RFC 5779 [2].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777250 >
                             < Session-Id >
                             [ DRMP ]
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             [ Destination-Host ]
                             { Auth-Request-Type }
                             { EAP-Payload }
                             [ User-Name ]
                             [ Calling-Station-Id ]
                             …
                             [ RAT-Type ]
                             [ ANID ]
                             [ QoS-Capability ]
                             [ MIP6-Feature-Vector ]
```

[Visited-Network-Identifier]
[Service-Selection]
[Terminal-Information]
[AN-Trusted]
[Full-Network-Name]
[Short-Network-Name]
*[Supported-Features]
[WLAN-Identifier]
[DER-Flags]
[TWAN-Connection-Mode]
[TWAN-Connectivity-Parameters]
* 2 [TWAG-CP-Address]
[TWAN-S2a-Failure-Cause]
[ERP-RK-Request]
…
*[AVP]

6.2.2.1.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a 3GPP AAA Proxy. The ABNF is re-used from the IETF RFC 5779 [2]. The ABNF also contains AVPs that are reused from IETF RFC 4072 [5].

< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >
< Session-Id >
[DRMP]
{ Auth-Application-Id }
{ Result-Code }
[Experimental-Result]
{ Origin-Host }
{ Origin-Realm }
{ Auth-Request-Type }
[EAP-Payload]
[User-Name]
[Session-Timeout]
[Accounting-Interim-Interval]
[EAP-Master-Session-Key]
[Context-Identifier]
[APN-OI-Replacement]
***[APN-Configuration]**
[MIP6-Feature-Vector]
[Mobile-Node-Identifier]
*[Redirect-Host]]
[Trace-Info]
[Subscription-ID]
*[Supported-Features]
[DEA-Flags]
[TWAN-Connection-Mode]
[TWAN-Connectivity-Parameters]
[Terminal-Information]
[Key]
[ERP-Realm]
…
*[AVP]

6.2.2.1.2 Commands for STa HSS/AAA Initiated Detach for Trusted non-3GPP Access

The ABNFs defined for the STa interface in clause 5.2.2.2 and in its clauses apply.

6.2.2.1.3 Commands for STa Access and Service Authorization Update Procedure

The ABNFs defined for the STa interface in clause 5.2.2.3 and in its clauses apply.

6.2.2.1.4 Commands for Trusted non-3GPP Access network Initiated Session Termination

The ABNFs defined for the STa interface in clause 5.2.2.4 and in its clauses apply.

6.2.2.2 Commands used in connection with the SWm interface

The ABNFs defined for the SWm interface in clause 7.2.2 and in its clauses apply.

6.2.2.3 Commands used in connection with the S6b interface

The ABNFs defined for the S6b interface in clause 9.2.2 and in its clauses apply.

6.2.3 Information Elements

6.2.3.1 General

The following table describes the Diameter AVPs defined for the SWd interface protocol in NBM mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

Table 6.2.3.1/1: Diameter SWd AVPs

	AVP Flag rules

Attribute Name	AVP Code	Clause defined	Value Type	Must	May	Should not	Must not
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V,P
QoS-Capability	578	5.2.3.4	Grouped	M			V,P
RAT-Type	1032	5.2.3.6	Enumerated	M,V			P
ANID	1504	5.2.3.7	UTF8String	M,V			P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
Mobile-Node-Identifier	506	5.2.3.2	UTF8String	M			V,P
AN-Trusted	1503	5.2.3.9	Enumerated	M,V			P
Full-Network-Name	1516	5.2.3.14	OctetString	V			M,P
Short-Network-Name	1517	5.2.3.15	OctetString	V			M,P
WLAN-Identifier	1509	5.2.3.18	Grouped	V			M,P
APN-Configuration	1430	8.2.3.7	Grouped	M,V			P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
DER-Flags	1520	5.2.3.20	Unsigned32	V			M,P
DEA-Flags	1521	5.2.3.21	Unsigned32	V			M,P
SSID	1524	5.2.3.22	UTF8String	V			M,P
HESSID	1525	5.2.3.23	UTF8String	V			M,P
TWAN-Connection-Mode	1527	5.2.3.25	Unsigned32	V			M,P
TWAN-Connectivity-Parameters	1528	5.2.3.26	Grouped	V			M,P
Connectivity-Flags	1529	5.2.3.27	Unsigned32	V			M,P
TWAN-PCO	1530	5.2.3.28	OctetString	V			M,P
TWAG-CP-Address	1531	5.2.3.29	Address	V			M,P
TWAG-UP-Address	1532	5.2.3.30	UTF8String	V			M,P
TWAN-S2a-Failure-Cause	1533	5.2.3.31	Unsigned32	V			M,P

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 [58].

NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.

The following table describes the Diameter AVPs re-used by the SWd interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within SWd. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol defined in IETF RFC 6733 [58], do not need to be supported.

Table 6.2.3.1/2: SWd re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
Accounting-Interim-Interval	IETF RFC 6733 [58]		
Auth-Request-Type	IETF RFC 6733 [58]		
Calling-Station-Id	IETF RFC 4005 [6]		
Subscription-ID	IETF RFC 4006 [20]		Must not set
EAP-Master-Session-Key	IETF RFC 4072 [5]		
EAP-Payload	IETF RFC 4072 [5]		
RAT-Type	3GPP TS 29.212 [23]		
Re-Auth-Request-Type	IETF RFC 6733 [58]		
Session-Timeout	IETF RFC 6733 [58]		
User-Name	IETF RFC 6733 [58]		
Terminal-Information	3GPP TS 29.272 [29]		
APN-OI-Replacement	3GPP TS 29.272 [29]		
Supported-Features	3GPP TS 29.229 [24]	See NOTE 1.	
Feature-List-ID	3GPP TS 29.229 [24]	See NOTE 1.	
Feature-List	3GPP TS 29.229 [24]	See NOTE 1.	
PDN-Type	3GPP TS 29.272 [29]		
Served-Party-IP-Address	3GPP TS 32.299 [30]		
DRMP	IETF RFC 7944 [53]	See clause 8.2.3.25	Must not set
ERP-RK-Request	IETF RFC 6942 [57]		Must not set
ERP-Realm	IETF RFC 6942 [57]		Must not set
Key	IETF RFC 6734 [56]	This is a grouped AVP containing Key-Type, Keying-Material and, optionally, Key-Lifetime.	Must not set
NOTE 1: There is no separate Diameter application ID defined for the SWd interface so a separate supported feature list is not required. The supported features depend on the command being proxied over SWd.			
NOTE 2: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.			
NOTE 3: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.			

Only those AVP initially defined in this reference point and for this procedure are described in the following clauses.

7 SWm Description

7.1 Functionality

7.1.1 General

The SWm reference point is defined between the ePDG and the 3GPP AAA Server or between the ePDG and the 3GPP AAA Proxy. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

The SWm reference point shall be used to authenticate and authorize the UE.

The SWm reference point is also used to transport NBM related mobility parameters in a case the UE attaches to the EPC via the S2b (based on PMIPv6 or GTPv2) and SWn reference points (i.e. IP Mobility Mode Selection information).

Additionally the SWm reference point may also be used to transport DSMIPv6 related mobility parameters in case the UE attaches to the EPC using the S2c reference point. In particular, in this case the SWm reference point may be used

for conveying the Home Agent IP address or FQDN from the AAA server to the ePDG for Home Agent discovery based on IKEv2 (see TS 24.303 [13]).

7.1.2 Procedures Description

7.1.2.1 Authentication and Authorization Procedures

7.1.2.1.1 General

The authentication and authorization procedure shall be used between the ePDG and 3GPP AAA Server/Proxy. When a PDN connection is activated by the UE an IKEv2 exchange shall be initiated. It shall be invoked by the ePDG, on receipt from the UE of a "tunnel establishment request" message. This shall take the form of forwarding an IKEv2 exchange with the purpose of authenticating in order to set up an IKE Security Association (SA) between the UE and the ePDG.

During the Access Authentication and Authorization procedure the ePDG may provide information on its PMIPv6 or GTPv2 capabilities to the 3GPP AAA Server. The 3GPP AAA Server may perform IP mobility mode selection between NBM or HBM as specified in clause 4.1.3.2 of 3GPP TS 23.402 [3]. The 3GPP AAA Server may provide to the ePDG an indication if either NBM or local IP address assignment shall be used. If NBM shall be used, the ePDG then decides the S2b protocol variant to use.

The User-Name AVP may contain a decorated NAI (as defined in clause 19.3.3 of 3GPP TS 23.003 [14]). In this case the 3GPP AAA Proxy shall process the decorated NAI and support routing of the Diameter request messages based on the decorated NAI as described in IETF RFC 5729 [37].

Upon a successful authorization, when NBM is used, the 3GPP AAA server shall return NBM related information back to the ePDG. This information may include the assigned PDN GW, UE IPv6 HNP and/or UE IPv4-HoA.

Upon a successful authorization, when DSMIPv6 is used, to enable HA address discovery based on IKEv2 (see TS 24.303 [13]), the 3GPP AAA server may also download PDN GW identity to the ePDG.

The PDN GW identity is a FQDN and/or IP address of the PDN GW. If a FQDN is provided, the ePDG shall derive it to IP address according to the selected mobility management protocol.

If DSMIPv6 is used, a single IKE SA is used for all PDN connections of the user. If PMIPv6 or GTPv2 is used, a separate IKE SA is created for each PDN connection of the user (refer to 3GPP TS 24.302 [26]).

Each new additional IKE SA shall be handled in a different Diameter session. In such cases, the IP mobility mode selected during the first authentication and authorization procedure is valid for all PDN connections of the user, therefore, dynamic IP mobility mode selection is not executed during the further procedures. The ePDG may select the same or different S2b protocol variant(s) towards different PDN GWs when NBM has been selected.

Based on local policies, EPC access for emergency services over an untrusted WLAN access is supported as specified in clause 4.5.7.2.1 of 3GPP TS 23.402 [3] for:

- UEs with a valid EPC subscription that are authenticated and authorized for EPC services;
- UEs that are authenticated only;
- UEs with an unauthenticated IMSI; and/or
- UICC-less UEs.

The SWm reference point shall perform authentication and authorization based on the reuse of the DER/DEA command set defined in Diameter EAP application, IETF RFC 4072 [5].

Table 7.1.2.1.1/1: Authentication and Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State.
EAP payload	EAP-Payload	M	This information element shall contain the encapsulated EAP payload used for the UE - 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This information element shall indicate whether the user is to be authenticated only, authorized only or both. It shall have the value of AUTHORIZE_AUTHENTICATE.
APN	Service-Selection	C	This information element shall contain the Network Identifier part of the APN for which the UE is requesting authorization. This AVP shall be present if the ePDG has received an APN from the UE and the UE did not indicate the establishment of an emergency session in the IKEv2 signalling. This AVP shall be absent if the UE indicated the establishment of an emergency session during the IKEv2 tunnel establishment (see clause 7.2.5 of 3GPP TS 24.302 [26]).
Visited Network Identifier (See 9.2.3.1.2)	Visited-Network-Identifier	C	This information element shall contain the identifier that allows the home network to identify the Visited Network. This AVP shall be present if the ePDG is not in the UE's home network i.e. the UE is roaming.
Access Type	RAT-Type	C	This information element shall be present if the access type is known by the ePDG. If present, it shall contain the non-3GPP access network access technology type that is serving the UE. When not known by the ePDG, this information element should be present and, in that case, it shall take the value VIRTUAL (1).
Mobility features	MIP6-Feature-Vector	O	This AVP shall be present, if the handling of any of the flags listed here requires dynamic (i.e. per user) handling for the VPLMN-HPLMN relation of the ePDG and 3GPP AAA Server. If present, the AVP shall contain the mobility features supported by the ePDG. Flags that are not relevant in the actual relation shall be set to zero. If dynamic IP mobility mode selection is used, the PMIP6_SUPPORTED flag and/or the GTPv2_SUPPORTED flag shall be set by the ePDG if PMIPv6 and/or GTPv2 are supported. PMIP6_SUPPORTED flag is defined in IETF RFC 5779 [2]. The MIP6_INTEGRATED flag shall be used to indicate to the 3GPP AAA server that the ePDG supports IKEv2 based Home Agent address discovery.
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the ePDG has determined that a previously assigned 3GPP AAA Server is unavailable.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
UE local IP address	UE-Local-IP-Address	O	The ePDG shall include this IE based on local policy for Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39]. The ePDG may also include this IE, regardless of Fixed Broadband access network interworking. If present, it shall contain the source IPv4 or IPv6 address of the IKE_SA_AUTH message from the UE.
Terminal Information	Terminal-Information	C	The ePDG shall include this IE and set it to the user's Mobile Equipment Identity, if this information is available. For an untrusted WLAN access, this grouped AVP shall contain the IMEI AVP and, if available, the Software-Version AVP. When the RAT type is not known by the ePDG, but the UE has provided the IMEI(SV), this grouped AVP shall contain the IMEI AVP and, if available, the Software-Version AVP.
Emergency Services	Emergency-Services	C	An ePDG which supports emergency services shall include this information element, with the Emergency-Indication bit set, if the UE indicated the establishment of an emergency session during the IKEv2 tunnel establishment (see clause 7.2.5 of 3GPP TS 24.302 [26]).

Table 7.1.2.1.1/2: Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	O	This information element, if present, shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes, if it contains a NAI other than an Emergency NAI for Limited Service State.
EAP payload	EAP-Payload	O	If present, this information element shall contain the encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication
Master-Session-Key	EAP-Master-Session-Key	C	This IE shall contain keying material for protecting the communication between the user and the ePDG. It shall be present when Result Code is set to DIAMETER_SUCCESS.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result code	Result-Code / Experimental-Result-Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]) or as per in NASREQ (see IETF RFC 4005 [4].
3GPP AAA Server URI	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Mobility Capabilities	MIP6-Feature-Vector	O	This AVP shall be present if it was received in the authentication and authorization request and the authentication and authorization succeeded. It shall contain the authorized mobility features. Flags that are not relevant in the actual relation shall be set to zero. The PMIP6_SUPPORTED flag and/or the GTPv2_SUPPORTED flag shall be set to indicate that NBM (PMIPv6 or GTPv2) is to be used. The ASSIGN_LOCAL_IP flag shall be set to indicate that a local IP address is to be assigned. The MIP6_INTEGRATED flag shall be set if a Home Agent address is provided for IKEv2 based Home Agent address discovery. In the latter case HA information for IKEv2 discovery is provided via the APN-Configuration AVP.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is used, the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Request and the Result-Code AVP is set to DIAMETER_SUCCESS.

APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS and the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Request. The APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is used, the following information elements per APN may be included: - APN - APN-AMBR - Authorized 3GPP QoS Profile - User home IP Address (if static IPv4 and/or IPv6 is allocated to the UE's subscribed APN) - Allowed PDN types - PDN GW identity (if the PDN connection was active in case of HO, or if there is a static PDN GW allocated to the UE's subscribed APN) - PDN GW allocation type - VPLMN Dynamic Address Allowed - Visited Network Identifier - Interworking-5GS-Indicator When local IP address assignment is used, this AVP shall only be present if IKEv2 based Home Agent discovery is used and - if the PDN connection was active in case of HO, or - if there is static PDN GW allocated to the UE's subscribed APN, or - if the 3GPP AAA Server/Proxy selects the PDN GW based on the identity of the ePDG In these cases, the following information elements shall be included: - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14]) - PDN GW identity NOTE 1.
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the ePDG. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent only if it is available.
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
Permanent User Identity	Mobile-Node-Identifier	C	This information element shall be present if NBM is used. If the user is authenticated, it shall contain an AAA/HSS assigned permanent user identity (i.e. IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]) to be used by: - the MAG in subsequent PBUs as the MN-ID identifying the user in the EPS network for PMIP based S2b, - by the ePDG to derive the IMSI to send in subsequent Create Session Request for GTP based S2b. For an emergency PDN connection, if the UE is UICC-less (i.e. the User Identity IE in the request contains an IMEI) or if the IMSI is not authenticated, the Permanent User Identity shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.

Serving GW Address	MIP6-Agent-Info	O	This AVP shall be used only in chained S2b-S8 cases and it shall be sent only if the Result-Code AVP is set to DIAMETER_SUCCESS.
UE Charging Data	3GPP-Charging-Characteristics	O	This information element contains the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
WLAN Location Information	Access-Network-Info	O	If present, this IE shall contain the location information of the WLAN Access Network where the UE is attached.
WLAN Location Timestamp	User-Location-Info-Time	C	This IE should be present if the WLAN Location Information IE is present. When present, this IE shall contain the NTP time at which the UE was last known to be in the location reported in the WLAN Location Information.
Emergency Info	Emergency-Info	C	This IE shall only be present if the Result-Code AVP is set to DIAMETER_SUCCESS. When present, it shall contain the identity of the dynamically allocated PDN-GW used for the establishment of emergency PDN connections. It shall be present for a non-roaming authenticated user, if this information was received from the HSS and if the Emergency-Services AVP is present, with the Emergency-Indication bit set, in the Authentication and Authorization Request.
UE Usage Type	UE-Usage-Type	C	This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the UE Usage Type of the subscriber.
Core Network Restrictions	Core-Network-Restrictions	C	This IE shall be present if this information is available in the user subscription. When present, this IE shall contain the Core Network Restrictions of the subscriber.
NOTE 1: If a static PDN GW allocated to the UE's subscribed APN has been received from the HSS, the 3GPP AAA Server/Proxy shall only provide the static PDN GW identity in the Authentication and Authorization Answer.			

7.1.2.1.2 3GPP AAA Server Detailed Behaviour

On receipt of the DER message, the 3GPP AAA Server shall check that the user data exists in the 3GPP AAA Server. If not, the 3GPP AAA Server shall use the procedures defined for the SWx interface to obtain access authentication and authorization data.

If the HSS returns DIAMETER_ERROR_USER_UNKWNOWN, the 3GPP AAA Server shall return the same error to the ePDG.

If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the ePDG with the Result-Code set to DIAMETER_REDIRECT_INDICATION and Redirect-Host set to the Diameter URI of the 3GPP AAA Server currently serving the user (this Diameter URI shall be constructed based on the Diameter Identity included in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

Otherwise, the 3GPP AAA Server shall proceed with the authentication and authorization procedure. The 3GPP AAA Server shall use the procedures defined in SWx interface to obtain authorization data from HSS.

If IMEI check is required by operator policy and the ePDG is in the HPLMN, the 3GPP AAA Server shall:

- if the IMEI(SV) is available, check the Mobile Equipment's identity status with the EIR, using the ME Identity Check procedure (see clause 11);
    - upon getting the IMEI check result from the EIR, determine whether to continue or stop the authentication and authorization procedure;
- if the IMEI(SV) is not available, determine whether to continue or stop the authentication and authorization procedure based on operator policy;
- if the 3GPP AAA Server determines that the authentication and authorization procedure shall be stopped, it shall respond to the ePDG with the Experimental-Result-Code DIAMETER_ERROR_ILLEGAL_EQUIPMENT.

Specific operator policies may be configured for emergency services, regarding whether to check the IMEI and, if the IMEI needs to be checked, whether to continue or stop the authentication and authorization procedure upon getting the IMEI check result or when the IMEI(SV) is not available.

If the 3GPP AAA Server receives a request message not related to any existing session and is able to recognize that the ePDG included the AAA-Failure-Indication AVP in the request, the 3GPP AAA Server shall also include the AAA-Failure-Indication AVP over the SWx interface, while retrieving the access authentication and authorization data from the HSS.

If the user does not have non-3GPP access subscription, then 3GPP AAA Server shall respond to the ePDG with Experimental-Result-Code DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION.

If a Visited- Network-Identifier is present in the request and if the user is not allowed to roam in the visited network, then the 3GPP AAA Server shall return Experimental-Result-Code set to DIAMETER_ERROR_ROAMING_NOT_ALLOWED.

If the user is not allowed to use the current access type, then the 3GPP AAA Server shall return Experimental-Result-Code set to DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED.

Otherwise the 3GPP AAA Server shall run EAP-AKA as specified in 3GPP TS 33.402 [19]. Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and, therefore, no authentication information shall be returned.

Upon receiving the authentication and authorization request from the ePDG, the 3GPP AAA Server marks the trust relationship as "untrusted" with the User Identity. If the 3GPP AAA Server detects that an S6b session already exists for this UE and the S6b session was established as a result of an authentication request for DSMIPv6, the 3GPP AAA Server shall send the trust relationship to the PDN GW as specified in clause 9.1.2.5.

Once authentication is successfully completed, the 3GPP AAA Server shall perform the following authorization checking (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

1) Check if the user is barred to use the non 3GPP Access. If it is so, then the Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED

2) Check whether the user is barred to use the subscribed APNs. If it is so, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

3) if the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Request, check if there was request for an APN received. If not, the default APN of the user is selected to be used during the actual authentication and authorization procedure.

4) if the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authentication and Authorization Request, check if user has a subscription for the requested APN or for the wildcard APN. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION

5) If present, check the flags of the received MIP6-Feature-Vector AVP: The evaluation of the flags is executed only in the first authentication and authorization procedure for the user after an initial attach or handover, in all the subsequent procedures, the AAA Server shall insert the same values.

   - If the MIP6-INTEGRATED flag is set and the 3GPP AAA server has authorized IKEv2 Home Agent assignment, the 3GPP AAA server shall include the Home Agent addresses in the APN-Configuration AVP in the response and the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag set. In this case, the 3GPP AAA Sever may select the Home Agent based on the identity of the ePDG as included in the Origin-Host AVP in the authentication and authorization request if no static PDN GW identity is received from the HSS. If the HA assignment via IKEv2 is not used, the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag not set shall be sent.

   - The PMIP6_SUPPORTED and/or GTPv2_SUPPORTED flag indicates to the 3GPP AAA server whether the ePDG supports NBM or not. As specified in 3GPP TS 23.402 [3], based on the information it has regarding the UE (see 3GPP TS 24.302 [26]), local/home network capabilities and local/home network policies, the 3GPP AAA server may perform mobility mode selection. If the 3GPP AAA server decides that NBM should be used, the PMIP6_SUPPORTED and GTPv2_SUPPORTED flags shall be set in the response to indicate the NBM support of the UE to the ePDG. If only the PMIP6_SUPPORTED or the GTPv2_SUPPORTED flag is present in the response, the ePDG shall assume that this also indicates the NBM support of the UE to the ePDG and the ePDG may select any S2b protocol variant (PMIPv6 or GTPv2). If the 3GPP AAA server decides that a local IP address should be assigned, the ASSIGN_LOCAL_IP flag shall be set in the response to indicate to the ePDG that a local IP address should be assigned.

NOTE 1: When selecting DSMIPv6, the AAA server assumes that the ePDG has the capability to assign a local IP address to the UE.

- The 3GPP AAA server shall not set the PMIP6_SUPPORTED/GTPv2_SUPPORTED and ASSIGN_LOCAL_IP flags both at the same time in the response.

Upon successful authentication and authorization, the Result-Code shall be set to DIAMETER_SUCCESS and:

- if the Emergency-Indication bit of the Emergency-Services AVP was not set in the Authentication and Authorization Request, the 3GPP AAA Server shall return user data relevant to the APN as received from the HSS. If the requested APN received from UE is authorized by the wildcard APN, the 3GPP AAA Server shall include the wildcard APN in the Service-Selection AVP of the APN-Configuration AVP;

- if the Emergency-Services AVP was present, with the Emergency-Indication bit set, in the Authentication and Authorization Request, the 3GPP AAA Server shall include the Emergency Info IE if this information was received from the HSS and the user is not roaming.

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and, therefore, no authorization information shall be returned.

For Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39], the 3GPP AAA server shall determine if the UE is connected via a BBF-defined WLAN access according to the UE local IP address in UE-Local-IP-Address AVP from the ePDG. If the UE is connected via a BBF-defined WLAN access, the 3GPP AAA server shall perform the enabling UE reflective QoS function as specified in 3GPP TS 24.139 [43].

The 3GPP AAA Server shall interpret the receipt of the Emergency-Services AVP, with the Emergency-Indication bit set, as an indication that the UE requests to access the EPC for emergency services.

The 3GPP AAA Server shall give preferential treatment to UEs which access the EPC for emergency services, e.g. in scenarios including network overload.

If the 3GPP AAA Server has WLAN Location Information about the UE, the 3GPP AAA Server shall provide it to the ePDG, along with the WLAN Location Timestamp if available (see clause 4.1.2.1.2).

If the 3GPP AAA Server supports IMS Emergency sessions over WLAN (see clause 4.5.7.2 of 3GPP TS 23.402 [3]), the 3GPP AAA Server shall proceed as specified above, but with the following modifications, for an Emergency Attach:

1) if the UE does not have an IMSI:

   - if local policies allow emergency sessions for all UEs, the 3GPP AAA Server shall skip the procedures defined for the SWx interface to obtain access authentication and authorization data, skip the authorization checkings and authorize the UE to access to EPC for emergency services. The Permanent User Identity IE in the answer shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14];

   - otherwise the 3GPP AAA Server shall reject the request with the Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN.

2) if the UE has an IMSI but the IMSI is not authenticated:

   - if local policies allow emergency sessions for unauthenticated UEs with an IMSI, the 3GPP AAA Server shall skip the procedures defined for the SWx interface to obtain access authorization data, shall skip the authorization checkings and shall return an answer with the DIAMETER_ERROR_USER_UNKWNOWN Result-Code to the ePDG to request the UE to provide its IMEI as specified in clause 13.3 of 3GPP TS 33.402 [19].

NOTE 2: According to the procedure specified in clause 7.4.4 of 3GPP TS 24.302 [26], this results in an ePDG, that is configured to support unauthenticated emergency session over WLAN and Mobile Equipment Identity signalling over untrusted WLAN, to query the UE's IMSI and to initiate a new Authentication and Authorization procedure with the same parameters as provided in the first Authentication and Authorization Request but with the addition of the UE's IMEI in the Terminal-Information AVP.

If the Authentication and Authorization Request also included the UE's IMEI (i.e. new authentication and authorization procedure after the ePDG queried the UE), the 3GPP AAA Server shall authorize the UE to

access to EPC for emergency services. The Permanent User Identity IE in the answer shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14];

- otherwise the 3GPP AAA Server shall reject the request with the Experimental-Result-Code set as specified for authentication failures in this clause.

3) if the UE has an authenticated IMSI but the UE is not authorized to access the EPC:

- if local policies allow emergency sessions for any authenticated UE, the 3GPP AAA Server shall authorize the UE to access to EPC for emergency services;

- otherwise the 3GPP AAA Server shall reject the request with the Experimental-Result-Code set as specified for authorization failures in this clause.

7.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy shall be required to handle roaming cases in which the ePDG is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy with the following additions.

If IMEI check is required by operator policy and the ePDG is in the VPLMN, the 3GPP AAA Proxy shall:

- if the IMEI(SV) is available, check the Mobile Equipment's identity status with the EIR, using the ME Identity Check procedure (see clause 11);

  - upon getting the IMEI check result from the EIR, determine whether to continue or stop the authentication and authorization procedure;

- if the IMEI(SV) is not available, determine whether to continue or stop the authentication and authorization procedure based on operator policy;

- if the 3GPP AAA Proxy determines that the authentication and authorization procedure shall be stopped, it shall:

  - respond to the ePDG with the Experimental-Result-Code DIAMETER_ERROR_ILLEGAL_EQUIPMENT, and

  - send a SWm Session Termination Request towards the 3GPP AAA Server (see clause 7.1.2.3).

Specific operator policies may be configured for emergency services, regarding whether to check the IMEI and, if the IMEI needs to be checked, whether to continue or stop the authentication and authorization procedure upon getting the IMEI check result or when the IMEI(SV) is not available.

On receipt of the first authentication and authorization request, the 3GPP AAA Proxy shall check locally configured information whether users from the HPLMN are allowed to activate a PDN connection from the non-3GPP access network via this (V)PLMN. If not, the Experimental-Result-Code shall be set to DIAMETER_ERROR_ROAMING_NOT_ALLOWED and the authentication response shall be sent to the ePDG.

On receipt of the authentication and authorization answer that completes a successful authentication, the 3GPP AAA Proxy

- may check locally configured information about using the chained S8-S2b option towards the given HPLMN. If chaining is required, the 3GPP AAA Proxy shall select a Serving GW from its network configuration database and shall include the Serving GW address in the response.

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.

- shall record the state of the connection (i.e. Authorization Successful).

- may select the Home Agent based on the identity of the ePDG as included in the Origin-Host AVP in the authentication and authorization request if IKEv2 based Home Agent discovery is used and VPLMN Dynamic Address Allowed AVP is received. In this case, the 3GPP AAA proxy shall include the Home Agent addresses in the APN-Configuration AVP in the response and the MIP6-Feature-Vector AVP with the MIP6-INTEGRATED flag set if no static PDN GW identity is received from the 3GPP AAA Server.

7.1.2.1.4 ePDG Detailed Behaviour

The ePDG shall initiate a new authentication and authorization procedure for each new IKE_SA. Each IKE_SA shall be handled in a different session.

The ePDG shall set flags signalling its capabilities to the same value in all authentication and authorization procedure for the same user (include the same MIP6-Feature-Vector). During the second and further authentication and authorization procedures, the ePDG shall discard the flag values received from the AAA Server and reuse the values received during the first procedure executed for the user.

An ePDG which supports emergency services shall include the Emergency-Services AVP, with the Emergency-Indication bit set, if the UE indicated the establishment of an emergency session during the IKEv2 tunnel establishment (see clause 7.2.5 of 3GPP TS 24.302 [26]).

For PMIPv6/GTPv2 based S2b, when receiving a Serving GW address in an authentication response, the ePDG shall check, whether it has already a Serving GW address stored for the user.

- If it has no Serving GW address available, it shall store the received value and use it as LMA address when creating PMIP bindings.
- If it has already a stored Serving GW address value, it shall ignore the received SGW-Address AVP.

NOTE 1: In case of untrusted access, there is an authentication session started for all PDN connection setup requests of a user. These sessions may invoke different 3GPP AAA Proxies, which in turn may assign different Serving GWs to the user. The ePDG behaviour ensures that in spite of this possibility, the same Serving GW is used for all PDN connections of the user.

NOTE 2: The ePDG knows if NBM is used or if a local IP address is assigned based on the flags in the MIP6-Feature-Vector or based on preconfigured information. If the PMIP6_SUPPORTED and/or the GTPv2_SUPPORTED flag are set in the MIP6-Feature-Vector received from the 3GPP AAA Server, the ePDG knows that NBM is used.

For PMIPv6/GTPv2 based S2b and a PDN connection other than for emergency services, the ePDG shall utilize the downloaded APN configuration data to authorize the UE requested home address types: IPv4 home address and/or IPv6 home network prefix.

For GTPv2 based S2b and a PDN connection for emergency services, the ePDG shall ignore APN configuration data received from the 3GPP AAA Server and shall use its Emergency Configuration Data to determine the APN to be associated with the emergency PDN connection and possibly the PGW to use (see clause 4.5.7.2 of 3GPP TS 23.402 [3]). During a handover of an emergency PDN connection to an untrusted WLAN access, the ePDG shall use the PGW identified in the Emergency Info IE if this information is received from the 3GPP AAA Server, the user is a non-roaming authenticated user and the ePDG is configured to use a dynamic PGW for emergency services for such users.

The ePDG may use the Visited_Network_Identifier to determine the S2b protocol type (PMIPv6 or GTPv2). The ePDG may be configured with the S2b protocol variant(s) on a per HPLMN granularity, or may retrieve information regarding the S2b protocol variants supported by the PDN GW (PMIPv6 or/and GTPv2) from the Domain Name Service Function as described in 3GPP TS 29.303[34]. If the ePDG supports Dedicated Core Networks and received the UE-Usage-Type from the 3GPP AAA Server, the ePDG shall select the PGW as specified in clause 5.8 of 3GPP TS 29.303 [34].

The ePDG shall select a combined PGW/SMF for PDN connections that may be subject to mobility to 5GS, e.g. for UEs supporting N1 mode (see 3GPP TS 24.302 [26]) and not restricted to interworking with 5GS by user subscription (see "5GC" bit within Core-Network-Restrictions AVP and Interworking-5GS-Indicator AVP specified) as specified in clause 5.12.3 of 3GPP TS 29.303 [34].

If GTPv2 is used on S2b and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the ePDG shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user.

If DSMIPv6 is used and if ePDG has received the PGW identity in form of the FQDN from the 3GPP AAA server, then the ePDG may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

If the ePDG determines that a previously assigned 3GPP AAA Sever is unavailable, it may attempt to send a new authentication and authorization request to an alternate 3GPP AAA Server. If the ePDG receives from this new server a

redirect indication towards the former server (due to the HSS having stored the former 3GPP AAA Server identity), it shall terminate all previously existing sessions and PDN connections for that user, and it shall re-send again the request towards the new server, but it shall include the AAA-Failure-Indication AVP in the new request.

The ePDG shall give preferential treatment to UEs which access the EPC for emergency services, e.g. in scenarios including network overload.

The ePDG shall store the WLAN Location Information associated with the UE when it receives such information from the 3GPP AAA Server.

If IMEI check is required by operator policy, the ePDG shall be configured to retrieve the IMEI(SV) from the UE (as specified in 3GPP TS 23.402 [26]) during the authentication and authorization procedure.

If the ePDG supports IMS Emergency sessions over WLAN (see clause 4.5.7.2 of 3GPP TS 23.402 [3]) and if local policies in the ePDG allows unauthenticated emergency sessions, the ePDG shall proceed during an Emergency Attach for a UE without a UICC or with an unauthenticated IMSI as specified above with the following modifications:

1) If the UE is UICC-less, the User Identity IE in the Authentication and Authorization Request shall contain the IMEI in Emergency NAI for Limited Service State format as defined in clause 19 of 3GPP TS 23.003 [14].

2) If the User Identity IE does not contain an IMEI (i.e. the UE has an IMSI), the ePDG shall request the IMEI from the UE as specified in clause 13.3 of 3GPP TS 33.402 [19] and clause 7.4.4 of 3GPP TS 24.302 [26] and include the IMEI in the Terminal-Information AVP in the next Authentication and Authorization Request message.

   The Authentication and Authorization Request in step 8 of clause 13.3 of 3GPP TS 33.402 [19] (i.e. after querying the UE's IMSI) shall contain the same parameters as provided in the first Authentication and Authorization Request (step 3) but with the addition of the IMEI in the Terminal-Information AVP.

NOTE 3: The IMEI cannot be signalled to the 3GPP AAA Server in the first Authentication and Authorization Request sent to the 3GPP AAA Server, since the ePDG requests the IMEI to the UE in the first IKE_AUTH_Response message after getting the first Authentication and Authorization Answer from the 3GPP AAA Server.

NOTE 4: The Authentication and Authorization Requests in steps 3 and 8 of clause 13.3 of 3GPP TS 33.402 [19] are handled independently from each other by the 3GPP AAA Server.

3) If the Permanent User Identity IE in the answer contains an IMEI based NAI but the User Identity IE in the request did not contain an IMEI based NAI, the ePDG shall derive that the IMSI was not authenticated and proceed accordingly with the setup of the Emergency PDN connection over S2b (see 3GPP TS 29.274 [38]).

7.1.2.2 Authorization Procedures

7.1.2.2.1 General

This procedure shall be used between the ePDG and 3GPP AAA Server and Proxy. It shall be invoked by the ePDG, upon receipt of a valid Re-Authorization Request message from the 3GPP AAA Server (see clause 7.1.2.5). It may also be initiated by the ePDG, when the ePDG detects a change of the outer IP address of the UE, to:

- update the 3GPP AAA Server with the new UE local IP address; and

- retrieve the most up to date WLAN Location Information stored at the 3GPP AAA Server, when the 3GPP AAA server has sent WLAN Location Information during the initial Authentication and Authorization procedure (see clause 4.5.7.2.8 of 3GPP TS 23.402 [3]).

This procedure shall be used by the ePDG to update the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example, removal of a specific APN associated with the subscriber, or change of the identity of a dynamically allocated PDN GW, see clause 8.1.2.3).

This procedure is mapped to the Diameter command codes AA-Request (AAR) and AA-Answer (AAA) specified in RFC 4005 [4]. Information element contents for these messages are shown in tables 7.1.2.2.1/1 and 7.1.2.2.1/2.

Table 7.1.2.2.1/1: SWm Authorization Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request Type	Auth-Request-Type	M	This information element shall contain the type of request. It shall have the value AUTHORIZE_ONLY.
AAR Flags	AAR-Flags	O	This IE contains a bit mask. See 7.2.3.5 for the meaning of the bits. This IE may be present and indicate that the ePDG requests to retrieve the most up to date WLAN Location Information of the UE, if the ePDG received the WLAN Location Information during the initial Authentication and Authorization procedure.
UE local IP address	UE-Local-IP-Address	C	This IE shall be present if the ePDG provided the UE Local IP address in the initial Authentication and Authorization Request and the UE Local IP address has changed.

Table 7.1.2.2.1/2: SWm Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Registration Result	Result-Code/ Experimental Result Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]) or as per in NASREQ (see IETF RFC 4005 [4]).
UE IPv4 Home Address	PMIP6-IPv4-Home-Address	O	If the authorization succeeded, and the user has an IPv4-HoA statically defined as part of his profile data, then this IE may be present. It shall contain the IPv4-HoA allocated and assigned to the UE.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI in the non-roaming case or in the home routed roaming case when constructing the PDN GW FQDN upon which it needs to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if NBM is used, the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request, and the Result-Code AVP is set to DIAMETER_SUCCESS.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS and the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When NBM is used, the following information elements per APN may be included: - APN - APN-AMBR - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN types - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - Visited Network Identifier When local IP address assignment is used, this AVP shall only be present if IKEv2 based Home Agent discovery is used and - if the PDN connection was active in case of HO, or - if there is static PDN GW allocated to the UE's subscribed APN. In these cases, the following information elements shall be included: - HA-APN (Home Agent APN as defined in 3GPP TS 23.003 [14]) - PDN GW identity
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is used to download the trace activation from the HSS to the ePDG. Only the Trace-Data AVP shall be included if trace activation is requested. Only the Trace-Reference AVP shall be included if trace deactivation is requested. If the Trace-Data AVP is included, it shall contain the following AVPs: - Trace-Reference - Trace-Depth - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List, for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.

MSISDN	Subscription-ID	C	This AVP shall contain the MSISDN of the UE and shall be sent only if it is available.
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
WLAN Location Information	Access-Network-Info	O	If present, this IE shall contain the location information of the WLAN Access Network where the UE is attached.
WLAN Location Timestamp	User-Location-Info-Time	C	This IE should be present if the WLAN Location Information IE is present. When present, this IE shall contain the NTP time at which the UE was last known to be in the location reported in the WLAN Location Information.

7.1.2.2.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall process the steps in the following order (if there is an error in any of the steps, the 3GPP AAA Server shall stop processing and return the corresponding error code):

1) Check that the user exists in the 3GPP AAA Server. The check shall be based on Diameter Session-id and User Name. If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) If the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request, check whether the user is allowed to access the APN. If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

3) The Result-Code shall be set to DIAMETER_SUCCESS and, if the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request, the 3GPP AAA Server shall return user data relevant to the APN as received from the HSS.

4) If the WLAN-Location-Info-Request bit is set to 1 in the AAR-Flags AVP and if the 3GPP AAA Server knows the WLAN Location Information of the UE, the 3GPP AAA Server shall provide it to the ePDG, along with the WLAN Location Timestamp if available (see clause 4.1.2.1.2).

If the Emergency-Indication bit of the Emergency-Services AVP was not set in the initial Authentication and Authorization Request, once the Authentication and Authorization procedure successfully finishes, the 3GPP AAA Server shall download, together with authentication data, the list of authorized APNs and the authorized mobility protocols in the authentication and authorization response from the HSS (see SWx procedure in Clause 8.1.2.1).

Exceptions to the cases specified here shall be treated by 3GPP AAA Server as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and, therefore, no authorization information shall be returned.

If the 3GPP AAA Server answers with DIAMETER_AUTHORIZATION_REJECTED, it shall terminate locally the associated SWm Diameter session.

7.1.2.2.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy shall be required to handle roaming cases in which the ePDG is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy, with the following extensions.

On receipt of the authorization answer, the 3GPP AAA Proxy:

- Shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.

- Shall record the state of the connection (i.e. Authorization Successful).

If the 3GPP AAA Proxy receives a DIAMETER_AUTHORIZATION_REJECTED response from the 3GPP AAA Server, it shall forward it to the ePDG, and terminate locally the associated SWm Diameter session.

7.1.2.2.4 ePDG Detailed Behaviour

Upon receipt of a valid Re-Authorization Request message from the 3GPP AAA Server, the ePDG shall initiate the authorization procedure after successfully completing the authentication of the user. The ePDG shall initiate a separate authorization session for each IKE_SA of the user. When initiated by the ePDG to retrieve the most up to date WLAN Location Information stored at the 3GPP AAA Server, the ePDG shall initiate the authorization procedure for one IKE_SA of the user.

If NBM is used, at successful completion of the procedure, the ePDG shall store the APN configuration data received from the 3GPP AAA Server. The ePDG shall utilize these data to authorize the requested home address types: IPv4 home address and/or IPv6 home network prefix.

NOTE: The user will be allowed to create PDN connections only to the subscribed APNs and use the address types that are allowed by the subscribed PDN types.

Upon receiving the authorization response:

- If NBM is used and if any other Result-Code than DIAMETER_SUCCESS was received in the response, the ePDG shall release the corresponding PDN connection (PMIPv6 binding or GTPv2 tunnel) and IKE_SA of the user, and terminate locally the associated SWm Diameter session.
- If DSMIPv6 is used,
  - If any other Result-Code than DIAMETER_SUCCESS was received, the ePDG shall release the corresponding IKE_SA of the user, and terminate locally the associated SWm Diameter session.
  - If the Result-Code DIAMETER_SUCCESS was received in the response, the ePDG shall update the previously provided authorization parameters.

NOTE: The ePDG knows if NBM is used or if a local IP address is assigned based on the flags in the MIP6-Feature-Vector received during the initial authentication and authorization procedure or based on preconfigured information. If the PMIP6_SUPPORTED and/or the GTPv2_SUPPORTED flag are set in the MIP6-Feature-Vector received from the 3GPP AAA Server, the ePDG knows that NBM is used.

If GTPv2 is used on S2b and if the Trace-Info AVP including Trace-Data has been received in the authorization response, the ePDG shall send a GTPv2 Trace Session Activation message (see 3GPP TS 29.274 [38]) to the PGW to start a trace session for the user. If the Trace-Info AVP including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the ePDG shall send a GTPv2 Trace Session Deactivation message to the PGW to stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

If DSMIPv6 is used and if ePDG has received the PGW identity in form of the FQDN from the 3GPP AAA server, then the ePDG may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

The ePDG shall store the WLAN Location Information associated with the UE when it receives such information from the 3GPP AAA Server. The ePDG shall delete any stored WLAN Location Information associated with the UE when it receives from the 3GPP AAA Server an Authorization Answer not including any WLAN Location Information and the WLAN-Location-Info-Request bit was set to 1 in the AAR-Flags AVP.

7.1.2.3 ePDG Initiated Session Termination Procedures

7.1.2.3.1 General

The SWm reference point allows the ePDG to inform the 3GPP AAA Server/Proxy about the termination of an IKE_SA between UE and ePDG, and that therefore the mobility session established on the ePDG for all associated PDN connections are to be removed.

The SWm Session Termination Request procedure shall be initiated by the ePDG to the 3GPP AAA Server which shall remove associated non-3GPP Access information. The AAA Server shall then return the SWm Session Termination Answer containing the result of the operation. These procedures are based on the reuse of Diameter STR and STA commands as specified in IETF RFC 6733 [58].

Table 7.1.2.3.1/1: SWm Session Termination Request

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Termination Cause	Termination-Cause	M	This information element shall contain the reason for the disconnection.

Table 7.1.2.3.1/2: SWm Session Termination Answer

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	M	This IE shall contain the result of the operation.

7.1.2.3.2 3GPP AAA Server Detailed Behavior

Upon reception of the Session Termination Request message from the ePDG, the 3GPP AAA Server shall check that there is an ongoing session associated to the two parameters received (Session-Id and User-Name).

If an active session is found and it belongs to the user identified by the User-Name parameter, the 3GPP AAA Server shall release the session resources associated to the specified session and a Session Termination Response shall be sent to the ePDG, indicating DIAMETER_SUCCESS.

Otherwise, the 3GPP AAA Server returns a Session Termination Response with the Diameter Error DIAMETER_UNKNOWN_SESSION_ID.

7.1.2.3.3 3GPP AAA Proxy Detailed Behavior

The 3GPP AAA Proxy is required to handle roaming cases in which the ePDG is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Session Termination Request message from the ePDG, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server.

On receipt of the Session Termination Answer message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the ePDG, and it shall release any local resources associated to the specified session only if the result code is set to DIAMETER_SUCCESS.

7.1.2.4 3GPP AAA Server Initiated Session Termination Procedures

7.1.2.4.1 General

The SWm reference point shall allow the 3GPP AAA Server to request the termination of an IKE_SA between UE and ePDG, and therefore the termination of all mobility session established for all associated PDN connections.

If the user has several accesses (IKE_SA) active at an ePDG, a separate Session Termination procedure shall be initiated for each of them.

The procedure shall be initiated by the 3GPP AAA Server. This procedure is based on the reuse of NASREQ IETF RFC 4005 [4] ASR, ASA, STR and STA commands.

Table 7.1.2.4.1/1: SWm Abort Session Request

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Auth-Session-State	Auth-Session-State	O	If present, this information element indicates to the ePDG whether the 3GPP AAA Server requires an STR message.

Table 7.1.2.4.1/2: SWm Abort Session Answer

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code	M	This IE shall contain the result of the operation.

Table 7.1.2.4.1/3: SWm Session Termination Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Termination-Cause	Termination-Cause	M	This information element shall contain the reason why the session was terminated. It shall be set to "DIAMETER_ADMINISTRATIVE" to indicate that the session was terminated in response to an ASR message.

Table 7.1.2.4.1/4: SWm Session Termination Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall contain the result of the operation.

7.1.2.4.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to instruct the ePDG to terminate the IKE_SA between UE and ePDG.

In the DSMIPv6 case, the 3GPP AAA Server shall initiate first the detach procedure over the S6b reference point towards the PDN GW. When this process has finalized, the 3GPP AAA Server can initiate the termination of the IKE_SA towards the ePDG.

The 3GPP AAA Server shall include the Auth-Session-State AVP in the ASR command with a value of NO_STATE_MAINTAINED if it does not require a STR from the ePDG. If it does require a STR from the ePDG, the 3GPP AAA Server shall either omit the Auth-Session-State AVP from the ASR command or include the Auth-Session-State AVP in the ASR command with a value of STATE_MAINTAINED.

On receipt of the ASR command, the ePDG shall check if there is an ongoing session associated with the received Session-Id. If an active session is found and it belongs to the user identified by the User-Name parameter, the ePDG shall terminate the associated IKE_SA between UE and ePDG and return an ASA to the 3GPP AAA Server with the Result-Code to DIAMETER_SUCCESS. Otherwise, the ePDG shall return an ASA to the 3GPP AAA Server with the Result-Code set to DIAMETER_UNKNOWN_SESSION_ID.

On receipt of the ASA with a Result-Code of DIAMETER_SUCCESS, the 3GPP AAA Server shall release any local resources associated with the specified session.

If required by the 3GPP AAA Server, the ePDG shall send an STR with the Termination-Cause set to DIAMETER_ADMINISTRATIVE. The 3GPP AAA Server shall set the Result-Code to DIAMETER_SUCCESS and return the STA command to the ePDG.

7.1.2.4.3 3GPP AAA Proxy Detailed Behaviour

When the 3GPP AAA Proxy receives the ASR from the 3GPP AAA Server it shall route the request to the ePDG.

If the 3GPP AAA Proxy requires an STR but the 3GPP AAA Server does not, the 3GPP AAA Proxy may override the value of the Auth-Session-State in the ASR and set it to STATE_MAINTAINED. In this case, the 3GPP AAA Proxy shall not forward the STR received from the ePDG onto the 3GPP AAA Server and shall return an STA command to the ePDG with the Result-Code set to DIAMETER_SUCCESS. The 3GPP AAA Proxy shall not override the value of the Auth-Session-State AVP under any other circumstances.

On receipt of the ASA message with Diameter Result Code set to DIAMETER_SUCCESS, the 3GPP AAA Proxy shall route the successful response to the 3GPP AAA Server and shall release any local resources associated with the session.

When the 3GPP AAA Proxy receives the STR from ePDG, it shall route the request to the 3GPP AAA Server. On receipt of the STA message, the 3GPP AAA Proxy shall route the response to the ePDG.

7.1.2.5 Authorization Information Update Procedures

7.1.2.5.1 General

This procedure shall be used between the 3GPP AAA Server and the ePDG for the purpose of modifying the previously provided authorization parameters. This may happen due to a modification of the subscriber profile in the HSS (for example change of the identity of a dynamically allocated PDN GW, see clause 8.1.2.3).

This procedure shall be performed in two steps:

- The 3GPP AAA Server shall issue an unsolicited re-authorization request towards the ePDG. Upon receipt of such a request, the ePDG shall respond to the request and indicate the disposition of the request. This procedure is based on the Diameter commands Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 6733 [58]. Information element contents for these messages shall be as shown in tables 7.1.2.5.1/1 and 7.1.2.5.1/2.

- Upon receiving the re-authorization request, the ePDG shall immediately invoke the authorization procedure specified in 7.1.2.2 for the session indicated in the request. This procedure is based on the Diameter commands AA-Request (AAR) and AA-Answer (AAA) specified in IETF RFC 4005 [4]. Information element contents for these messages are shown in tables 7.1.2.2.1/1 and 7.1.2.2.1/2.

Table 7.1.2.5.1/1: SWm Authorization Information Update Request

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Re-Auth Request Type	Re-Auth-Request-Type	M	This IE shall define whether the user is to be authorized only or authenticated and authorized. AUTHORIZE_ONLY shall be set in this case.
Routing Information	Destination-Host	M	This information element shall be obtained from the Origin-Host AVP, which was included in a previous command received from the trusted non-3GPP access.

Table 7.1.2.5.1/2: SWm Authorization Information Update Answer

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. If this IE contains an identity based on IMSI, this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Result	Result-Code	M	This IE shall contain the result of the operation.

7.1.2.5.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA server shall make use of the re-authorization procedure defined in the Diameter base protocol, IETF RFC 6733 [58] to indicate that relevant service authorization information shall be updated in the ePDG.

7.1.2.5.3 ePDG Detailed Behaviour

Upon receipt of the Re-authorization Request message from the 3GPP AAA Server or the 3GPP AAA Proxy, the ePDG shall check that there is an ongoing session associated to any of the parameters received in the message (identified by the Session-Id AVP and the User-Name AVP).

If an active session is found, the ePDG shall initiate an authorization procedure for the session identified by the Session-Id AVP and the User-Name AVP and a Re-authorization Answer message shall be sent to the 3GPP AAA Server or the 3GPP AAA Proxy with the Result-Code indicating DIAMETER_SUCCESS. This new authorization procedure shall be performed as described in clause 7.1.2.2.

If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, then an Re-authorization Answer message shall be sent to the 3GPP AAA Server or the 3GPP AAA Proxy with the Result-Code indicating DIAMETER_UNKNOWN_SESSION_ID.

Exceptions to the cases specified here shall be treated by ePDG as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY and, therefore, no authorization procedure shall be initiated.

Table 7.1.2.5.3/1 details the valid result codes that the ePDG can return in the response.

Table 7.1.2.5.3/1: Re-authorization Answer valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_UNKNOWN_SESSION_ID	The request failed because the user is not found in ePDG.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

7.2 Protocol Specification

7.2.1 General

The SWm reference point shall be based on Diameter, as defined in IETF RFC 6733 [58] and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 4072 [5], which provides a Diameter application to support the transport of EAP (IETF RFC 3748 [8]) frames over Diameter.
- IETF RFC 5779 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.

- IETF RFC 5447 [6], which defines Diameter extensions for Mobile IPv6 NAS to AAA interface.

In the case of an untrusted non-3GPP IP access, the MAG to 3GPP AAA server or the MAG to 3GPP AAA proxy communication shall use the MAG to AAA interface functionality defined in IETF RFC 5779 [2] and the NAS to AAA interface functionality defined in IETF RFC 5447 [6].

The Diameter application for the SWm reference point shall use the Diameter Application Id with value 16777264.

7.2.2 Commands

7.2.2.1 Commands for SWm Authentication and Authorization Procedures

7.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 5779 [2].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777264 >
                             < Session-Id >
                             [ DRMP ]
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             [ Destination-Host ]
                             { Auth-Request-Type }
                             { EAP-Payload }
                             [ User-Name ]
                             [ RAT-Type ]
                             [ Service-Selection ]
                             [ MIP6-Feature-Vector ]
                             [ QoS-Capability ]
                             [ Visited-Network-Identifier ]
                             [ AAA-Failure-Indication ]
                             *[ Supported-Features ]
                             [ UE-Local-IP-Address ]
                             [ OC-Supported-Features ]
                             [ Terminal-Information ]
                             [ Emergency- Services ]
                             …
                             *[ AVP ]
```

7.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DER) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to the ePDG. The ABNF is based on the one in IETF RFC 5779 [2].

```
< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777264>
                            < Session-Id >
                            [ DRMP ]
                            { Auth-Application-Id }
                            { Auth-Request-Type }
                            { Result-Code }
                            { Origin-Host }
                            { Origin-Realm }
                            [ EAP-Payload ]
                            [ User-Name ]
                            [ EAP-Master-Session-Key ]
                            [ APN-OI-Replacement ]
```

[APN-Configuration]
[MIP6-Feature-Vector]
[Mobile-Node-Identifier]
[Trace-Info]
[Subscription-ID]
[Session-Timeout]
[MIP6-Agent-Info]
[3GPP-Charging-Characteristics]
*[Redirect-Host]
*[Supported-Features]
[OC-Supported-Features]
[OC-OLR]
*[Load]
[Access-Network-Info]
[User-Location-Info-Time]
[UE-Usage-Type][Emergency-Info]
[Core-Network-Restrictions]
…
*[AVP]

7.2.2.1.3 Diameter-AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a ePDG to a 3GPP AAA Server/Proxy.

<AA-Request> ::= < Diameter Header: 265, REQ, PXY, 16777264 >
< Session-Id >
[DRMP]
{ Auth-Application-Id }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ Auth-Request-Type }
[User-Name]
[OC-Supported-Features]
[AAR-Flags]
[UE-Local-IP-Address]
…
*[AVP]

7.2.2.1.4 Diameter-AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from 3GPP AAA Server/Proxy to a ePDG.

<AA-Answer> ::= < Diameter Header: 265, REQ, PXY, 16777264 >
< Session-Id >

[DRMP]
{ Auth-Application-Id }
{ Auth-Request-Type }
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[APN-OI-Replacement]
[APN-Configuration]
[Trace-Info]
[Subscription-ID]
[3GPP-Charging-Characteristics]
[Session-Timeout]
[OC-Supported-Features]
[OC-OLR]
*[Load]
[Access-Network-Info]
[User-Location-Info-Time]
…
*[AVP]

7.2.2.2 Commands for ePDG Initiated Session Termination

7.2.2.2.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 6733 [58], and is defined as follows:

< Session-Termination-Request > ::= < Diameter Header: 275, REQ, PXY, 16777264 >
< Session-Id >
[DRMP]
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ Auth-Application-Id }
{ Termination-Cause }
[User-Name]
[OC-Supported-Features]
…
*[AVP]

7.2.2.2.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit clear in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a ePDG. The ABNF is based on the one in IETF RFC 6733 [58], and is defined as follows:

< Session-Termination-Answer > ::= < Diameter Header: 275, PXY, 16777264 >
< Session-Id >
[DRMP]
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
[OC-Supported-Features]
[OC-OLR]
*[Load]
…
*[AVP]

7.2.2.3 Commands for 3GPP AAA Server Initiated Session Termination

7.2.2.3.1 Abort-Session-Request (ASR) Command

The Abort-Session-Request (ASR) command shall be indicated by the Command-Code field set to 274 and the "R" bit set in the Command Flags field, and shall be sent from a 3GPP AAA Server/Proxy to an ePDG. The ABNF is based on that in IETF RFC 4005 [4].

```
< Abort-Session-Request > ::= < Diameter Header: 274, REQ, PXY, 16777264 >
                              < Session-Id >
                              [ DRMP ]
                              { Origin-Host }
                              { Origin-Realm }
                              { Destination-Realm }
                              { Destination-Host }
                              { Auth-Application-Id }
                              [ User-Name ]
                              [ Auth-Session-State ]
                              …
                              *[ AVP ]
```

7.2.2.3.2 Abort-Session-Answer (ASA) Command

The Abort-Session-Answer (ASA) command shall be indicated by the Command-Code field set to 274 and the "R" bit cleared in the Command Flags field, and shall be sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on that in IETF RFC 4005 [4].

```
< Abort-Session-Answer > ::= < Diameter Header: 274, PXY, 16777264 >
                             < Session-Id >
                             [ DRMP ]
                             { Result-Code }
                             { Origin-Host }
                             { Origin-Realm }
                             …
                             *[ AVP ]
```

7.2.2.3.3 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from an ePDG to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58] Session-Termination-Request command.

```
<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777264 >
                                  < Session-Id >
                                  [ DRMP ]
                                  { Origin-Host }
                                  { Origin-Realm }
                                  { Destination-Realm }
                                  [ Destination-Host ]
                                  { Auth-Application-Id }
                                  { Termination-Cause }
                                  [ User-Name ]
                                  [ OC-Supported-Features ]
                                  …
                                  *[ AVP ]
```

7.2.2.3.4 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to an ePDG. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777264 >
                                 < Session-Id >
                                 [ DRMP ]
                                 { Result-Code }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 [ OC-Supported-Features ]
                                 [ OC-OLR ]
                                 *[ Load ]
                                 *[ AVP ]
```

7.2.2.4 Commands for Authorization Information Update

7.2.2.4.1 Re-Auth-Request (RAR) Command

The Re-Auth-Request (RAR) command shall be indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field, and shall be sent from a 3GPP AAA Server/Proxy to a ePDG. The ABNF is based on the one in IETF RFC 4005 [4] and is defined as follows.

```
< Re-Auth-Request > ::=  < Diameter Header: 258, REQ, PXY, 16777264 >
                         < Session-Id >
                         [ DRMP ]
                         { Origin-Host }
                         { Origin-Realm }
                         { Destination-Realm }
                         { Destination-Host }
                         { Auth-Application-Id }
                         { Re-Auth-Request-Type }
                         [ User-Name ]
                         …
                         *[ AVP ]
```

7.2.2.4.2 Re-Auth-Answer (RAA) Command

The Re-Auth-Answer (RAA) command shall be indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field, and shall be sent from a ePDG to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 4005 [4] and is defined as follows.

```
< Re-Auth-Answer > ::=< Diameter Header: 258, PXY, 16777264 >
                       < Session-Id >
                       [ DRMP ]
                       { Result-Code }
                       { Origin-Host }
                       { Origin-Realm }
                       [ User-Name ]
                       …
                       *[ AVP ]
```

7.2.3 Information Elements

7.2.3.1 General

The following table describes the Diameter AVPs defined for the SWm interface protocol for untrusted non-3GPP access, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

Table 7.2.3.1/1: Diameter SWm AVPs

				AVP Flag rules			
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**
APN-Configuration	1430	8.2.3.7	Grouped	M,V			P
Mobile-Node-Identifier	506	5.2.3.2	OctetString	M			V,P
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V,P
QoS-Capability	578	9.2.3.2.4	Grouped	M			V,P
RAT-Type	1032	5.2.3.6	Enumerated	M,V			P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
Trace-Info	1505	8.2.3.1.3	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
AAA-Failure-Indication	1518	8.2.3.21	Unsigned32	V			M,P
Emergency- Services	1538	7.2.3.4	Unsigned32	V			M,P
Access-Network-Info	1526	5.2.3.24	Grouped	V			M,P
AAR-Flags	1539	7.2.3.5	Unsigned32	V			M,P
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 [58]. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.							

The following table describes the Diameter AVPs re-used by the SWm interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within SWm. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol defined in IETF RFC 6733 [58], do not need to be supported.

Table 7.2.3.1/2: SWm re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
Auth-Request-Type	IETF RFC 6733 [58]		
Subscription-ID	IETF RFC 4006 [20]		
EAP-Master-Session-Key	IETF RFC 4072 [5]		
EAP-Payload	IETF RFC 4072 [5]		
Re-Auth-Request-Type	IETF RFC 6733 [58]		
Session-Timeout	IETF RFC 6733 [58]		
User-Name	IETF RFC 6733 [58]		
MIP6-Agent-Info	IETF RFC 5447 [6]		
APN-OI-Replacement	3GPP TS 29.272 [29]		
Terminal-Information	3GPP TS 29.272 [29]		
Supported-Features	3GPP TS 29.229 [24]		
Feature-List-ID	3GPP TS 29.229 [24]	See clause 7.2.3.2	
Feature-List	3GPP TS 29.229 [24]	See clause 7.2.3.3	
3GPP-Charging-Characteristics	3GPP TS 29.061 [31]		
UE-Local-IP-Address	3GPP TS 29.212 [23]		
OC-Supported-Features	IETF RFC 7683 [47]	See clause 8.2.3.22	
OC-OLR	IETF RFC 7683 [47]	See clause 8.2.3.23	
User-Location-Info-Time	3GPP TS 29.212 [23]	See clause 5.3.101	
DRMP	IETF RFC 7944 [53]	See clause 8.2.3.25	Must not set
Emergency-Info	3GPP TS 29.272 [29]		
Load	IETF RFC 8583 [54]	See clause 8.2.3.26	Must not set
UE-Usage-Type	3GPP TS 29.272 [29]		
Core-Network-Restrictions	3GPP TS 29.272 [29]		
NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.			

Only those AVP initially defined in this reference point and for this procedure are described in the following clauses.

7.2.3.2 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the SWm application.

7.2.3.3 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the SWm application.

NOTE: There are no SWm features defined for this release.

7.2.3.4 Emergency-Services

The Emergency-Services AVP is of type Unsigned32 and it shall contain a bitmask. The meaning of the bits is defined in table 7.2.3.4/1:

Table 7.2.3.4/1: Emergency-Services

Bit	Name	Description
0	Emergency-Indication	This bit, when set, indicates a request to establish a PDN connection for emergency services.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver.		

7.2.3.5 AAR-Flags

The AAR-Flags AVP is of type Unsigned32 and it shall contain a bitmask. The meaning of the bits is defined in table 7.2.3.5/1:

Table 7.2.3.5/1: AAR-Flags

Bit	Name	Description
0	WLAN-Location-Info-Request	This bit, when set, indicates an ePDG request to retrieve the most up to date WLAN Location Information of the UE stored at the 3GPP AAA Server.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver.		

7.2.4 Session Handling

The Diameter protocol between the ePDG and the 3GPP AAA Server or the 3GPP AAA Proxy shall always keep the session state, and use the same Session-Id parameter for the lifetime of each Diameter session.

A Diameter session shall identify

- a PDN Connection of a given user, if NBM is used
- a user, if DSMIPv6 is used.

In order to indicate that the session state is to be maintained, the Diameter client and server shall not include the Auth-Session-State AVP, either in the request or in the response messages (see IETF RFC 6733 [58]).

8 SWx Description

8.1 Functionality

8.1.1 General

The SWx reference point is defined between the 3GPP AAA Server and the HSS. The description of the reference point and its functionality is given in 3GPP TS 23.402 [3].

The SWx reference point is used to authorize the UE and to transport NBM related mobility parameters when NBM is used to establish connectivity to the EPC.

The SWx is used to authenticate and authorize the UE when the S2a, S2b or S2c reference points are used to connect to EPC. This reference point is also used to update the HSS with the PDN-GW address information. Additionally, this reference point may be used to retrieve and update other mobility related parameters including static QoS profiles for non-3GPP accesses.

Additional requirements for the SWx interface can be found in clause 12 of 3GPP TS 23.402 [3].

8.1.2 Procedures Description

8.1.2.1 Authentication Procedure

8.1.2.1.1 General

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the 3GPP AAA Server when a new set of authentication information for a given subscriber is to be retrieved from an HSS. This can happen for example, when a new trusted or untrusted non 3GPP/IP access subscriber has accessed the 3GPP AAA Server for authentication or when a new set of authentication information is required for one of the subscribers already

registered in the 3GPP AAA server. The procedure shall be invoked by 3GPP AAA Server when it detects that the VPLMN or access network has changed.

Table 8.1.2.1.1/1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Visited Network Identifier	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the Visited Network. The 3GPP AAA Server shall include this information element when received from signalling across the SWd.
Number Authentication Items	SIP-Number-Auth-Items	M	This information element shall indicate the number of authentication vectors requested
Authentication Data	SIP-Auth-Data-Item	M	See tables 8.1.2.1.1/2 and 8.1.2.1.1/3 for the contents of this information element. The content shown in table 8.1.2.1.1/2 shall be used for a normal authentication request; the content shown in table 8.1.2.1.1/3 shall be used for an authentication request after synchronization failure.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name, this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name shall be obtained from the Origin-Host AVP, which is received from a previous command from the HSS or from the SLF; otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.
Access Network Identity	ANID	C	This IE shall contain the access network identifier used for key derivation at the HSS. (See 3GPP TS 24. 302 [26] for all possible values). This IE shall be present if the Authentication Method is EAP-AKA'.
Access Type	RAT-Type	M	This IE shall contain the radio access technology that is serving the UE. (See 3GPP TS 29.212 [23] for all possible values). When this IE is not received by the 3GPP AAA Server, neither from the ePDG nor from the non-3GPP access network, it shall take the value VIRTUAL (1).
Terminal Information	Terminal-Information	O	This information element shall contain information about the user's mobile equipment. The AVP shall be present only if received from the non-3GPP access network, in authentication and authorization request. The AVP shall be transparently forwarded by the 3GPP AAA server. (see NOTE 1)
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the 3GPP AAA Server currently registered in the HSS, is unavailable.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
NOTE 1: The Terminal-Information AVP is not present in this message for a WLAN access.			

Table 8.1.2.1.1/2: Authentication Data content - request

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Method	SIP-Authentication-Scheme	M	This information element shall indicate the authentication method It shall contain one of the values EAP-AKA or EAP-AKA'. EAP-AKA is specified in IETF RFC 4187 [44] and EAP-AKA' is specified in IETF RFC 5448 [27].

Table 8.1.2.1.1/3: Authentication Data content - request, synchronization failure

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Method	SIP-Authentication-Scheme	M	This information element shall indicate the authentication method It shall contain one of the values EAP-AKA or EAP-AKA'.
Authorization Information	SIP-Authorization	M	This IE shall contain the concatenation of Rand, as sent to the terminal, and auts, as received from the terminal. Rand and auts shall both be binary encoded.

Table 8.1.2.1.1/4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See I IETF RFC 6733 [58])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Number Authentication Items	SIP-Number-Auth-Items	C	This AVP shall indicate the number of authentication vectors delivered in the Authentication Data information element. It shall be present when the result is DIAMETER_SUCCESS.
Authentication Data	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero or it is not present, then this AVP shall not be present. See table 8.1.2.1.1/5 for the contents of this information element.
3GPP AAA Server Name	3GPP-AAA-Server-Name	C	This AVP shall contain the Diameter address of the 3GPP AAA Server. This AVP shall be sent when the user has been previously authenticated by another 3GPP AAA Server and therefore there is another 3GPP AAA Server serving the user.
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.1.2.1.1/5: Authentication Data content - response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Method	SIP-Authentication Scheme	M	This IE shall contain one of the values EAP-AKA or EAP-AKA'.
Authentication Information AKA	SIP-Authenticate	M	This IE shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [16] for further details about RAND and AUTN.
Authorization Information AKA	SIP-Authorization	M	This IE shall contain binary encoded, the expected response XRES. See 3GPP TS 33.203 [16] for further details about XRES.
Confidentiality Key AKA	Confidentiality-Key	M	This information element shall contain the confidentiality key CK or CK'. It shall be binary encoded.
Integrity Key AKA	Integrity-Key	M	This information element shall contain the integrity key IK or IK'. It shall be binary encoded.

8.1.2.1.2 Detailed behaviour

The HSS shall, in the following order (if there is an error in any of the steps, the HSS shall stop processing and return the corresponding error code):

1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check that the user has non-3GPP subscription and that the user is allowed in the EPC. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTON.

3. If a Visited-Network-Identifier is present, check that the user is allowed to roam in the visited network. If the user is not allowed to roam in the visited network, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED.

4. Check the access type. If the access type indicates any value that is restricted for the user, then the Experimental-Result-Code shall be set to DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED.

5. The HSS shall check if there is an existing 3GPP AAA Server already assisting the user

   - If there is a 3GPP AAA Server already serving the user, the HSS shall compare the 3GPP AAA server name received in the request to the 3GPP AAA Server name stored in the HSS.

   - If they are not identical and the received message contains the AAA-Failure-Indication AVP, the HSS shall remove the old 3GPP AAA Server name previously assigned for this subscriber, and store the name of the new 3GPP AAA Server that sent the request containing the AAA-Failure-Indication AVP, and continue from step 6. The HSS should attempt to notify the old 3GPP AAA Server about the new server assignment, by means of the network initiated de-registration procedure (see clause 8.1.2.2.3) indicating as reason code "NEW_SERVER_ASSIGNED".

   - If they are not identical the HSS shall return the old 3GPP AAA Server to the requester 3GPP AAA Server and return an error by setting the Experimental-Result-Code to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

   - The requester 3GPP AAA Server, upon detection of a 3GPP AAA Server name in the response assumes that the user already has a 3GPP AAA Server assigned, so makes use of Diameter redirect function to indicate the 3GPP AAA Server name where to address the authentication request.

6. The HSS shall check the request type.

   - If the request indicates there is a synchronization failure, the HSS shall process AUTS as described in 3GPP TS 33.203 [16] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

   - If the request indicates authentication, the HSS shall generate the authentication vectors for the requested authentication method, EAP-AKA or EAP-AKA', as described in 3GPP TS 33.402 [19]. The HSS shall download Authentication-Data-Item up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The result code shall be set to DIAMETER_SUCCESS.

- If there is no 3GPP AAA Server already serving the user, the HSS shall store the received 3GPP AAA Server name.

Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

Origin-Host AVP shall contain the 3GPP AAA Server identity.

8.1.2.2 Location Management Procedures

8.1.2.2.1 General

According to the requirements described in 3GPP TS 23.402 [3], SWx reference point shall enable:

- Registration of the 3GPP AAA Server serving an authorized trusted or untrusted non-3GPP access user in the HSS.

- Retrieval of charging-related information from HSS.

- Deregistration procedure between the 3GPP AAA Server and the HSS.

- Retrieval of subscriber profile from HSS.

8.1.2.2.2 UE/PDN Registration/DeRegistration Notification

8.1.2.2.2.1 General

This procedure is used between the 3GPP AAA Server and the HSS.

- To register the current 3GPP AAA Server address in the HSS for a given non-3GPP user. This procedure is invoked by the 3GPP AAA Server after a new subscriber has been authenticated by the 3GPP AAA Server.

- To de-register the current 3GPP AAA Server address in the HSS for a given non-3GPP user. This procedure is invoked when the 3GPP AAA Server removes the access information for a non-3GPP user after all sessions for the user (i.e. the STa, SWm, S6b sessions) have been terminated.

- To download the subscriber profile to the 3GPP AAA Server on demand. This procedure is invoked when for some reason the subscription profile of a subscriber is lost.

- To update the HSS with the identity and the PLMN ID of a dynamically allocated PDN GW as a result of the first PDN connection establishment associated to an APN.

- To update the HSS with the identity of the dynamically allocated PDN GW selected for the establishment of an emergency PDN connection.

Table 8.1.2.2.2.1/1: Non-3GPP IP Access Registration request

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Server Assignment Type	Server-Assignment-Type	M	This IE shall contain the type of procedure the 3GPP AAA Server requests in the HSS. When this IE contains REGISTRATION value, the 3GPP AAA Server requests the HSS to perform a registration of the non-3GPP user. When this IE contains USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / AUTHENTICATION_FAILURE / AUTHENTICATION_TIMEOUT, the 3GPP AAA Server requests the HSS to de-register the non-3GPP user. When this IE contains AAA_USER_DATA_REQUEST value, the 3GPP AAA Server requests the HSS to download the subscriber user profile towards the 3GPP AAA Server as part of 3GPP AAA Server initiated profile download request, but no registration is requested. When this IE contains PGW_UPDATE value, the 3GPP AAA Server requests the HSS to update the PGW identity for the non-3GPP user for an APN in the user subscription or for emergency services. Any other value shall be considered as an error case.
Routing Information	Destination-Host	C	If the 3GPP AAA Server knows the HSS name this AVP shall be present. This information is available if the 3GPP AAA Server already has the HSS name stored. The HSS name shall be obtained from the Origin-Host AVP, which is received from the HSS as part of authentication response; otherwise only the Destination-Realm is included so that it is resolved to an HSS address in an SLF-like function. Once resolved the Destination-Host AVP shall be included with the suitable HSS address and it shall be stored in the 3GPP AAA Server for further usage.
PGW identity	MIP6-Agent-Info	C	This IE shall contain, either the identity of the dynamically allocated PDN GW, or the identity of a dynamically allocated PDN GW selected for the establishment of emergency PDN connections, and is included if the Server-Assignment-Type is set to PGW_UPDATE.
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identity of the PLMN where the PDN-GW was allocated, in cases of dynamic PDN-GW assignment. It shall be present when the PGW Identity is present and does not contain an FQDN.
Context Identifier	Context-Identifier	O	For non-emergency PDN connection establishment, this parameter shall identify the APN Configuration with which the reallocated PDN GW shall be correlated, and it may be included if it is available and the Server-Assignment-Type is set to PGW_UPDATE. For emergency PDN connection establishment, this information element shall be left absent.
APN Id	Service-Selection	C	For non-emergency PDN connection establishment, this information element shall contain the Network Identifier part of the APN, and it shall be included if the Server-Assignment-Type is set to PGW_UPDATE. For emergency PDN connection establishment, this information element shall be left absent.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
Terminal Information	Terminal-Information	C	The 3GPP AAA Server shall include this IE and set it to the user's Mobile Equipment Identity, if this information is available, and if the Server-Assignment-Type is set to REGISTRATION. This IE shall also be present, independently of the value of the Server-Assignment-Type, if the Terminal-Information has changed from the last value previously reported to the HSS. This grouped AVP shall contain the IMEI AVP and, if available, the Software-Version AVP, for a trusted or untrusted WLAN access. When the RAT type is not known by the 3GPP AAA Server, but the UE has provided the IMEI(SV), this grouped AVP shall contain the IMEI AVP and, if available, the Software-Version AVP.

Emergency Services	Emergency-Services	C	The 3GPP AAA Server shall include this information element, and set the Emergency-Indication bit, to notify the HSS that a new PDN-GW has been selected for the establishment of an emergency PDN connection, whose identity is conveyed in the "PGW identity" IE. This IE shall only be included when the Server-Assignment-Type is set to PGW_UPDATE.

Table 8.1.2.2.2.1/2: Non-3GPP IP Access Registration response

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Registration result	Result-Code / Experimental-Result	M	This IE contains the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile	Non-3GPP-User-Data	C	This IE shall contain the relevant user profile. Clause 8.2.3.1 details the contents of the AVP. It shall be present when Server-Assignment-Type in the request is equal to AAA_USER_DATA_REQUEST or REGISTRATION and the Result-Code is equal to DIAMETER_SUCCESS.
3GPP AAA Server Name	3GPP-AAA-Server-Name	C	This AVP shall contain the Diameter address of the 3GPP AAA Server. This AVP shall be present when the user has been previously authenticated by another 3GPP AAA Server and therefore there is another 3GPP AAA Server serving the user.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

8.1.2.2.2.2 Detailed behaviour

When a new trusted or untrusted non-3GPP IP access subscriber has been authenticated by the 3GPP AAA Server, the 3GPP AAA Server initiates the registration towards the HSS. The HSS shall, in the event of an error in any of the steps, stop processing and return the corresponding error code.

At reception of the Non-3GPP IP Access Registration, the HSS shall perform (in the following order):

1. Check that the user is known. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS shall check if there is an existing 3GPP AAA Server already assisting the user

   - If there is a 3GPP AAA Server already serving the user, the HSS shall compare the 3GPP AAA Server name received in the request to the 3GPP AAA Server name stored in the HSS.

   - If they are not identical the HSS shall return the old 3GPP AAA Server to the requester 3GPP AAA Server and return an error by setting the Experimental-Result-Code to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

     The requester 3GPP AAA Server, upon detection of a 3GPP AAA Server name in the response assumes that the user already has a 3GPP AAA Server assigned, so makes use of Diameter redirect function to indicate the 3GPP AAA Server name where to address the Non-3GPP IP Access Registration request.

   - If they are identical but there is no APN configuration information in HSS for the user, the HSS shall return the Experimental Result Code DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION and it shall remove the 3GPP AAA Server name previously assigned for this subscriber.

   - If there is not a 3GPP AAA Server already serving the user, the HSS shall return an error, setting the Result-Code to DIAMETER_UNABLE_TO_COMPLY in the Response command.

3. After the HSS has determined that the requesting 3GPP AAA server is identical to the registered 3GPP AAA server, the HSS shall check the Server Assignment Type value received in the request:

   - If it indicates REGISTRATION, the HSS shall set the subscribers User Status to REGISTERED for the authenticated and authorized trusted or untrusted non-3GPP IP access subscriber, download the relevant user profile information and set the Result-Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command. For those APNs that have been authorized as a consequence of having the Wildcard APN in the user subscription, the HSS shall include the specific APN name and associated PDN-GW identity inside the Specific-APN-Info AVP of the Wildcard APN.

   - If it indicates USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / AUTHENTICATION_FAILURE / AUTHENTICATION_TIMEOUT, the HSS shall remove the 3GPP AAA Server name previously assigned for the subscriber, set the User Status for the subscriber to NOT_REGISTERED and set the Result-Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command. The HSS shall not remove the stored dynamic PGW-ID and APN information for the subscriber.

   - If it indicates AAA_USER_DATA_REQUEST, the HSS shall download the relevant user profile information to the requester 3GPP AAA Server and set the Result-Code AVP to DIAMETER_SUCCESS in the Response command.

   - If it indicates PGW_UPDATE, the HSS shall check if the subscriber is registered.

     If the subscriber is registered and the Emergency-Services AVP is present in the request, with the Emergency-Indication bit set, the HSS shall store the PDN GW Identity as the PDN GW used to establish emergency PDN connections by the non-3GPP access network, and update the MME with this information as specified in 3GPP TS 29.272 [29].

     If the subscriber is registered and the Emergency-Indication bit of the Emergency-Services AVP is not set in the request, and there is not a static PDN GW subscribed, the HSS shall store the PGW identity and PLMN (if it is received in the command) for the non-3GPP user and the APN identified by the APN Id or by the Context Identifier if present in the request; otherwise, the HSS shall not update or delete the stored PDN GW and, for this case, shall set the result code to DIAMETER_UNABLE_TO_COMPLY.

   If the APN corresponding to the PGW identity is not present in the subscription but the wild card APN is present in the subscription, the HSS shall store the new PDN GW identity and PLMN for an APN if present in the request. The HSS shall set the Result-Code AVP to DIAMETER_SUCCESS in the Server-Assignment-Response command. If the Context Identifier is included in the request, the HSS may use it to locate the APN Configuration.

   If the APN corresponding to the PGW identity is not present in the subscription and the wild card APN is not present in the subscription, the HSS shall reject the request and set the Result-Code AVP to DIAMETER_UNABLE_TO_COMPLY.

   If the subscriber is not registered, the HSS shall reject the request and set the Experimental-Result-Code AVP to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

   - If it indicates any other value, the Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY, and no registration/de-registration or profile download procedure shall be performed.

Origin-Host AVP shall contain the 3GPP AAA Server identity.

If the subscription data received for a certain APN indicates that the APN was authorized as a consequence of having the Wildcard APN in the user subscription in HSS, then the 3GPP AAA Server shall not store this APN data beyond the lifetime of the UE sessions related to the specific APN and the 3GPP AAA Server shall delete them upon disconnection of the UE. If the PGW Identity contains an FQDN of the PDN GW, the 3GPP AAA Server shall retrieve the PGW PLMN ID from the MIP-Home-Agent-Host AVP within the MIP6-Agent-Info AVP which contains the PGW Identity.

For trusted WLAN access, if the transparent single-connection mode is used as specified in 3GPP TS 24.302 [26], the 3GPP AAA Server may be configured by local policy to not update the HSS with the PGW Identity used over TWAN for the default APN of the user (i.e. to skip the Non-3GPP IP Access Registration request with Server-Assignment-Type set to "PGW_UPDATE").

NOTE: This 3GPP AAA Server option can be used when the same APN is configured for TWAN and other access technologies in which case the network can select different PDN GWs for PDN connections to this APN. Updating the HSS with the selected PDN GW identity for Trusted WLAN access could affect PDN connections over other access technologies.

8.1.2.2.3 Network Initiated De-Registration by HSS, Administrative

8.1.2.2.3.1 General

This procedure is used between the 3GPP AAA Server and the HSS to remove a previous registration and all associated state. When the de-registration procedure is initiated by HSS, indicating that a subscription has to be removed, the 3GPP AAA Server subsequently triggers the detach procedure via the appropriate interface.

Table 8.3.2.3: Network Initiated Deregistration by HSS request

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Reason for de-registration	Deregistration-Reason	M	This IE shall contain the reason for the de-registration as the HSS shall send to the 3GPP AAA server a reason for the de-registration. The de-registration reason shall be composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [24]) that determines the behaviour of the 3GPP AAA Server.
Routing Information	Destination-Host	M	This IE shall contain the 3GPP AAA server name that is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server,
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.3.2.4: Network Initiated Deregistration by HSS response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the Result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

8.1.2.2.3.2 Detailed behaviour

The HSS shall de-register the affected identity and invoke this procedure to inform the 3GPP AAA server to remove the subscribed user from the 3GPP AAA Server.

The HSS shall send in the Deregistration-Reason AVP the reason for the de-registration, composed by a textual message (if available) aimed for the user and a reason code that determines the action the 3GPP AAA server has to perform. The possible reason codes are:

- PERMANENT_TERMINATION: The non-3gpp subscription or service profile(s) has been permanently terminated or the Core Network Restrictions do not allow access to EPC anymore. The HSS shall clear the user's 3GPP AAA Server name and set the User Status to NOT_REGISTERED. The 3GPP AAA Server should start the network initiated de-registration towards the user.

- NEW_SERVER_ASSIGNED: The HSS indicates to the 3GPP AAA Server that a new 3GPP AAA Server has been allocated to the user (e.g. because the previous assigned 3GPP AAA Server was found unavailable at a certain point). The 3GPP AAA Server shall remove all user data and session information for the user indicated in the de-registration request. The 3GPP AAA Server shall not start the network initiated de-registration towards the user.

8.1.2.3 HSS Initiated Update of User Profile

8.1.2.3.1 General

According to the requirements described in 3GPP TS 23.402 [3], 3GPP TS 32.422 [32] and 3GPP TS 23.380 [52], SWx reference point shall enable:

- Indication to 3GPP AAA Server of change of non-3GPP subscriber profile within HSS;

- Activation and deactivation of the subscriber and equipment trace in the PDN GW.

- Request of identity and location information of the access network and/or UE local time zone.

- Indication to the 3GPP AAA Server that the HSS-based P-CSCF restoration procedure for WLAN, shall be executed as described in 3GPP TS 23.380 [52] clause 5.6.

This procedure is used between the 3GPP AAA Server and the HSS. The procedure is invoked by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server. This may happen due to a modification in the HSS.

The procedure is also invoked by the HSS to update the 3GPP AAA Server with

- the identity of a dynamically allocated PDN GW which is included in the APN-Configuration AVP in the User Profile as a result of the first PDN connection establishment associated with an APN over 3GPP access; or

- the identity of a dynamically allocated PGN GW for emergency services as a result of the establishment of an emergency PDN connection in E-UTRAN.

This procedure is mapped to the Diameter command codes Push-Profile-Request (PPR) and Push-Profile-Answer (PPA) specified in the 3GPP TS 29.229 [24]. Information element contents for these messages are shown in tables 8.1.2.3.1/1 and 8.1.2.3.1/2.

Table 8.1.2.3.1/1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
User profile	Non-3GPP-User-Data	M	This IE shall contain the updated user profile. Clause 8.2.3.1 details the contents of the AVP. In case of trace activation or deactivation, the Trace-Info AVP shall be included, and this may be the only AVP that is present under this grouped AVP.
Routing Information	Destination-Host	M	This IE shall contain the 3GPP AAA Server name that is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server
PPR Flags	PPR-Flags	O	This Information Element contains a bit mask. See 8.2.3.17 for the meaning of the bits.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.1.2.3.1/2: User Profile Update response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Access Network Information	Access-Network-Info	O	If present, this IE shall contain the identity and location information of the access network where the UE is attached.
Local Time Zone	Local-Time-Zone	O	If present, this IE shall contain the time zone of the location in the access network where the UE is attached.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

8.1.2.3.2 HSS Detailed behaviour

The HSS shall make use of this procedure to update the relevant user profile in the 3GPP AAA server (e.g. change of subscription data or change of the identity of a dynamically allocated PDN GW associated with an APN), or activate / deactivate subscriber and equipment trace in the PDN GW.

The HSS shall make use of this procedure to request the identity, location information and UE local time zone of the access network where the UE is currently attached. In this case, the HSS shall set the Access-Network-Info-Request and/or the UE-Local-Time-Zone-Request bits in the PPR-Flags AVP; if the HSS sends this command for the only purpose of requesting access network information or the local time zone of the UE (i.e., the user profile is not actually modified), the Non-3GPP-User-Data shall be included in the command as an empty AVP. The HSS shall only invoke this procedure if the 3GPP AAA Server has indicated support for the corresponding feature (see clause 8.2.3.16).

The HSS shall make use of this procedure to request to the 3GPP AAA Server the execution of the HSS-based P-CSCF restoration procedure, as described in 3GPP TS 23.380 [52] clause 5.4 if the 3GPP AAA Server indicated the support of this procedure in an earlier command to the HSS. In this case, the HSS shall set the "P-CSCF Restoration Request" bit in the PPR Flags and the procedure shall only be used for the purpose of the P-CSCF restoration for WLAN; then, the Non-3GPP-User-Data AVP shall be included as an empty AVP. .

The HSS shall make use of this procedure to update the identity of a dynamically allocated PDN GW for emergency services in the 3GPP AAA server, if the 3GPP AAA Server indicated the support of the Emergency Services Continuity feature in an earlier command to the HSS.

8.1.2.3.3 3GPP AAA Server Detailed behaviour

When the HSS-initiated user profile update procedure is successful, the 3GPP AAA Server shall overwrite entirely, for the subscriber identity indicated in the request, the currently stored user profile data with the information received from the HSS, if at least one APN-Configuration AVP is included in the Non-3GPP-User-Data AVP received from HSS. If no APN-Configurations are included in the Non-3GPP-User-Data AVP, the 3GPP AAA Server shall only update the currently stored user profile data with the new received data from the HSS.

If the HSS-initiated user profile update procedure is not successful, the 3GPP AAA Server shall not modify the stored user profile.

After a successful user profile download, the 3GPP AAA Server shall initiate re-authentication procedure as described in clause 7.2.2.4 if the subscriber has previously been authenticated and authorized to untrusted non-3GPP access. If the subscriber has previously been authenticated and authorized to trusted non-3GPP IP Access then the 3GPP AAA Server shall initiate a re-authorization procedure as described in clause 5.1.2.3.

As multiple authorization sessions may exist for the user (see clause 7.1.2.1), the 3GPP AAA Server shall examine the need to execute re-authorization for each of these sessions, and may execute the multiple re-authorization procedures in parallel. In case the user's non-3GPP subscription has been deleted or the user's APN has been barred, the re-authorization shall be executed in all ongoing user related authorization sessions. Otherwise, the re-authorization procedure shall be invoked for the authorization sessions for which at least one of the following conditions is fulfilled:

- The user's subscribed APN has been deleted from the HSS.
- The APN configuration data has been previously downloaded to the ePDG and the new version of APN configuration received from HSS reflects a modification in these data.

Following a successful download of subscription and equipment trace data, the 3GPP AAA Server shall forward the trace data by initiating reauthorization towards all PDN GWs that have an active authorization session.

When the UE is attached to a Trusted WLAN, if the HSS has invoked the User Profile Update procedure by setting the Access-Network-Info-Request and/or UE-Local-Time-Zone-Request bits in the PPR-Flags, the 3GPP AAA Server shall initiate a re-authorization procedure towards the TWAN by setting the Re-Auth–Request-Type to AUTHORIZE_ONLY; the TWAN shall send the identification, location information of the Access Point where the UE is attached and the local time zone of the UE, in the subsequent authorization request (AAR command) that follows the re-authorization request/answer exchange (RAR/RAA). If the 3GPP AAA Server determines that the UE is not currently attached to a Trusted WLAN, it shall not initiate any re-authorization procedure towards the access network, and it shall not include any network access information or UE local time zone in the response to the HSS.

NOTE: The 3GPP AAA Server cannot answer the Push Profile Request received from the HSS until the AAR command has ben received from the TWAN, since it needs to receive the information from the access network, before sending back the Push Profile Answer to the HSS.

If the 3GPP AAA Server receives the Push-Profile-Request command with an empty Non-3GPP-User-Data AVP, but some other action is indicated by setting any of the bits in the PPR-Flags AVP, the 3GPP AAA Server shall ignore the Non-3GPP-User-Data AVP, i.e., it shall not apply any changes to the stored user profile.

When the PPR Flags are received with the "P-CSCF Restoration Request" bit set, if an IMS PDN connection is established via a trusted or untrusted WLAN access for which the PGW has indicated the support of the P-CSCF restoration feature in an earlier command, the 3GPP AAA Server shall execute the HSS-based P-CSCF restoration for WLAN procedure, as described in 3GPP TS 23.380 [52] clause 5.6. Otherwise, the 3GPP AAA Server does not execute the HSS-based P-CSCF restoration for WLAN procedure.

Table 8.1.2.3.3/1 details the valid result codes that the 3GPP AAA Server can return in the response.

Table 8.1.2.3.3/1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in 3GPP AAA Server.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

8.1.2.4 Fault Recovery Procedures

8.1.2.4.1 HSS Reset Indication

8.1.2.4.1.1 General

This procedure is used by the HSS to indicate to the 3GPP AAA Server that it has restarted, and the registration data and the dynamic data stored for a set of users may have been lost.

This procedure is mapped to the Diameter command codes Push-Profile-Request (PPR) and Push-Profile-Answer (PPA) specified in the 3GPP TS 29.229 [24]. Information Element contents for these messages are shown in tables 8.1.2.4.1.1/1 and 8.1.2.4.1.1/2.

Table 8.1.2.4.1.1/1: HSS Reset Indication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
User List	User-Name (See IETF RFC 6733 [58])	M	This information element shall indicate the users affected by the HSS restart. It shall contain either: - The string "*", if all users are affected by the restart - The leading digits of the IMSI series of the set of users affected by the restart.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.
PPR Flags	PPR-Flags	M	This Information Element contains a bit mask. See 8.2.3.17 for the meaning of the bits. The HSS shall set the Reset-Indication bit when sending PPR to the 3GPP AAA Server.

Table 8.1.2.4.1.1/2: HSS Reset Indication Response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

8.1.2.4.1.2 HSS Detailed behaviour

The HSS shall use this procedure to indicate to the 3GPP AAA Server about a restart event, affecting a set of users, for whom their registration data and dynamic data may have been lost. The HSS shall only send this command if the 3GPP AAA Server has indicated support for the "HSS Restoration" feature. In this case, the HSS shall set the Reset-Indication bit in the PPR-Flags AVP in the PPR command.

NOTE: If there are multiple 3GPP AAA Servers deployed in the HPLMN, and the HSS is configured (in an implementation-specific manner) in such a way that it can determine that a certain 3GPP AAA Server does not contain any of the users affected by the restart, it can skip sending the PPR command to that specific 3GPP AAA Server.

8.1.2.4.1.3 3GPP AAA Server Detailed behaviour

If the 3GPP AAA Server supports the "HSS Restoration" feature, it shall answer with a successful result to the PPR command, and it shall mark those users affected by the HSS restart as "pending to be restored in HSS".

The 3GPP AAA Server shall use the HSS Identity received in the Origin-Host AVP (by comparing it with the value stored after a successful MAA command) and may make use of the received "User List" Information Element in order to determine which subscriber records are impacted, if any. If the 3GPP AAA Server determines that there are no subscribers affected by the HSS restart, it shall answer with a successful result to the HSS.

8.1.2.4.2 HSS Restoration

8.1.2.4.2.1 General

This procedure is used by the 3GPP AAA Server to restore in the HSS the registration data and the dynamic data for a certain user. The 3GPP AAA Sever shall use this procedure only after having received a previous indication from HSS of a restart event affecting that user.

This procedure is mapped to the Diameter command codes Server-Assignment-Request (SAR) and Server-Assignment-Answer (SAA) specified in the 3GPP TS 29.229 [24]. Information element contents for these messages are shown in tables 8.1.2.4.2.1/1 and 8.1.2.4.2.1/2.

Table 8.1.2.4.2.1/1: HSS Restoration Request

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the IMSI of the user, for whom the registration data and dynamic data is being restored in HSS, and it shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Server Assignment Type	Server-Assignment-Type	M	This IE shall contain the value "RESTORATION".
Active APN	Active-APN	C	This Information Element, if present, contains the list of active APNs stored by the 3GPP AAA Server for this user, including the identity of the PDN GW assigned to each APN. For the explicitly subscribed APNs, the following information shall be present: - Context-Identifier: context id of subscribed APN in use - Service-Selection: name of subscribed APN in use - MIP6-Agent-Info: including PDN GW identity in use for subscribed APN - Visited-Network-Identifier: identifies the PLMN where the PDN GW was allocated For the Wildcard APN, the following information shall be present: - Context-Identifier: context id of the Wildcard APN - Specific-APN-Info: list of APN-in use and related PDN GW identity when the subscribed APN is the wildcard APN
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

Table 8.1.2.4.2.1/2: HSS Restoration Response

Information element name	Mapping to Diameter AVP	Cat.	Description
IMSI	User-Name (See IETF RFC 6733 [58])	M	This information element shall contain the user IMSI and shall be formatted according to 3GPP TS 23.003 [14], clause 2.2.
Registration result	Result-Code / Experimental-Result	M	This IE contains the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host.

8.1.2.4.2.2 HSS Detailed behaviour

Upon receipt of the SAR command, if the HSS supports the "HSS Restoration" feature, and the user's IMSI is known, the HSS shall update the registration data (from the Origin-Host AVP received in the 3GPP AAA Server command) and dynamic data of the user (included in the "Active APN" Information Element), and answer with a successful result.

8.1.2.4.2.3 3GPP AAA Server Detailed behaviour

The 3GPP AAA Server shall use this command to update the HSS with the registration data and dynamic data it has for a user affected by the HSS restart, identified by the "User List" IE received previously in the PPR command, and marked in the 3GPP AAA Server as "pending to be restored in HSS". The 3GPP AAA Server shall only make use of this procedure in the HSS has indicated support for the "HSS Restoration" feature.

The 3GPP AAA Server shall invoke the SAR command towards the HSS, after having received further interactions over other reference points (S6b, STa, SWm …) for a user marked as "pending to be restored in HSS".

Once the 3GPP AAA Server receives confirmation from HSS, in the SAA command, that the user has been successfully restored in the HSS, via the "HSS Restoration Response" command, it shall clear the "pending to be restored in HSS" flag for that user.

8.2 Protocol Specification

8.2.1 General

The SWx reference point shall be Diameter based. This is defined as an IETF vendor specific Diameter application, where the Vendor ID is 3GPP. The Application Id used shall be 16777265.

8.2.2 Commands

8.2.2.1 Authentication Procedure

The Multimedia-Authentication-Request (MAR) command, indicated by the Command-Code field set to 303 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the HSS in order to request security information. This corresponds to clause 8.1.2.1.

Message Format

```
< Multimedia-Auth-Request > ::= < Diameter Header: 303, REQ, PXY, 16777265 >
                                < Session-Id >
                                [ DRMP ]
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                [ Destination-Host ]
                                { User-Name }
                                [ RAT-Type ]
                                [ ANID ]
                                [ Visited-Network-Identifier]
                                [ Terminal-Information ]
                                { SIP-Auth-Data-Item }
                                { SIP-Number-Auth-Items }
                                [AAA-Failure-Indication ]
                                [ OC-Supported-Features ]
                                *[ Supported-Features ]
                                …
                                *[ AVP ]
```

The Multimedia-Authentication-Answer (MAA) command, indicated by the Command-Code field set to 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Authentication-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in clause 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in IETF RFC 6733 [58].

Message Format

```
< Multimedia-Auth-Answer > ::= < Diameter Header: 303, PXY, 16777265 >
                               < Session-Id >
                               [ DRMP ]
                               { Vendor-Specific-Application-Id }
                               [ Result-Code ]
                               [ Experimental-Result ]
                               { Auth-Session-State }
                               { Origin-Host }
                               { Origin-Realm }
                               { User-Name}
                               [ SIP-Number-Auth-Items ]
                               *[ SIP-Auth-Data-Item ]
                               [ 3GPP-AAA-Server-Name ]
                               [ OC-Supported-Features ]
                               [ OC-OLR ] ]
                               *[ Load ]
                               *[ Supported-Features ]
                               …
                               *[ AVP ]
```

NOTE: As the Diameter commands described in this specification have been defined based on the former specification of the Diameter base protocol, the Vendor-Specific-Application-Id AVP is still listed as a required AVP (an AVP indicated as {AVP}) in the command code format specifications defined in this specification to avoid backward compatibility issues, even if the use of this AVP has been deprecated in the new specification of the Diameter base protocol (IETF RFC 6733 [58]).

8.2.2.2 HSS Initiated Update of User Profile Procedure

The Push-Profile-Request (PPR) command, indicated by the Command-Code field set to 305 and the 'R' bit set in the Command Flags field, is sent by the HSS to the 3GPP AAA Server in order to update the subscription data whenever a modification has occurred in the subscription data; this corresponds to clause 8.1.2.3. This command is also sent by HSS to indicate a restart event to the 3GPP AAA Server, so the registration data and the dynamic data previously stored in HSS can be restored; this corresponds to clause 8.1.2.4.1.

Message Format

```
< Push-Profile-Request > ::=  < Diameter Header: 305, REQ, 16777265 >
                              < Session-Id >
                              [ DRMP ]
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }
                              { Origin-Host }
                              { Origin-Realm }
                              { Destination-Host }
                              { Destination-Realm }
                              { User-Name }
                              [ Non-3GPP-User-Data ]
                              [ PPR-Flags ]
                              *[ Supported-Features ]
                              …
                              *[ AVP ]
```

The Push-Profile-Answer (PPA) command, indicated by the Command-Code field set to 305 and the 'R' bit cleared in the Command Flags field, is sent by the HSS in response to the Push-Profile-Request command. The Result-Code or

Experimental-Result AVP may contain one of the values defined in clause 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in IETF RFC 6733 [58].

Message Format

```
< Push-Profile-Answer > ::=     < Diameter Header: 305, PXY, 16777265 >
                                < Session-Id >
                                [ DRMP ]
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                [ Access-Network-Info ]
                                [ Local-Time-Zone ]
                                *[ Supported-Features ]
                                …
                                *[ AVP ]
```

NOTE: As the Diameter commands described in this specification have been defined based on the former specification of the Diameter base protocol, the Vendor-Specific-Application-Id AVP is still listed as a required AVP (an AVP indicated as {AVP}) in the command code format specifications defined in this specification to avoid backward compatibility issues, even if the use of this AVP has been deprecated in the new specification of the Diameter base protocol (IETF RFC 6733 [58]).

8.2.2.3 Non-3GPP IP Access Registration Procedure

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to 301 and the 'R' bit set in the Command Flags field, is sent by the 3GPP AAA Server to the HSS; this corresponds to clause 8.1.2.2.2. This command is also sent by the 3GPP AAA Server to restore the registration data and the dynamic data previously stored in HSS, which may have been lost after a restart; this corresponds to clause 8.1.2.4.2.

Message Format

```
< Server-Assignment-Request > ::=     < Diameter Header: 301, REQ, PXY, 16777265 >
                                      < Session-Id >
                                      [ DRMP ]
                                      { Vendor-Specific-Application-Id }
                                      { Auth-Session-State }
                                      { Origin-Host }
                                      { Origin-Realm }
                                      [ Destination-Host ]
                                      { Destination-Realm }
                                      [ Service-Selection ]
                                      [ Context-Identifier ]
                                      [ MIP6-Agent-Info ]
                                      [ Visited-Network-Identifier ]
                                      { User-Name}
                                      { Server-Assignment-Type }
                                      *[ Active-APN ]
                                      [ OC-Supported-Features ]
                                      *[ Supported-Features ]
                                      [ Terminal-Information ]
                                      [ Emergency-Services ]
                                      …
                                      *[ AVP ]
```

The Server-Assignment-Answer (SAA) command, indicated by the Command-Code field set to 301 and the 'R' bit cleared in the Command Flags field, is sent by the HSS to the 3GPP AAA Server to confirm the registration, de-registration, user profile download or restoration procedure. The Result-Code or Experimental-Result AVP may

contain one of the values defined in clause 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in IETF RFC 6733 [58].

Message Format

```
< Server-Assignment-Answer > ::=< Diameter Header: 301, PXY, 16777265 >
                                 < Session-Id >
                                 [ DRMP ]
                                 { Vendor-Specific-Application-Id }
                                 [ Result-Code ]
                                 [ Experimental-Result ]
                                 { Auth-Session-State }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 { User-Name}
                                 [ Non-3GPP-User-Data ]
                                 [ 3GPP-AAA-Server-Name ]
                                 [ OC-Supported-Features ]
                                 [ OC-OLR ] ]
                                 *[ Load ]
                                 *[ Supported-Features ]
                                 …
                                 *[ AVP ]
```

NOTE: As the Diameter commands described in this specification have been defined based on the former specification of the Diameter base protocol, the Vendor-Specific-Application-Id AVP is still listed as a required AVP (an AVP indicated as {AVP}) in the command code format specifications defined in this specification to avoid backward compatibility issues, even if the use of this AVP has been deprecated in the new specification of the Diameter base protocol (IETF RFC 6733 [58]).

8.2.2.4 Network Initiated De-Registration by HSS Procedure

The Registration-Termination-Request (RTR) command, indicated by the Command-Code field set to 304 and the "R" bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to request the de-registration of a user. This corresponds to clause 8.1.2.2.3.

Message Format

```
<Registration-Termination-Request> ::=  < Diameter Header: 304, REQ, PXY, 16777265 >
                                        < Session-Id >
                                        [ DRMP ]
                                        { Vendor-Specific-Application-Id }
                                        { Auth-Session-State }
                                        { Origin-Host }
                                        { Origin-Realm }
                                        { Destination-Host }
                                        { Destination-Realm }
                                        { User-Name }
                                        { Deregistration-Reason }
                                        *[ Supported-Features ]
                                        …
                                        *[ AVP ]
```

The Registration-Termination-Answer (RTA) command, indicated by the Command-Code field set to 304 and the "R" bit cleared in the Command Flags field, is sent by a client in response to the Registration-Termination-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in clause 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in IETF RFC 6733 [58].

Message Format

```
<Registration-Termination-Answer> ::=  < Diameter Header: 304, PXY, 16777265 >
                                       < Session-Id >
                                       [ DRMP ]
```

{ Vendor-Specific-Application-Id }
[Result-Code]
[Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[Supported-Features]
…
*[AVP]

NOTE: As the Diameter commands described in this specification have been defined based on the former specification of the Diameter base protocol, the Vendor-Specific-Application-Id AVP is still listed as a required AVP (an AVP indicated as {AVP}) in the command code format specifications defined in this specification to avoid backward compatibility issues, even if the use of this AVP has been deprecated in the new specification of the Diameter base protocol (IETF RFC 6733 [58]).

8.2.3 Information Elements

8.2.3.0 General

The following table describes the Diameter AVPs defined for the SWx interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

Table 8.2.3.0/1: Diameter SWx AVPs

				AVP Flag rules			
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**
Non-3GPP-User-Data	1500	8.2.3.1	Grouped	M,V			P
Non-3GPP-IP-Access	1501	8.2.3.3	Enumerated	M,V			P
Non-3GPP-IP-Access-APN	1502	8.2.3.4	Enumerated	M,V			P
ANID	1504	5.2.3.7	UTF8String	M,V			P
Trace-Info	1505	8.2.3.13	Grouped	V			M,P
PPR-Flags	1508	8.2.3.17	Unsigned32	V			M,P
TWAN-Default-APN-Context-Id	1512	8.2.3.18	Unsigned32	V			M,P
TWAN-Access-Info	1510	8.2.3.19	Grouped	V			M,P
Access-Authorization-Flags	1511	8.2.3.20	Unsigned32	V			M,P
WLAN-Identifier	1509	5.2.3.18	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
AAA-Failure-Indication	1518	8.2.3.21	Unsigned32	V			M,P
Access-Network-Info	1524	5.2.3.24	Grouped	V			M,P
3GPP-AAA-Server-Name	318	8.2.3.24	DiameterIdentity	M, V			P
ERP-Authorization	1541	8.2.3.27	Unsigned32	V			M,P
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 ETF RFC 6733 [58]. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.							

The following table describes the Diameter AVPs re-used by the SWx interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use within SWx. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter base protocol (see IETF RFC 6733 [58]), do not need to be supported.

Table 8.2.3.0/2: SWx re-used Diameter AVPs

Attribute Name	Reference	Comments	M-bit
User-Name	ETF RFC 6733 [58]		
Session-Timeout	ETF RFC 6733 [58]		
Subscription-ID	IETF RFC 4006 [20]		
MIP6-Agent-Info	IETF RFC 5447 [6]		
MIP6-Feature-Vector	IETF RFC 5447 [6]		
Service-Selection	IETF RFC 5778 [11]		
3GPP-Charging-Characteristics	3GPP TS 29.061 [31]		
RAT-Type	3GPP TS 29.212 [23]		
Visited-Network-Identifier	3GPP TS 29.229 [24]		
SIP-Number-Auth-Items	3GPP TS 29.229 [24]		
SIP-Item-Number	3GPP TS 29.229 [24]		
SIP-Auth-Data-Item	3GPP TS 29.229 [24]		
SIP-Authentication-Scheme	3GPP TS 29.229 [24]		
SIP-Authenticate	3GPP TS 29.229 [24]		
SIP-Authorization	3GPP TS 29.229 [24]		
Confidentiality-Key	3GPP TS 29.229 [24]		
Integrity-Key	3GPP TS 29.229 [24]		
Server-Assignment-Type	3GPP TS 29.229 [24]		
Deregistration-Reason	3GPP TS 29.229 [24]		
Supported-Features	3GPP TS 29.229 [24]		
Feature-List-ID	3GPP TS 29.229 [24]		
Feature-List	3GPP TS 29.229 [24]		
APN-Configuration	3GPP TS 29.272 [29]		
Context-Identifier	3GPP TS 29.272 [29]		
Terminal-Information	3GPP TS 29.272 [29]		
AMBR	3GPP TS 29.272 [29]		
APN-OI-Replacement	3GPP TS 29.272 [29]		
Trace-Reference	3GPP TS 29.272 [29]		
Trace-Data	3GPP TS 29.272 [29]		
Active-APN	3GPP TS 29.272 [29]		
BSSID	3GPP TS 32.299 [30]		
Location-Information	IETF RFC 5580 [46]		
Location-Data	IETF RFC 5580 [46]		
Operator-Name	IETF RFC 5580 [46]		
Local-Time-Zone	3GPP TS 29.272 [29]		
OC-Supported-Features	IETF RFC 7683 [47]	See clause 8.2.3.22	Must not set
OC-OLR	IETF RFC 7683 [47]	See clause 8.2.3.23	Must not set
DRMP	IETF RFC 7944 [53]	See clause 8.2.3.25	Must not set
Emergency-Info	3GPP TS 29.272 [29]		
Load	IETF RFC 8583 [54]	See clause 8.2.3.26	Must not set
UE-Usage-Type	3GPP TS 29.272 [29]		
Core-Network-Restrictions	3GPP TS 29.272 [29]		

NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies.

NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.

Only those AVP initially defined in this reference point or AVP with values initially defined in this reference point and for this procedure are described in the following clauses.

8.2.3.1 Non-3GPP-User-Data

The Non-3GPP-User-Data AVP is of type Grouped. It contains the information related to the user profile relevant for EPS.

AVP format:

```
Non-3GPP-User-Data ::=  < AVP Header: 1500 10415 >
                            [ Subscription-ID ]
                            [ Non-3GPP-IP-Access ]
                            [ Non-3GPP-IP-Access-APN ]
                            *[ RAT-Type ]
                            [ Session-Timeout ]
                            [ MIP6-Feature-Vector ]
                            [ AMBR ]
                            [ 3GPP-Charging-Characteristics ]
                            [ Context-Identifier ]
                            [ APN-OI-Replacement ]
                            *[ APN-Configuration ]
                            [ Trace-Info ]
                            [ TWAN-Default-APN-Context-Id ]
                            *[ TWAN-Access-Info]
                            [ UE-Usage-Type ]
                            [ Emergency-Info ]
                            [ ERP-Authorization ]
                            [ Core-Network-Restrictions ]
                            *[ AVP ]
```

The Subscription-ID, if present in this grouped AVP, shall contain either an MSISDN (if this identity is present in the subscription), or an External Identifier (if the subscriber does not have an MSISDN identity but has an External Identifier in the subscription).

The AMBR included in this grouped AVP shall include the AMBR associated to the user's subscription (UE-AMBR).

The APN-OI-Replacement included in this grouped AVP shall include the UE level APN-OI-Replacement associated to the user's subscription. This APN-OI-Replacement has lower priority than APN level APN-OI-Replacement that is included in the APN-Configuration AVP.

The Non-3GPP-User-Data AVP shall only contain APN-Configuration AVP(s) configured in the user subscription with an IP PDN type.

The Context-Identifier in this grouped AVP shall identify the user's default APN configuration. The TWAN-Default-APN-Context-Id AVP identifies the default APN configuration for EPC access over Trusted WLAN. This AVP shall be present if the default APN configuration for EPC access over Trusted WLAN differs from the default APN configuration for 3GPP access and other non-3GPP accesses. This AVP may be present otherwise.

The RAT-Type AVP(s) shall include the access technology type(s) not allowed for the user as specified in clause 2.13.126 of 3GPP TS 23.008 [49].

The Emergency-Info AVP shall contain the identity of the PDN-GW used for the establishment of emergency PDN connections.

The MIP6-Feature-Vector may provide HSM and/or NBM authorization information (see clause 8.2.3.28).

For the conditions specified in clause 8.1.2.3.2, the Non-3GPP-User-Data AVP shall be empty, i.e. not include any AVP.

If the Non-3GPP-User-Data AVP is not empty, the Non-3GPP-IP-Acess AVP, the Non-3GPP-IP-Access-APN AVP, the Context-Identifier AVP and at least one item of the APN-Configuration AVP shall always be included, except when the Non-3GPP-User-Data AVP is used for downloading trace activation or deactivation information on the SWx interface, for an already registered user, or when the Non-3GPP-User-Data is used for downloading the Emergency-Info. In those specific cases, the Trace-Info AVP, or respectively the Emergency-Info AVP, shall be included and the presence of any further AVPs is optional.

8.2.3.2 Subscription-ID

The Subscription-ID AVP is of type Grouped and indicates the user identity to be used for charging purposes. It is defined in the IETF RFC 4006 [20]. EPC shall make use only of the MSISDN and External Identifier values.

When the identity to be conveyed is an MSISDN, the AVP Subscription-Id-Type shall be set to value "END_USER_E164".

When the identity to be conveyed is an External Identifier, the AVP Subscription-Id-Type shall be set to value "END_USER_NAI".

Then AVP Subscription-Id-Data, with type UTF8String, shall contain the identity of the user.

AVP format:

```
Subscription-Id ::=  < AVP Header: 443 >
                                [ Subscription-Id-Type ]
                                [ Subscription-Id-Data ]
```

8.2.3.3 Non-3GPP-IP-Access

The Non-3GPP-IP-Access AVP (AVP code 1501) is of type Enumerated, and allows operators to determine if the subscriber is barred from using the non-3GPP access network. The following values are defined:

NON_3GPP_SUBSCRIPTION_ALLOWED (0)

The subscriber has non-3GPP subscription and is authorized to use the non-3GPP access network.

NON_3GPP_SUBSCRIPTION_BARRED (1)

The subscriber is barred from using the non-3GPP access network.

8.2.3.4 Non-3GPP-IP-Access-APN

The Non-3GPP-IP-Access-APN AVP (AVP code 1502) is of type Enumerated, and allows operator to disable all APNs for a subscriber at one time. The following values are defined:

Non_3GPP_APNS_ENABLE (0)

Enable all APNs for a subscriber.

Non_3GPP_APNS_DISABLE (1)

Disable all APNs for a subscriber

8.2.3.5 RAT-Type

The RAT-Type AVP (AVP code 1032) is of type Enumerated. The encoding of the AVP is specified in 3GPP TS 29.212 [23].

8.2.3.6 Session-Timeout

The Session-Timeout AVP is of type Unsigned32. It is defined in IETF RFC 6733 [58] and indicates the maximum period for a session measured in seconds. This AVP is used for re-authentication purposes. If this field is not used, the non-3GPP Access Node will apply default time intervals.

8.2.3.7 APN-Configuration

The APN-Configuration AVP is of type Grouped AVP and is defined in 3GPP TS 29.272 [29].

The following AVPs defined in the APN-Configuration AVP in 3GPP TS 29.272 [29] are not applicable to Non-3GPP accesses and therefore need not be included in the APN-Configuration AVP over the SWx, SWd, SWm, STa and S6b reference points:

- LIPA-Permission AVP
- Restoration-Priority AVP
- SIPTO-Local-Network-Permission AVP
- WLAN-offloadability AVP
- Non-IP-PDN-Type-Indicator AVP
- Non-IP-Data-Delivery-Mechanism AVP
- SCEF-ID AVP
- SCEF-Realm AVP
- Preferred-Data-Mode AVP

8.2.3.8 ANID

The ANID AVP is defined in clause 5.2.3.7.

8.2.3.9 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is defined in 3GPP TS 29.229 [24]. The optional AVPs that are needed in SWx reference point are included in the ABNF representation below.

AVP format:

```
SIP-Auth-Data-Item ::= < AVP Header: 612 10415 >
                       [ SIP-Item-Number ]
                       [ SIP-Authentication-Scheme ]
                       [ SIP-Authenticate ]
                       [ SIP-Authorization ]
                       [ Confidentiality-Key ]
                       [ Integrity-Key ]
                       *[ AVP ]
```

8.2.3.10 Confidentiality-Key

The Confidentiality-Key AVP is defined in 3GPP TS 29.229 [24]. It is of type OctetString, and contains the Confidentiality Key (CK') or, after key derivation using the Access Network Identifier, the Confidentiality Key (CK'). For the 3GPP AAA server it is transparent whether the value received corresponds to CK or CK'.

8.2.3.11 Integrity-Key

The Integrity-Key AVP is defined in 3GPP TS 29.229 [24]. It is of type OctetString, and contains the Integrity Key (IK) or, after key derivation using the Access Network Identifier, the Integrity Key (IK'). For the 3GPP AAA server it is transparent whether the value received corresponds to IK or IK'.

8.2.3.12 Server-Assignment-Type AVP

The Server-Assignment-Type AVP is defined in 3GPP TS 29.229 [24] and it is of type Enumerated, and indicates the type of server update being performed in a Server-Assignment-Request operation. As part of the SWx protocol specification, the following values are additionally defined:

AAA_USER_DATA_REQUEST (12)

This value is used to request the non-3GPP user profile data from the 3GPP AAA Server to the HSS.

PGW_UPDATE (13)

This value is used to store, update or delete the PDN-GW Identity in the HSS, as requested from the 3GPP AAA Server.

RESTORATION (14)

This value is used to store in the HSS registration data and dynamic data that may have been potentially lost after a restart event.

8.2.3.13 Trace-Info

The Trace-Info AVP is of type Grouped. This AVP shall contain the information related to subscriber and equipment trace function and the required action, i.e. activation of deactivation

AVP format

Trace-Info ::= < AVP header: 1505 10415>

[Trace-Data]

[Trace-Reference]

*[AVP]

Either the Trace-Data or the Trace-Reference AVP shall be included. When trace activation is needed, Trace-Data AVP shall be included, while the trace deactivation request shall be signalled by including the Trace-Reference directly under the Trace-Info. The Trace-Reference AVP is of type OctetString. The Diameter AVP is defined in 3GPP TS 29.272 [29].

8.2.3.14 Trace-Data

The Trace-Data AVP is of type Grouped. The Diameter AVP is defined in 3GPP TS 29.272 [29].

8.2.3.15 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the SWx application.

8.2.3.16 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the SWx application. The meaning of the bits shall be as defined in table 8.2.3.16/1.

Table 8.2.3.16/1: Features of Feature-List-ID 1 used in SWx

Feature bit	Feature	M/O	Description
0	HSS Restoration	O	HSS Restoration This feature is applicable for the MAR/MAA, PPR/PPA and SAR/SAA command pairs. If the 3GPP AAA Server does not indicate support for this feature in a former MAR or SAR command, the HSS shall not send a PPR command to indicate a restart event to the 3GPP AAA Server.
1	Access-Network-Information-Retrieval	O	Access Network Information Retrieval This feature is applicable for the MAR/MAA and PPR/PPA and SAR/SAA command pairs. If the 3GPP AAA Server does not indicate support for this feature in a former MAR or SAR command, the HSS shall not send a PPR command to request access network information from the 3GPP AAA Server.
2	UE Local Time Zone Retrieval	O	UE Local Time Zone Retrieval This feature is applicable for the MAR/MAA and PPR/PPA and SAR/SAA command pairs. If the 3GPP AAA Server does not indicate support for this feature in a former MAR or SAR command, the HSS shall not send a PPR command to request the local time zone of the UE from the 3GPP AAA Server.
3	P-CSCF Restoration for WLAN	O	Support of P-CSCF Restoration for WLAN This feature is applicable to the MAR/MAA and PPR/PPA and SAR/SAA command pairs over the SWx interface, when the 3GPP AAA Server supports the execution of the P-CSCF restoration procedures for WLAN as described in 3GPP TS 23.380 [52] clause 5.6. If the 3GPP AAA Server does not indicate support of this feature in a former MAR or SAR command, the HSS shall not send a PPR command requesting the execution of HSS-based P-CSCF restoration procedures for WLAN,
4	Emergency Services Continuity	O	Support of Emergency Services Continuity This feature is applicable to the PPR/PPA and SAR/SAA command pairs over the SWx interface, when the HSS and the 3GPP AAA Server support the continuity of emergency services upon mobility between 3GPP and WLAN accesses, as specified in clause 4.5.7.2 of 3GPP TS 23.402 [3]. If the 3GPP AAA Server does not indicate support of this feature in a former SAR command, the HSS shall not include the Emergency Info in a SAA command and shall not send a PPR command to update the Emergency Info. If the HSS does not indicate support of this feature in a former SAA command (e.g. during the registration of the non-3GPP user), the 3GPP AAA Server shall not send a SAR command to update the Emergency Info. If the HSS supports this feature on SWx, it shall also support the Emergency Service Continuity feature on S6a, see 3GPP TS 29.272 [29].
5	ERP	O	Support of EAP Reauthentication Protocol This feature is applicable to the MAR/MAA and PPR/PPA command pairs over the SWx interface. If the 3GPP AAA Server does not indicate support of this feature in a former MAR command, the HSS shall not include ERP authorization data in the subscription profile, and it shall not send subsequent PPR commands to update the ERP authorization status of this user. If the HSS does not indicate support of this feature in the MAA command, the 3GPP AAA Server shall not expect the reception of explicit authorization of ERP in the subscription profile, and may allow/disallow ERP for all subscribers, according to local policy.

6	Dedicated Core Networks	O	Support of Dedicated Core Networks This feature is applicable to the SAR/SAA and PPR/PPA command pairs over the SWx interface. If the 3GPP AAA Server does not indicate support of this feature in the SAR command, the HSS shall not send DCN-related subscription data (e.g., UE Usage Type) in SAA, and shall not send subsequent PPR commands when such subscription data are updated. If the 3GPP AAA Server does not indicate support of this feature in the PPA command and the HSS has already sent DCN-related subscription data in PPR, the HSS may store this indication and not send further updates related to DCN subscription data.
Feature bit: The order number of the bit within the Supported-Features AVP, e.g. "1". Feature: A short name that can be used to refer to the bit and to the feature. M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O"). Description: A clear textual description of the feature.			

Features that are not indicated in the Supported-Features AVPs within a given application message shall not be used to construct that message.

8.2.3.17 PPR-Flags

The PPR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.2.3.17/1:

Table 8.2.3.17/1: PPR-Flags

Bit	Name	Description
0	Reset-Indication	This bit, when set, indicates that the HSS has undergone a restart event and the registration data and dynamic data needs to be restored, if available at the 3GPP AAA Server.
1	Access-Network-Info-Request	This bit, when set, indicates that the HSS requests the 3GPP AAA Server the identity and location information of the access network where the UE is currently attached.
2	UE-Local-Time-Zone-Request	This bit, when set, indicates that the HSS requests the 3GPP AAA Server the time zone of the location in the access network where the UE is attached.
3	P-CSCF Restoration Request	This bit, when set, indicates to the 3GPP AAA Server that the HSS requests the execution of the HSS-based P-CSCF restoration procedures for WLAN, as described in 3GPP TS 23.380 [52] clause 5.6.
NOTE: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving 3GPP AAA Server.		

8.2.3.18 TWAN-Default-APN-Context-Id

The TWAN-Default-APN-Context-Id AVP is of the type Unsigned32 and shall identify the context identifier of the subscriber's default APN to be used for Trusted WLAN access to EPC over S2a.

Note: The default APN for Trusted WLAN access to EPC over S2a can differ from the default APN for 3GPP and other non-3GPP accesses.

8.2.3.19 TWAN-Access-Info

The TWAN-Access-Info AVP is of type Grouped.

If no WLAN-Identifier AVP is included in the TWAN-Access-Info AVP, the allowed access methods shall apply to any arbitrary Trusted WLAN. See clause 5.1.2.1.2.

If the Access-Authorization-Flags AVP is not present in the TWAN-Access-Info AVP, EPC access and Non-Seamless WLAN Offload shall be considered to be not allowed.

A specific Trusted-WLAN shall appear in at most one TWAN-Access-Info AVP.

There shall be at most one TWAN-Access-Info AVP not including any WLAN-Identifier.

AVP Format:

```
TWAN-Access-Info::=  < AVP Header: 1510 10415 >
                          [ Access-Authorization-Flags ]
                          [ WLAN-Identifier ]
                         *[ AVP ]
```

8.2.3.20 Access-Authorization-Flags

The Access-Authorization-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 8.2.3.20/1:

Table 8.2.3.20/1: Access-Authorization-Flags

Bit	Name	Description
0	EPC-Access-Authorization	This bit, when set, indicates that the UE is allowed to access the EPC when connected via Trusted WLAN access. This flag, when not set, indicates that the UE is not allowed to access EPC when connected via Trusted WLAN access.
1	NSWO-Access-Authorization	This bit, when set, indicates that the UE is allowed Non-Seamless WLAN Offload access via Trusted WLAN access. This flag, when not set, indicates that the UE is not allowed to Non-Seamless WLAN Offload via Trusted WLAN access.
NOTE: Bits not defined in this table shall be cleared by the sending HSS and discarded by the receiving 3GPP AAA Server.		

NOTE: UE is allowed to access the EPC when connected via Trusted WLAN access only if the Non-3GPP-IP-Access-APN AVP does not disable all APNs and the EPC-Access-Authorization bit is set.

8.2.3.21 AAA-Failure-Indication

The AAA-Failure-Indication AVP is of type Unsigned32 and it shall contain a bitmask. The meaning of the bits is defined in table 8.2.3.21/1:

Table 8.2.3.21/1: AAA-Failure-Indication

Bit	Name	Description
0	AAA Failure	This bit, when set, indicates that a previously assigned 3GPP AAA Server is unavailable.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the receiver.		

8.2.3.22 OC-Supported-Features

The OC-Supported-Features AVP is of type Grouped and it is defined in IETF RFC 7683 [47]. This AVP is used to support Diameter overload control mechanism, see Annex B for more information.

8.2.3.23 OC-OLR

The OC-OLR AVP is of type Grouped and it is defined in IETF RFC 7683 [47]. This AVP is used to support Diameter overload control mechanism, see Annex B for more information.

8.2.3.24 3GPP-AAA-Server-Name

The 3GPP-AAA-Server-Name AVP is of type DiameterIdentity, and defines the Diameter address of the 3GPP AAA Server node.

8.2.3.25 DRMP

The DRMP AVP is of type Enumerated and is defined in IETF RFC 7944 [53]. This AVP allows the 3GPP functional entities to indicate the relative priority of Diameter messages. The DRMP AVP may be used to set the DSCP marking for transport of the associated Diameter message.

8.2.3.26 Load

The Load AVP is of type Grouped and it is defined in IETF RFC 8583 [54]. This AVP is used to support Diameter load control mechanism, see Annex E for more information.

8.2.3.27 ERP-Authorization

The ERP-Authorization AVP is of type Unsigned32 and it indicates whether the subscriber is authorized, or not, to make use of the EAP Reauthentication Protocol. The following values are defined:

ERP_NOT_AUTHORIZED (0)

ERP_AUTHORIZED (1)

8.2.3.28 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP (AVP Code 124) is of type Unsigned64 and contains a 64 bit flags field of the mobile IP capabilities authorized by the HSS.

The following capabilities are defined for the SWx interface:

- MIP6_INTEGRATED (0x0000000000000001)
  This flag means that DSMIPv6 is authorized.

- PMIP6_SUPPORTED (0x0000010000000000)
  This flag means that NBM is authorized.

- MIP4_SUPPORTED (0x0000100000000000)
  This flag means that MIPv4 is authorized.

- GTPv2_SUPPORTED (0x0000400000000000)
  This flag means that NBM is authorized.

NBM shall be considered as authorized if at least one of the PMIP6_SUPPORTED and GTPv2_SUPPORTED flag is set.

NOTE: The selection of the protocol variant (GTPv2 or PMIPv6) on S2a/S2b is determined solely by the TWAN/ePDG. It does not matter whether the HSS sets the PMIP6_SUPPORTED and/or GTPv2_SUPPORTED flags to authorize NBM.

Based on operator policy, the 3GPP AAA Server may also authorize the use of NBM, irrespective of the presence or content of the MIP6-Feature-Vector AVP in the Non-3GPP User Data.

8.2.4 Session Handling

The Diameter protocol between the 3GPP AAA Server and the HSS shall not keep the session state and each Diameter request/response interaction shall be transported over a different diameter session which is implicitly terminated.

In order to indicate that session state shall not be maintained, the diameter client and server shall include the Auth-Session-State AVP set to the value NO_STATE_MAINTAINED (1), as described in IETF RFC 6733 [58]. As a consequence, the server shall not maintain any state information about this session and the client shall not send any

session termination request. Neither the Authorization-Lifetime AVP nor the Session-Timeout AVP shall be present in requests or responses.

8.3 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the 3GPP AAA server to find the identity of the HSS that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS or when a 3GPP AAA server is configured to use pre-defined HSS address/identity.

This User identity to HSS resolution mechanism may rely on routing capabilitites provided by Diameter and be implemented in the home operator network within dedicated Diameter Agents (Redirect Agents or Proxy Agents) responsible for determining the HSS identity based on the provided user identity. If this Diameter based implementation is selected by the Home network operator, the principles described below shall apply.

In networks where more than one independently addressable HSS are utilized by a network operator, and the 3GPP AAA server is not configured to use pre-defined HSS address/identity, each 3GPP AAA server shall be configured with the address/identity of the Diameter Agent (Redirect Agent or Proxy Agent) implementing this resolution mechanism.

To get the HSS identity that holds the subscriber data for a given user identity, the 3GPP AAA server shall send the Diameter request normally destined to the HSS to a pre-configured address/identity of a Diameter agent supporting the User identity to HSS resolution mechanism.

- If this Diameter request is received by a Diameter Redirect Agent, the Diameter Redirect Agent shall determine the HSS identity based on the provided user identity and sends to the 3GPP AAA server a notification of redirection towards the HSS identity, in response to the Diameter request. Multiple HSS identities may be included in the response from the Diameter Redirect Agent, as specified in IETF RFC 6733 [58]. In such a case, the 3GPP AAA server shall send the Diameter request to the first HSS identity in the ordered list received in the Diameter response from the Diameter Redirect Agent. If no successful response to the Diameter request is received, the 3GPP AAA server shall send a Diameter request to the next HSS identity in the ordered list. This procedure shall be repeated until a successful response from an HSS is received.

- If this Diameter request is received by a Diameter Proxy Agent, the Diameter Proxy Agent shall determine the HSS identity based on the provided user identity and - if the Diameter load control mechanism is supported (see IETF RFC 8583 [54]) - optionally also based on previously received load values from Load AVPs of type HOST. The Diameter Proxy Agent shall then forward the Diameter request directly to the determined HSS. The 3GPP AAA server shall determine the HSS identity from the response to the Diameter request received from the HSS.

After the User identity to HSS resolution, the 3GPP AAA server shall store the HSS identity/name/Realm and shall use it in further Diameter requests associated to the same user dentity.

NOTE: Alternatives to the user identity to HSS resolution Diameter based implementation are outside the scope of this specification.

9 S6b Description

9.1 Functionality

9.1.1 General

The S6b reference point is defined between the 3GPP AAA Server and the PDN-GW. The definition of the reference point and its functionality is given in 3GPP TS 23.402 [3].

When the UE attaches to the EPC using the S2c reference point, the S6b reference point is used to authenticate and authorize the UE, and update the PDN-GW address to the 3GPP AAA server and HSS.

When the UE attaches to the EPC using the S2a/S2b reference point in the PMIPv6 or GTPv2 mode, the S6b reference point is used to update the 3GPP AAA server or the 3GPP AAA proxy with the PDN-GW address information and with

the selected S2a/S2b protocol variant. Furthermore, this reference point may be used to retrieve and update other mobility related parameters including static QoS profiles for non-3GPP accesses.

The S6b reference point is also used to authenticate and authorize the incoming MIPv4 Registration Request in the case the UE attaches to the EPC over the S2a reference point using MIPv4 FACoA procedures.

The S6b reference point is used by the 3GPP AAA Server in the case the UE attaches to the EPC using the S2c reference point to indicate to the PDN GW that a PDN GW reallocation shall be performed. This indication triggers the actual Home Agent reallocation procedure as specified in 3GPP TS 24.303 [13].

The S6b reference point is also used to download subscriber and equipment trace information to the PDN GW.

The S6b reference point is also used by the 3GPP AAA Server to indicate to the PDN GW that the HSS-based P-CSCF restoration procedure for WLAN shall be executed as described in 3GPP TS 23.380 [52] clause 5.6.

9.1.2 Procedures Description

9.1.2.1 Authentication and Authorization Procedures when using DSMIPv6

9.1.2.1.1 General

The S6b interface shall enable the authentication and authorization between the UE and the 3GPP AAA Server/Proxy for DSMIPv6.

When an UE performs the DSMIPv6 initial attach, it runs an IKEv2 exchange with the PDN GW as specified in 3GPP TS 24.303 [13]. In this exchange EAP AKA is used for UE authentication over IKEv2. The PDN GW acts as an IKEv2 responder and an EAP pass-through authenticator for this authentication.

The S6b authentication and authorization procedure is invoked by the PDN GW after receiving an IKE_SA_AUTH message from the UE. The S6b reference point performs authentication based on reuse of the DER/DEA command set defined in Diameter EAP. The exact procedure follows the steps specified in IETF RFC 5778 [11].

NOTE: This procedure is only used with DSMIPv6-capable UEs; therefore, only PDNs with PDN Types IPv6 or IPv4v6 are accessible in this case.

Table 9.1.2.1/1: Authentication and Authorization Request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User identity	User-Name	M	This information element shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE shall be used in this case.
EAP Payload	EAP-Payload	M	This IE shall contain the Encapsulated payload for UE – 3GPP AAA Server mutual authentication
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity does not contain an FQDN.
Access Type	RAT-Type	C	This Information Element shall contain the non-3GPP access network technology type that is serving the UE. This IE shall be present if it is available when the PDN GW sends the request.
PDN GW Identity	MIP6 -Agent-Info	M	This IE shall contain the FQDN and/or IPv6 address(es) of the PDN GW that the user shall be connected to. If the PDN GW includes the IP address in the PDN GW Identity, it shall include the HA IPv6 address and, if used, the IPv4 address, as DSMIPv6 is used.
MIP Subscriber Profile	MIP6-Feature-Vector	M	This AVP shall be included to inform the 3GPP AAA Server about the used mobility protocol. None of the PMIP6_SUPPORTED or MIP4_SUPPORTED flags shall be set, since DSMIPv6 is used in this case.
APN	Service-Selection	O	If present, this IE shall contain the Network Identifier part of the APN extracted from the IKE_AUTH message. It shall include the APN that the user shall be connected to. It shall be only included if received from UE. In case it is not received, the 3GPP AAA Server shall assign the received PDN-GW identity to the default APN.
QoS capabilities	QoS-Capability	O	This IE shall be included if present in the request message. It shall indicate to the 3GPP AAA Server that the PGW requests downloading a static QoS profile for the UE. The PGW may include this IE only at the initial attach of the UE.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
Care of Address	MIP-Careof-Address	O	If present, this IE shall contain the IPv4 or the IPv6 Care of Address of the UE as defined in IETF RFC 5778 [11]
AAA Failure Indication	AAA-Failure-Indication	O	If present, this information element shall indicate that the request is sent after the PDN-GW has determined that a previously assigned 3GPP AAA Server is unavailable.
DER S6b Flags	DER-S6b-Flags	O	This Information Element contains a bit mask. See 9.2.3.7 for the meaning of the bits.
UE local IP address	UE-Local-IP-Address	O	The PDN GW shall include this IE based on local policy for Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39]. If present, it shall contain the source IPv4 or IPv6 address of the IKE_SA_AUTH message from the UE.

Table 9.1.2.1/2: Authentication and Authorization Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User Identity	User-Name	O	This information element, if present, shall contain the identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]. This IE shall include the leading digit used to differentiate between authentication schemes.
EAP Payload	EAP-Payload	O	If present, this IE shall contain the Encapsulated payload for UE – 3GPP AAA Server mutual authentication
Master Session Key	EAP-Master-Session-Key	C	This IE shall contain the Keying material for protecting the communication between the UE and PDN GW. It shall be present only if the result code is set to success.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_AUTHENTICATE. See IETF RFC 4072 [5].
Result Code	Result-Code / Experimental-Result-Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]) or as per in NASREQIETF RFC 4005 [58]). The Result-Code DIAMETER_MULTI_ROUND_AUTH shall be used in the responses that trigger further requests from the PDN GW and DIAMETER_SUCCESS shall be included at the successful completion of the authentication and authorization procedure. The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. If the Result-Code is set to DIAMETER_SUCCESS_RELOCATE_HA as defined in IETF RFC 5778 [11], then the 3GPP AAA server is indicating to the PGW that it shall initiate a HA switch procedure towards the UE.
MIP Subscriber Profile	MIP6-Feature-Vector	C	This AVP shall be present if the authorization was successful. None of the PMIP6_SUPPORTED or MIP4_SUPPORTED flags shall be set, since DSMIPv6 is used in this case.
Permanent User Identity	Mobile-Node-Identifier	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This IE shall contain an AAA/HSS assigned permanent user identity (i.e. an IMSI in root NAI format as defined in clause 19 of 3GPP TS 23.003 [14]). This IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This AVP shall contain the default APN, the list of authorized APNs, user profile information. APN-Configuration is a grouped AVP including the following information elements per APN: - APN - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - Allowed PDN type (IPv4, IPv6, IPv4v6, IPv4_OR_IPv6) - APN-AMBR
Reallocated PGW Address	MIP6-Agent-Info	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS_RELOCATE_HA indicating to the PDN GW that it shall initiate a HA switch procedure towards the UE. This information element shall contain the PDN GW identity of the target PDN GW.
Session Time	Session-Timeout	C	If the authentication and authorization succeeded, then this IE shall contain the time this authorization is valid for.

QoS resources	QoS-Resources	C	This AVP shall be included only if the QoS-Capability AVP was received in the authorization request and the authorization succeeded. Then the 3GPP AAA server shall include a static QoS profile in this IE during the UE initial attach if the PDN GW included QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0.
UE Charging Data	3GPP-Charging-Characteristics	O	If present, this information element shall contain the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
3GPP AAA Server URI	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Trust Relationship Indicator	AN-Trusted	C	This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted, or untrusted. This AVP shall be present if the 3GPP AAA Server is able to make decision on whether the access network is Trusted or Untrusted.
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated for the user in the HSS and signalling based activation is to be used to download the trace activation from the HSS to the PDN GW. Only the Trace-Data AVP shall be included to the Trace-Info AVP and shall contain the following AVPs: - Trace-Reference - Trace-Depth - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List,for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

9.1.2.1.2 PDN GW Detailed Behaviour

After completing the IKE_SA_INIT exchange, upon receipt of an IKE_AUTH message, including the IDi payload but not the AUTH payload, the PDN GW shall send an Diameter-EAP-Request (DER) message towards the 3GPP AAA Server / Proxy. The EAP Payload AVP shall contain an EAP-Response/Identity with the identity extracted from the IDi field.

Upon receipt of an IKE_AUTH message with an EAP payload from the UE, the PDN GW shall send an Diameter-EAP-Request (DER) with the EAP Payload AVP containing the according EAP-Response to the 3GPP AAA Server / Proxy.

Upon receipt of a Diameter-EAP-Answer (DEA) message from the 3GPP AAA Server / Proxy, the PDN GW shall then send an IKE_AUTH message containing the according EAP Payload to the UE.

Upon receipt of an IKE_AUTH message with the AUTH payload after the EAP authentication was successful, the PDN_GW shall proceed as specified in 3GPP TS 24.303 [13].

If the handover indication to the PGW is missing, i.e. IPv6 Home Network Prefix assigned to the UE is not included in IKE_AUTH request message as specified in 3GPP TS 24.303 [13], the PGW shall notify 3GPP AAA Server that the UE performs initial attach by setting Initial-Attach-Indicator in the DER-S6b-flags AVP.

The PDN GW shall utilize the downloaded APN configuration data, among others, to decide whether the user's request for an IPv4 home address and/or IPv6 home address prefix shall be accepted or rejected.

If the Result-Code AVP is set to DIAMETER_SUCCESS_RELOCATE_HA and if the PGW has received a PGW identity in form of the FQDN from the 3GPP AAA server, then the PGW may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

If Trace-Info AVP has been received in the authentication and authorization response, the PDN GW shall start a trace session for the user. For details, see 3GPP TS 32.422 [32].

If the PDN-GW determines that a previously assigned 3GPP AAA Sever is unavailable, it may attempt to send a new authentication and authorization request to an alternate 3GPP AAA Server. If the PDN-GW receives from this new server a redirect indication towards the former server (due to the HSS having stored the former 3GPP AAA Server identity), it shall terminate all previously existing sessions and PDN connections for that user, and it shall re-send again the request towards the new server, but it shall include the AAA-Failure-Indication AVP in the new request.

9.1.2.1.3 3GPP AAA Server Detailed Behaviour

For S6b, on receipt of the DER message, the 3GPP AAA Server shall process the DER message according to 3GPP TS 33.402 [19].

Upon successful completion, a DIAMETER_SUCCESS shall be returned to indicate successful authentication procedure and authentication information shall be returned. If the APN requested by the PDN GW is authorized by the wildcard APN, the 3GPP AAA Server shall include the wildcard APN in the Service-Selection AVP of the APN-Configuration AVP. The AAA server shall also include, among others, the MIP6-Feature-Vector AVP, including the subscriber profile of the UE in terms of DSMIPv6 feature the UE is authorized to use.

If the HSS indicates that the user is currently being served by a different PDN GW, the 3GPP AAA Server shall respond to to the PDN GW with the Result-Code set to DIAMETER_SUCCESS_RELOCATE_HA and include the new assigned PDN GW identity in the MIP6-Agent-Info AVP.

If receiving the UE Care of Address from the PDN GW and Initial-Attach-Indicator set by the PGW in DER-S6b-flags, the 3GPP AAA Server may select a different PDN GW which is closer to the UE than the currently serving PDN GW as specified in 3GPP TS 23.402 [3] based on the received UE Care of Address. In this case, the 3GPP AAA Server shall respond to the PDN GW with the Result-Code set to DIAMETER_SUCCESS_RELOCATE_HA and include the selected PDN GW identity in the MIP6-Agent-Info AVP.

If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the PDG-GW with the Result-Code set to DIAMETER_REDIRECT_INDICATION and Redirect-Host set to the Diameter URI of the 3GPP AAA Server currently serving the user (this Diameter URI shall be constructed based on the Diameter Identity included in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

If the 3GPP AAA Server receives a request message not related to any existing session and is able to recognize that the PDN-GW included the AAA-Failure-Indication AVP in the request, the 3GPP AAA Server shall also include the AAA-Failure-Indication AVP over the SWx interface, while retrieving the access authentication and authorization data from the HSS.

The 3GPP AAA Server shall run EAP-AKA as specified in 3GPP TS 33.402 [19]. Exceptions shall be treated as error situations and the result code shall be set to DIAMETER_UNABLE_TO_COMPLY.

Before sending out the AKA challenge, the 3GPP AAA Server shall decide whether the access network is handled as Trusted or Untrusted and set the value of the AN-Trusted AVP correspondingly in the answer message to indicate the trust relationship of the access network to the PDN GW. The 3GPP AAA Server shall make the decision based on the UE Identity and the trust relationship information marked during the authentication and authorization procedure over STa, SWa or SWm. If the 3GPP AAA server is unable to determine the trust relationship of the access network, it shall not include the AN-Trusted AVP in the answer message to the PDN GW.

For Fixed Broadband access network interworking as specified in 3GPP TS 23.139 [39],

- For trusted access, the 3GPP AAA server shall determine if the UE is connected via a BBF-defined WLAN access according to the UE local IP address in UE-Local-IP-Address AVP from the PDN GW. If the UE is connected via a BBF-defined WLAN access, the 3GPP AAA server shall perform the enabling UE reflective QoS function as specified in 3GPP TS 24.139 [43].

- For untrusted access, the UE local IP address is assigned by the ePDG and not by the non-3GPP access network. Hence, in this case the 3GPP AAA Server shall ignore the UE local IP address in UE-Local-IP-Address AVP from the PDN GW.

9.1.2.1.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the authentication answer that completes a successful authentication, the 3GPP AAA Proxy shall record the state of the connection (i.e. Authentication Successful).

If receiving the UE Care of Address from the PDN GW which is in the VPLMN, the 3GPP AAA Proxy may select a different PDN GW which is closer to the UE than the currently serving PDN GW as specified in 3GPP TS 23.402 [3] based on the received UE Care of Address. In this case, the 3GPP AAA Proxy shall respond to the PDN GW with the Result-Code set to DIAMETER_SUCCESS_RELOCATE_HA and include the selected PDN GW identity in the MIP6-Agent-Info AVP.

9.1.2.2 Authorization Procedures when using PMIPv6 or GTPv2

9.1.2.2.1 General

The following authorization procedures take place upon a reception of a PBU at the PDN GW from the MAG or upon a reception of a Create Session Request at the PDN GW from the trusted non-3GPP access network or from the ePDG.

The PDN GW shall update its identity to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time. If the PDN GW reports to the 3GPP AAA server that GTPv2 is used over the S2a or S2b interface, the 3GPP AAA Server may decide not to download parameters to the PDN GW on the S6b interface which are already provided to the PGW via the trusted non-3GPP access network through the STa and GTPv2 based S2a interfaces or via the ePDG through the SWm and the GTPv2 based S2b interfaces (e.g, static QoS profile, Trace Information, APN-AMBR).

The procedures are based on the reuse of NASREQ IETF RFC 4005 [4] AAR and AAA commands and the Diameter extensions defined for PMIP in IETF RFC 5779 [2].

Table 9.1.2.2.1/1: Authorization request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE shall defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be used in this case.
PDN GW Identity	MIP6-Agent-Info	C	If present, this IE shall contain the identity of the selected PDN GW for the UE and the corresponding PDN connection. It shall be present on the first authorization request sent by the PGW to the 3GPP AAA Server for a given APN. Also, it shall be present to communicate to the 3GPP AAA Server the identity of the PDN GW used for the establishment of emergency PDN connections.
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity is present and does not contain an FQDN.
Mobility features	MIP6-Feature-Vector	M	This IE shall contain the mobility features used by the PDN GW. The PDN GW shall set the PMIP6_SUPPORTED flag or the GTPv2_SUPPORTED flag according to the protocol variant used over the S2a or the S2b interface.
APN	Service-Selection	M	This IE shall contain the Network Identifier part of the APN extracted from the PBU or the Create Session Request message. For emergency PDN connection establishment (i.e., when Emergency-Services AVP is present, with the Emergency-Indication bit set), this IE may be ignored by the 3GPP AAA Server.
QoS capabilities	QoS-Capability	O	If included in the request message, this IE shall indicate to the 3GPP AAA server that the PDN GW requests downloading a static QoS profile for the UE. The PDN GW may include this IE only at the initial attach of the UE. The PDN GW should not include this IE if GTPv2 is used over the S2a or the S2b interface. The PDN GW shall not include this IE if the Emergency-Indication bit of the Emergency-Services AVP is set in the message.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
Origination Time Stamp	Origination-Time-Stamp	C	The PGW shall include this IE if it received the Origination Time Stamp from the MME/SGSN or TWAN/ePDG and if the PGW supports the procedure specified in clause 13.2 of 3GPP TS 29.274 [38]. If included in the request message, this IE shall contain the Origination Time Stamp value provided to the PGW in the Create Session Request or PBU message. This indicates the time at which the originating entity initiated the request.
Maximum Wait Time	Maximum-Wait-Time	C	The PGW shall include this IE if it received the Maximum Wait Time from the MME/SGSN or TWAN/ePDG, and the PGW supports the procedure specified in clause 13.3 of 3GPP TS 29.274 [38], and the 3GPP AAA Server pertains to the same PLMN as the PGW or if the 3GPP AAA Server pertains to a different PLMN and operator policy in the PGW allows to use this procedure towards this PLMN. If included in the request message, this IE shall contain the Maximum Wait Time provided to the PGW in the Create Session Request or PBU message.This indicates the duration during which the originator of the request waits for a response.
Emergency Services	Emergency-Services	C	The PGW shall include this information element, with the Emergency-Indication bit set, during the establishment of an emergency PDN connection.

Table 9.1.2.2.1/2: Authorization answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result code	Result-Code	M	This IE shall contain the result of the operation. The possible values of the Result-Code AVP are defined in IETF RFC 6733 [58]. This IE shall be set to DIAMETER_SUCCESS if the update of the PDN GW identity succeeded. It shall be set to DIAMETER_AUTHORIZATION_REJECTED if the update of the PDN GW identity failed.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Authorized mobility features	MIP6-Feature-Vector	C	The 3GPP AAA Server shall insert this AVP if the authorization was successful. The PMIP6_SUPPORTED or the GTPv2_SUPPORTED flag shall be set according to the value received in the Authorization request.
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This AVP shall contain the user profile information. APN-Configuration is a grouped AVP and shall include the following information elements: - APN - Authorized 3GPP QoS profile - APN-AMBR This information element need not be included in the Authorization answer, if the MIP6-Feature-Vector in the Authorization request indicates that GTPv2 is used over S2a or S2b. This information element shall not be included in the Authorization Answer if the Emergency-Indication bit of the Emergency-Services AVP is set in the Authorization Request.
QoS resources	QoS-Resources	C	This AVP shall be included only if the QoS-Capability AVP was received in the authorization request and the authorization succeeded. Then the 3GPP AAA server shall include a static QoS profile in this IE during the UE initial attach if the PDN GW included a QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0.
3GPP AAA Server URI	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.

Trace information	Trace-Info	C	This AVP shall be included if the MIP6-Feature-Vector in the Authorization request indicates that PMIPv6 is used over S2a or S2b and if the subscriber and equipment trace has been activated or deactivated for the user in the HSS GW and signalling based activation is used to download the trace (de)activation from the HSS to the PDN GW. In an authorization response sent during the authorization procedure at PDN connection setup, the Trace-Data AVP shall be included. In an authorization response sent during the service authorization information update procedure, - the Trace-data AVP shall be included if trace activation is requested - the Trace-Reference AVP shall be included, if trace deactivation is requested. If the Trace-Data AVP is included, it shall contain the following AVPs: - Trace-Reference - Trace-Depth - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List,for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.

9.1.2.2.2 PDN GW Detailed Behaviour

Upon receipt of a PBU message from the MAG or upon receipt of a Create Session Request from the trusted non-3GPP access network or the ePDG which requires the establishment of a new PDN connection via the non-3GPP access, the PDN GW shall initiate an authorization procedure, by sending an Authorization Request message to the 3GPP AAA server or to the 3GPP AAA Proxy, with the Auth-Request-Type set to AUTHORIZE_ONLY, in order to update the PGW Address for the APN and the selected S2a or S2b protocol variant, as well as to optionally download any UE specific APN profile information such as IP address allocation information, QoS Information, Session timeouts, Session Idle timeouts etc.

The Create Session Request received from the trusted non-3GPP access network or the ePDG may include the identities of the 3GPP AAA server assigned to the UE i.e. the Origin-Host and Origin-Realm of the 3GPP AAA server included in the DEA message received by the ePDG/TWAN over SWm or STa interface. If supported, the PDN GW shall use these identities to address the Authorization Request message to the selected 3GPP AAA server.

The PDN GW shall include in the request the APN where the user shall be connected to. The PGW shall additionally include the Emergency-Services AVP, with the Emergency-Indication bit set, during the establishment of an emergency PDN connection.

The PDN GW Identity and PLMN shall only be included in the initial request to the 3GPP AAA server; subsequent authorization messages (due to a handover to a different MAG, for instance) shall not include it again.

After reception of the Authorization Response message, the PDN GW shall check that the Result-Code is set to DIAMETER_SUCCESS and, if so, it shall proceed to connect the user to the specified APN.

For PMIPv6 based S2a or S2b, if Trace-Info AVP including Trace-Data has been received in the authorization response, the PDN GW shall start a trace session for the user. If Trace-Info including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the PDN GW shall stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

For GTPv2 based S2a or S2b, the PDN GW shall ignore the Trace-Info AVP if received in the authorization response.

NOTE: For GTPv2 based S2a or S2b, trace is activated and deactivated via the STa and S2a interfaces or via the SWm and S2b interfaces.

9.1.2.2.3 3GPP AAA Server Detailed Behaviour

Upon receipt of the Authorization Request message from the PDN GW, the 3GPP AAA Server shall check whether the user's profile is available.

If the user's data exist in the 3GPP AAA Server, it shall check, whether it also has an active access authorization session for the user.

- If not, the 3GPP AAA Server shall reject the authorization request, including the Result-Code DIAMETER_AUTHORIZATION_REJECTED.

- If the 3GPP AAA Server has an existing authorization session,

  - If the APN requested by the PDN GW is included in the list of authorized APNs of the user or if the Emergency-Indication bit of the Emergency-Services AVP is set in the Authorization Request, then the 3GPP AAA Server shall:

    - set the Result-Code to DIAMETER_SUCCESS;

    - include the APN-Configuration AVP in the authorization answer if PMIP is used over S2a or S2b; the APN-Configuration AVP may also be included if GTPv2 is used over S2a or S2b. When the APN-Configuration AVP is included in the authorization answer, the Service-Selection AVP within the APN-Configuration AVP shall contain the wildcard APN if the APN requested by the PDN GW is authorized by the wildcard APN;

    - update the PDN GW information for the APN for the UE on the HSS as specified in clause 8.1.2.2.2, if the Emergency-Indication bit of the Emergency-Services AVP is not set in the Authorization Request; and

    - update on the HSS the PDN GW Identity used for the establishment of emergency PDN connections for the UE, as specified in clause 8.1.2.2.2, based on operator policy (e.g. on whether the operator uses a static PDN GW or not for emergency services), if the Emergency-Services AVP is present, with the Emergency-Indication bit set, in the Authorization Request and the user is non-roaming and authenticated.

  - If the APN requested by the PDN GW is not included in the list of authorized APNs and the Emergency-Indication AVP is not present in the Authorization Request, then the status code DIAMETER_AUTHORIZATION_REJECTED shall be returned to the PDN GW to indicate an unsuccessful authorization.

If the user's profile does not exist in the 3GPP AAA Server, it shall retrieve the Diameter identity of the 3GPP AAA Server currently serving the user from the HSS following the procedures for subscriber profile download as specified in clause 8.1.2.2.2. Depending on the HSS response,

- If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the PDN-GW with the Result-Code set to DIAMETER_REDIRECT_INDICATION and Redirect-Host set to the Diameter URI of the 3GPP AAA Server currently serving the user (this Diameter URI shall be constructed based on the Diameter Identity included in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

- If the HSS returns DIAMETER_ERROR_USER_UNKNOWN, the 3GPP AAA Server shall return the same error to the PDN GW.

- If the HSS sends the user's profile to the 3GPP AAA Server, the authorization shall be rejected by setting the Result-Code to DIAMETER_AUTHORIZATION_REJECTED. The 3GPP AAA Server shall delete the downloaded user profile.

NOTE 1: The last outcome corresponds to the case that the user has no active access authorization procedure. This is considered as an error situation, e.g. the Trusted Non-3GPP access network may have sent PBU without authorizing the user.

NOTE 2: After the 3GPP AAA Server has accepted a new S6b session from a particular PGW, the 3GPP AAA server can consider that any existing S6b session(s) for the same UE – APN combination supported via a different PGW (i.e. with a different Origin-Host AVP) is obsolete and can send ASR command(s) to initiate the termination of the hanging session(s) in that PGW.

If the 3GPP AAA Server supports the detection and handling of late arriving requests as specified in clause 13.2 of 3GPP TS 29.274 [38], upon receipt of an Authorization Request which collides with an existing session context, for the same UE and APN but a different PGW (i.e. different Origin-Host AVP), the 3GPP AAA Server shall accept the new Authorization Request only if it contains a more recent Origination Time Stamp than the Origination Time Stamp stored for the existing S6b session. An incoming Authorization Request shall be considered as more recent than an existing session and be accepted if no Origination Time Stamp information was provided for at least one of the two sessions. The 3GPP AAA Server shall reject an incoming Authorization Request whose Origination Time Stamp is less recent than the Origination Time Stamp of the existing session by setting the Experimental-Result-Code to DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST.

If the 3GPP AAA Server supports the detection and handling of late arriving requests as specified in clause 13.3 of 3GPP TS 29.274 [38], upon receipt of an Authorization Request which contains the Origination Time Stamp and the Maximum Wait Time parameters, the 3GPP AAA Server should check that the request has not already timed out at the originating entity. The 3GPP AAA Server may perform additional similar checks before sending the answer, e.g. upon receipt of a response from the HSS. The 3GPP-AAA Server should reject an Authorization Request that is known to have timed out by setting the Experimental-Result-Code to DIAMETER_ERROR_TIMED_OUT_REQUEST.

9.1.2.2.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the authorization answer, the 3GPP AAA Proxy

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authorization Successful).

9.1.2.3 PDN GW Initiated Session Termination Procedures

9.1.2.3.1 General

The S6b reference point allows the PDN GW to inform the 3GPP AAA server that the UE disconnected a PDN connection associated to an APN, or that the PDN connection was handed over to the 3GPP access, and therefore the mobility session established for this PDN connection is to be removed.

The procedure shall be initiated by the PDN GW. These procedures are based on the reuse of Diameter STR and STA commands as specified in IETF RFC 6733 [58].

Each PDN connection shall be identified by the Diameter Session-Id parameter.

Table 9.1.2.3.1/1: S6b Session Termination Request

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Termination Cause	Termination-Cause	M	This IE shall contain the reason for the disconnection, according to the values and reasons described in IETF RFC 6733 [58]. In particular: - If the session is terminated as a result of a PDN disconnection initiated by the UE, the Termination-Cause shall be set to the value DIAMETER_LOGOUT (1) - If the session is terminated as a result of a PDN handover towards 3GPP access, the Termination-Cause shall be set to the value DIAMETER_USER_MOVED (7)

Table 9.1.2.3.1/2: S6b Session Termination Answer

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for S6b errors.

9.1.2.3.2 PDN GW Detailed Behaviour

The PDN GW shall make use of this procedure when the PDN Connection associated to the diameter session is, either disconnected, or handed over to the 3GPP access.

Upon receipt of the Session Termination Answer message from the 3GPP AAA Server or from the 3GPP AAA Proxy, the PDN GW shall check the Result Code AVP, and in case of a DIAMETER_SUCCESS code, it shall release the context associated to the active session identified by the Session-Id parameter used in the initial authorization exchange.

9.1.2.3.3 3GPP AAA Server Detailed Behaviour

Upon receipt of the Session Termination Request message from the PDN GW or from the 3GPP AAA Proxy, the 3GPP AAA Server shall check that there is an ongoing session associated to any of the parameters received in the message (Session-Id and User Name).

If an active session is found, the 3GPP AAA Server shall release the session context associated to the specified session, and a Session Termination Answer message shall be sent to the PDN GW or 3GPP AAA Proxy, indicating DIAMETER_SUCCESS.

If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, then a Session Termination Answer message shall be sent to the PDN GW or 3GPP AAA Proxy, indicating DIAMETER_UNKNOWN_SESSION_ID.

9.1.2.3.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Session Termination Request message from the PDN GW, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server.

On receipt of the Session Termination Answer message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the PDN GW, and it shall release any local resources associated to the specified sessions only if the result code is set to DIAMETER_SUCCESS.

9.1.2.4 3GPP AAA Initiated Session Termination Procedures

9.1.2.4.1 General

The S6b reference point allows the 3GPP AAA server to order a PDN GW to remove a PDN connection previously activated by the UE.

This procedure shall be initiated by the 3GPP AAA server. This indicates to the PDN GW to remove the corresponding PDN connection (identified by Session-ID AVP and User-Name AVP). This procedure is based on the reuse of NASREQ IETF RFC 4005 [4] ASR, ASA, STR and STA commands.

The 3GPP AAA Server shall include the Auth-Session-State AVP in the ASR command with a value of NO_STATE_MAINTAINED if it does not require a STR from the PDN GW. If it does require a STR from the PDN GW, the 3GPP AAA Server shall either omit the Auth-Session-State AVP from the ASR command or include the Auth-Session-State AVP in the ASR command with a value of STATE_MAINTAINED.

Table 9.1.2.4.1/1: S6b Abort Session Request

Information Element name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Auth-Session-State	Auth-Session-State	O	If present, this information element shall indicate to the PDN GW whether the 3GPP AAA Server requires an STR message.

Table 9.1.2.4.1/2: S6b Abort Session Answer

Information Element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 9.1.2.4.1/3: S6b Session Termination Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Termination-Cause	Termination-Cause	M	This information element shall contain the reason why the session was terminated. It shall be set to "DIAMETER_ADMINISTRATIVE" to indicate that the session was terminated in response to an ASR message.

Table 9.1.2.4.1/4: S6b Session Termination Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result-Code	Result-Code	M	This IE shall indicate the result of the operation.

9.1.2.4.2 PDN GW Detailed Behaviour

Upon receipt of the Abort Session Request message from the 3GPP AAA Server or from the 3GPP AAA Proxy, the PDN GW shall check that there is an ongoing session with the received session-ID.

If an active session is found:

- In the PMIPv6 or GTPv2 or MIPv4 cases, the PDN GW shall release any resources associated with the identified diameter session, but it shall not terminate any associated PDN connection.

- In the DSMIPv6 case, the PDN GW shall initiate a termination procedure for the associated PDN connection, and shall release any resources associated with the identified diameter session.

If the termination procedure is successful for the identified session, an Abort Session Answer message shall be sent to the 3GPP AAA Server or 3GPP AAA Proxy, indicating DIAMETER_SUCCESS.

If the Session-Id included in the request does not correspond with any active session, or if an active session is found but it does not belong to the user identified by the User Name parameter, then an Abort Session Answer message shall be sent to the 3GPP AAA Server or 3GPP AAA Proxy, indicating DIAMETER_UNKNOWN_SESSION_ID.

If the termination procedure for the identified session cannot be completed successfully, an Abort Session Answer message shall be sent to the 3GPP AAA Server or 3GPP AAA Proxy, indicating DIAMETER_UNABLE_TO_COMPLY.

If the termination procedure was successful for the identified session and the STR is required by the 3GPP AAA Server, the PDN GW shall send an STR to the 3GPP AAA Server with the Termination-Cause set to DIAMETER_ADMINISTRATIVE.

9.1.2.4.3 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall intiate a separate procedure for each active PDN connection of the user, even if the user has several PDN connections via the same PDN GW.

Upon receipt of the Abort Session Answer message from the PDN GW or from the 3GPP AAA Proxy, the 3GPP AAA Server shall check the Result Code AVP, and in case of a DIAMETER_SUCCESS code, it shall release the context associated to the active session identified by the Session-Id parameter.

If the error code DIAMETER_UNABLE_TO_COMPLY is received in the Result Code AVP, the 3GPP AAA Server shall not release the context for the identified session.

If the error code DIAMETER_UNKNOWN_SESSION_ID is received in the Result Code AVP, the 3GPP AAA Server shall release the context for the identified session.

On receipt of the STR from PDN GW, the 3GPP AAA Server shall return an STA command with the Result-Code set to DIAMETER_SUCCESS.

9.1.2.4.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the Abort Session Request message from the 3GPP AAA Server, the 3GPP AAA Proxy shall route the message to the PDN GW.

If the 3GPP AAA Proxy requires an STR but the 3GPP AAA Server does not, the 3GPP AAA Proxy may override the value of the Auth-Session-State in the ASR and set it to STATE_MAINTAINED. In this case, the 3GPP AAA Proxy shall not forward the STR received from the PDN GW onto the 3GPP AAA Server and shall return an STA command to the PDN GW with the Result-Code set to DIAMETER_SUCCESS. The 3GPP AAA Proxy shall not override the value of the Auth-Session-State AVP under any other circumstances.

On receipt of the Abort Session Answer message from the PDN GW, the 3GPP AAA Proxy shall route the message to the 3GPP AAA Server, and it shall release any local resources associated to the specified session only if the result code is set to DIAMETER_SUCCESS.

When the 3GPP AAA Proxy receives the STR from PDN GW, it shall route the request to the 3GPP AAA Server. On receipt of the STA message, the 3GPP AAA Proxy shall route the response to the PDN GW.

9.1.2.5 Service Authorization Information Update Procedures

9.1.2.5.1 General

The S6b reference point allows the 3GPP AAA server to modify the authorization information previously provided to the PDN GW, i.e. during Service Authentication and Authorization when using DSMIPv6, or Service Authorization using PMIPv6 or GTPv2 or MIPv4, or the service authorization information provided during a previous Service Authorization update. This procedure is triggered by the modification of the non-3GPP profile of the UE or by activating or deactivating subscriber and equipment trace in the HSS or by the request of a P-CSCF restoration for WLAN. This procedure is also triggered by the authentication and authorization via STa or SWm, when the 3GPP AAA Server detects that an S6b session already exists for the UE, as specified in clause 5.1.2.1.2 and 7.1.2.1.2. In this case, the 3GPP AAA Server shall use this procedure to send the trust relationship to the PDN GW.

The Service Authorization Information Update procedure is performed in two steps:

1. The 3GPP AAA server issues an unsolicited re-authentication and/or re-authorization request towards the PDN GW. Upon receipt of this request, the PDN GW responds to the request and indicates the disposition of the request. If the re-authorization request is used for the purpose of the P-CSCF restoration for WLAN, only the P-CSCF Restoration Request bit shall be set in the RAR Flags. This procedure is based on the reuse of Diameter RAR and RAA commands as specified in IETF RFC 6733 [58]. The information element content for these messages is shown in tables 9.1.2.5.1/1 and 9.1.2.5.1/2.

2. After receiving the re-authorization request, the PDN GW invokes the authorization procedure for the APN identified by the session ID included in the former re-authorization request message. The authorization procedure for PMIPv6 or GTPv2 is described in the clause 9.1.2.2. Tables 9.1.2.5.1/3 and 9.1.2.5.1/4 describe the message contents in case of DSMIPv6.

Table 9.1.2.5.1/1: S6b Re-authorization request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Request Type	Re-Auth-Request-Type	M	This shall define whether re-authentication or re-authorization is required. AUTHORIZE_ONLY shall be used in this case.
RAR Flags	RAR-Flags	C	This Information Element contains a bit mask. See 9.2.3.1.5 for the meaning of the bits.

Table 9.1.2.5.1/2: S6b Re-authorization response

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 9.1.2.5.1/3: Authorization Request when using DSMIPv6

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User identity	User-Name	M	This information element shall contain the permanent identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be used in this case.
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity does not contain an FQDN.
Access Type	RAT-Type	M	This IE shall contain the non-3GPP access network technology type that is serving the UE.
PDN GW Identity	MIP6 -Agent-Info	M	This IE shall contain the FQDN and/or IP address(es) of the PDN GW that the user is connected to.
APN	Service-Selection	O	This IE shall contain the Network Identifier part of the APN extracted from the IKE_AUTH message. It shall include the APN that the user shall be connected to. It shall be only included if received from UE. In case it is not received, the 3GPP AAA server shall assign the received PDN-GW identity to the default APN.
QoS capabilities	QoS-Capability	C	If included in the request message, this IE shall indicate to the 3GPP AAA server that the PGW is capable of downloading a static QoS profile for the UE. The PGW shall include this IE only during UE the initial attach.

Table 9.1.2.5.1/4: Authorization Answer when using DSMIPv6

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result Code	Result-Code / Experimental-Result-Code	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used for errors defined in the Diameter base protocol (see IETF RFC 6733 [58]) or as per in NASREQIETF RFC 4005 [4]). 1xxx should be used for multi-round, 2xxx for success. The Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
APN and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This AVP shall contain the default APN, the list of authorized APNs, and user profile information. The APN-Configuration is a grouped AVP and shall include the following information elements per APN: - APN - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - VPLMN Dynamic Address Allowed. This information element might not be present if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW.
Session Time	Session-Timeout	C	If the authentication and authorization succeeded, then this IE shall contain the time this authorization is valid for. This information element might not be present if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW.
QoS resources	QoS-Resources	C	If the authentication and authorization succeeded, then the 3GPP AAA server shall include a static QoS profile in this IE during the UE initial attach if the PGW included QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0. This IE shall contain the QoS Profile authorized by the 3GPP AAA server for the requested APN based on the subscribed QoS parameters. This information element might not be present if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW.
Trace information	Trace-Info	C	This AVP shall be included if the subscriber and equipment trace has been activated or deactivated for the user in the HSS and signaling based activation is used to download the trace (de)activation from the HSS to the PDN GW. Trace-data AVP shall be included (directly under the Trace-Info) if trace activation is requested Trace-Reference AVP shall be included, if trace deactivation is requested. If the Trace-Data AVP is included, it shall contain the following AVPs: - Trace-Reference - Trace-Depth - Trace-Event-List, for PGW - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List,for PGW, if this AVP is not present, trace report generation is requested for all interfaces for PGW listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW". If this AVP is not included, trace activation in PDN GW is required.

Trust Relationship Indicator	AN-Trusted	C	This AVP shall contain the 3GPP AAA Server's decision on handling the non-3GPP access network, i.e. trusted, or untrusted. This AVP shall be sent if this re-authorization procedure is triggered by the authentication and authorization via STa or SWm, when the 3GPP AAA Server detects that an S6b session already exists for the UE and the S6b session was established as a result of an authentication request for DSMIPv6.

9.1.2.5.2 Detailed Behaviour

The 3GPP AAA server shall make use of this procedure in two steps to indicate and update relevant service authorization information in the PDN GW.

The 3GPP AAA server shall send a re-authorization request for all authorization sessions that are active for the user except for the request of a P-CSCF restoration for WLAN which only applies to the session related to the IMS APN.

Each PDN GW, upon reception of an unsolicited re-authentication and/or re-authorization request shall perform the following check and if there is an error detected, the PDN GW shall stop processing and return the corresponding error code.

Check the Re-Auth-Request-Type AVP:

1. If it indicates AUTHENTICATE_ONLY, Result-Code shall be set to DIAMETER_INVALID_AVP_VALUE.
2. If it indicates AUTHORIZE_ONLY, then, depending on the used IP mobility protocol:
   - In case of PMIPv6 or GTPv2, the PDN GW shall perform an authorization procedure as described in clause 9.1.2.2. If the P-CSCF Restoration Request bit in the RAR Flags is set:
     - for the case where the PDN GW triggers the extended P-CSCF restoration mechanism, the PDN GW may send the authorisation request with only mandatory AVPs.
     - for the case where the PDN GW triggers the basic P-CSCF restoration mechanism, the PDN GW shall send a Session Termination Request to the 3GPP AAA Server.
   - In case of DSMIPv6, the PDN GW shall perform an authorization procedure, sending an authorization request described in Tables 9.1.5.1/3 and 9.1.5.1/4. If the Trust-Relationship-Update flag is set in the RAR Flags present in the request, the PDN GW may send an authorization request with only mandatory AVPs.
3. If it indicates AUTHORIZE_AUTHENTICATE, Result-Code shall be set to DIAMETER_INVALID_AVP_VALUE.

When receiving the authorization request, if the authorization procedure is triggered by the 3GPP AAA Server to send the trust relationship to the PDN GW, the 3GPP AAA Server shall send the trust relationship of the access network for the subscriber to the PDN GW with Result-Code DIAMETER_SUCCESS. If the received AA-Request is triggered by the P-CSCF Restoration Request bit set in the RAR Flags sent to the PDN GW, the 3GPP AAA Server may send an authorization answer to the PDN GW with Result-Code DIAMETER_SUCCESS with only the mandatory AVPs described in Table 9.1.2.2.1/2. Otherwise, the 3GPP AAA Server shall check, whether

- the subscriber still has non-3GPP subscription to access EPC network
- the non-3GPP APNs are enabled for the user, and
- the updated user profile contains the APN, for which the given authorization session was created.

If any of the checked conditions are not met, the 3GPP AAA Server shall set the Result-Code to DIAMETER_AUTHORIZATION_REJECTED. Otherwise, it shall respond with Result-Code DIAMETER_SUCCESS.

After successful service authorization information update procedure, the PDN GW shall overwrite the stored user and APN data, for the subscriber identity indicated in the request, with the information received from the 3GPP AAA server. A session termination shall be initiated if the subscriber is no longer authorized to use the activated APN. If only trust relationship of the access network is received, the PDN GW shall keep all stored user and APN data for the subscriber identity as indicated in the request.

If the P-CSCF-Restoration-Request bit in the RAR Flags is set, the PDN GW shall keep all stored user data and APN data for the subscriber identity indicated in the request unless this data is present in the authorisation answer and proceed with the P-CSCF restoration for WLAN as specified in 3GPP TS 23.380 [52].

For PMIPv6 based S2a or S2b, if Trace-Info AVP including Trace-Data has been received in the authorization response, the PDN GW shall start a trace session for the user. If Trace-Info including Trace-Reference (directly under the Trace-Info) has been received in the authorization response, the PDN GW shall stop the ongoing trace session, identified by the Trace-Reference. For details, see 3GPP TS 32.422 [32].

For GTPv2 based S2a or S2b, the PDN GW shall ignore the Trace-Info AVP if received in the authorization response.

NOTE: For GTPv2 based S2a or S2b, trace is activated and deactivated via the STa and S2a interfaces or via the SWm and S2b interfaces.

9.1.2.6 Authorization Procedures when using MIPv4 FACoA

9.1.2.6.1 General

The following authorization procedures take place upon a reception of a RRQ at the PDN GW from the FA.

The PDN GW shall update its identity to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time.

MIPv4 security parameters shall be exchanged between the PDN GW and the 3GPP AAA Server.

The procedures are based on the reuse of NASREQ IETF RFC 4005 [4] AAR and AAA commands.

Table 9.1.2.6.1/1: Authorization request

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Permanent User Identity	User-Name	M	This IE shall contain the permanent user identity. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and shall be formatted as defined in clause 19 of 3GPP TS 23.003 [14]; this IE shall not include the leading digit prepended in front of the IMSI used to differentiate between authentication schemes.
Authentication Request Type	Auth-Request-Type	M	This IE shall define whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be used in this case.
PDN GW Identity	MIP6-Agent-Info	O	This IE shall contain the address and possibly the FQDN of the selected PDN GW for the UE and the corresponding PDN connection
PGW PLMN ID	Visited-Network-Identifier	C	This IE shall contain the identifier that allows the home network to identify the PLMN where the PGW is located. It shall be present when the PGW Identity is present and does not contain an FQDN.
Mobility features	MIP6-Feature-Vector	M	This IE shall contain the mobility features used by the PDN GW. The MIP4_SUPPORTED flag shall be set
APN	Service-Selection	C	If present this IE shall contain the Network Identifier part of the APN extracted from the RRQ message. In case it is not received, the 3GPP AAA Server shall assign the received PDN-GW identity to the default APN.
QoS capabilities	QoS-Capability	O	If included in the request message, this IE shall indicate to the 3GPP AAA Server that the PDN GW requests downloading of a static QoS profile for the UE. The PDN GW may include this IE only at the initial attach of the UE.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
MN-HA security parameter index	MIP-MN-HA-SPI	C	This IE shall contain the MN-HA security parameter index which is used in identifying MN-HA shared key as defined by 3GPP TS 33.402 [19]. It shall be included when the PDN-GW does not have the MN-HA shared key required to verify the MIPv4 RRQ message.

Table 9.1.2.6.1/2: Authorization answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result code	Result-Code	M	This IE shall contain the result of the operation. The possible values of the Result-Code AVP are defined in IETF RFC 6733 [58]. This IE shall be set to DIAMETER_SUCCESS if the authorization of a MAG or the update of the PDN GW identity succeeded. It shall be set to DIAMETER_AUTHORIZATION_REJECTED if the authorization of a new MAG or the update of the PDN GW identity failed.
Authentication Request Type	Auth-Request-Type	M	It shall contain the value AUTHORIZE_ONLY. See IETF RFC 4072 [5].
Authorized mobility features	MIP6-Feature-Vector	C	The 3GPP AAA Server shall insert this AVP if the authorization was successful. The MIP4_SUPPORTED flag shall be set.
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.
QoS resources	QoS-Resources	C	This AVP shall be included only if the QoS-Capability AVP was received in the authorization request and the authorization succeeded. Then the 3GPP AAA Server shall include a static QoS profile in this IE during the UE initial attach if the PDN GW included QoS-Capabilities AVP in the request message and the UE has been provisioned with a static QoS profile. The QoS profile template value in this IE shall be set to 0.
3GPP AAA Server URI	Redirect-Host	C	This information element shall be sent if the Result-Code value is set to DIAMETER_REDIRECT_INDICATION. When the user has previously been authenticated by another 3GPP AAA Server, it shall contain the Diameter URI of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The command shall contain zero or more occurrences of this information element. When choosing a destination for the redirected message from multiple Redirect-Host AVPs, the receiver shall send the Diameter request to the first 3GPP AAA Server in the ordered list received in the Diameter response. If no successful response to the Diameter request is received, the receiver shall send the Diameter request to the next 3GPP AAA Server in the ordered list. This procedure shall be repeated until a successful response is received from a 3GPP AAA Server.
Supported Features (See 3GPP TS 29.229 [24])	Supported-Features	O	If present, this information element shall contain the list of features supported by the origin host for the lifetime of the Diameter session.
MN-HA shared key	MIP-Session-Key	C	This information element contains the MN-HA shared key as defined by 3GPP TS 33.402 [19], it shall be included if the Result-Code value is set to DIAMETER_SUCCESS and the MIP-MN-HA-SPI was sent in the authorization request..
APN Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. This AVP shall contain the user profile information. APN-Configuration is a grouped AVP and shall include the following information elements: - APN - Authorized 3GPP QoS profile - APN-AMBR

9.1.2.6.2 PDN GW Detailed Behaviour

Upon receipt of a RRQ message from the FA, the PDN GW shall initiate an authorization procedure, by sending an Authorization Request message to the 3GPP AAA Server or to the 3GPP AAA Proxy, with the Auth-Request-Type set to AUTHORIZE_ONLY, in order to update the PGW Address for the APN, as well as to download any UE specific APN profile information such as IP address allocation information, QoS Information, Session timeouts, Session Idle timeouts, MIPv4 security parameters etc.

If the APN was included in the RRQ message, the PDN GW shall include in the request the APN where the user shall be connected.

The PDN GW Identity shall only be included in the initial request to the 3GPP AAA Server; subsequent authorization messages (due to a handover to a different FA, for instance) shall not include it again.

If the PDN GW does not have a MN-HA shared key associated with the SPI received in the RRQ MN-HA-AE, the PDN GW shall include the SPI in the Authorization Request to the 3GPP AAA Server.

After successful reception of the Authorization Request message, the PDN GW shall check that the Result-Code is set to DIAMETER_SUCCESS and, if so, it shall use the MN-HA key to verify the MN-HA AE of the RRQ received from the FA.

If the PDN-GW successfully verifies the MN-HA-AE it shall proceed to connect the user to the specified APN, and will send the RRP message to the FA.

9.1.2.6.3 3GPP AAA Server Detailed Behaviour

Upon receipt of the Authorization Request message from the PDN GW, the 3GPP AAA Server shall update the PDN GW information for the APN for the UE on the HSS. If the APN was not received from the PDN GW the 3GPP AAA Server shall assign the received PDN-GW identity to the default APN .

The 3GPP AAA Server must check that the user exists. If the user's data exists in the 3GPP AAA Server, it shall check, whether it also has an active access authorization session for the user.

- If not, the 3GPP AAA Server shall reject the authorization request, including the Result-Code DIAMETER_AUTHORIZATION_REJECTED.
- If the 3GPP AAA Server has an existing authorization session,
  - If the APN requested by the PDN GW is included in the list of authorized APNs of the user, then the 3GPP AAA Server shall include the Service-Selection AVP in the authorization answer. If no APN was requested the Service-Selection AVP shall contain the default APN.
    - If the MN-HA-SPI was included in the request and it matches the SPI belonging to a SA of the user then the 3GPP AAA Server shall include the MIP-Session-Key of the SA in the authorization answer and set the Result-Code to DIAMETER_SUCCESS.
    - If the MN-HA-SPI was included in the request and there is no match with a SPI belonging to a SA of the user then the status code DIAMETER_AUTHORIZATION_REJECTED shall be returned to the PDN GW to indicate an unsuccessful authorization.
  - If the APN requested by the PDN GW is not included in the list of authorized APNs, then the status code DIAMETER_AUTHORIZATION_REJECTED shall be returned to the PDN GW to indicate an unsuccessful authorization.

If the user's profile does not exist in the 3GPP AAA Server, it shall retrieve the Diameter identity of the 3GPP AAA Server currently serving the user from the HSS following the procedures for subscriber profile download as specified in clause 8.1.2.2.2. Depending on the HSS response,

- If the HSS indicates that the user is currently being served by a different 3GPP AAA Server, the 3GPP AAA Server shall respond to the PDG-GW with the Result-Code set to DIAMETER_REDIRECT_INDICATION and Redirect-Host set to the Diameter URI of the 3GPP AAA Server currently serving the user (this Diameter URI shall be constructed based on the Diameter Identity included in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).
- If the HSS returns DIAMETER_ERROR_USER_UNKNOWN, the 3GPP AAA Server shall return the same error to the PDN GW.
- If the HSS sends the user's profile to the 3GPP AAA Server, the authorization shall be rejected by setting the Result-Code to DIAMETER_AUTHORIZATION_REJECTED. The 3GPP AAA Server shall delete the downloaded user profile.

NOTE: The last outcome corresponds to the case that the user has no active access authorization procedure. This is considered as an error situation, e.g. the Trusted Non-3GPP access network may have sent RRQ without authorizing the user.

9.1.2.6.4 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy is required to handle roaming cases in which the PDN GW is located in the VPLMN. The 3GPP AAA Proxy shall act as a stateful proxy.

On receipt of the authorization answer, the 3GPP AAA Proxy

- shall check locally configured information for the maximum allowed static QoS parameters valid for visitors from the given HPLMN and modify the QoS parameters received from the 3GPP AAA Server, to enforce the policy limitations.
- shall record the state of the connection (i.e. Authorization Successful).

9.2 Protocol Specification

9.2.1 General

The S6b reference point shall be based on Diameter, as defined in IETF RFC 6733 [58], and contain the following additions and extensions:

- IETF RFC 4005 [4], which defines a Diameter protocol application used for Authentication, Authorization and Accounting (AAA) services in the Network Access Server (NAS) environment.
- IETF RFC 5779 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF RFC 5777 [9], which defines attribute value pairs to convey QoS information between Diameter peers.

The PDN GW to 3GPP AAA server or the PDN GW to 3GPP AAA proxy communication shall use the LMA to AAA interface functionality defined in IETF RFC 5779 [2] to update the 3GPP AAA server with PDN GW identity, indicate the protocol selected on S2a or S2b and optionally retrieve mobility related parameters and static QoS profiles, when PMIPv6 or GTPv2 based S2a or S2b is used.

The PDN-GW acts as a LMA when the UE attaches to the EPC using the S2a or S2b reference points and PMIPv6 is used. The PDN GW also follows the LMA to AAA interface functionality defined in IETF RFC 5779 [2] when UE attaches to the EPC using S2a or S2b reference point and GTPv2 is used. The PDN GW acts as HA when the UE attaches to the EPC using the S2a reference point and MIPv4 is used.

In the case the UE attached to the EPC using the S2c reference point, then the communication between the PDN GW and HA, IETF RFC 5778 [11] shall be used. The Application Id to be advertised over the S6b reference point corresponds to the DSMIPv6 "Diameter Mobile IPv6 IKE (MIP6I)" Application Id as defined in IETF RFC 5778 [11].

IKEv2 EAP-based initiator authentication is used for authenticating and authorizing the UE and updating the PDN-GW identity. In this case, the PDN GW shall behave as described in 3GPP TS 33.402 [19].

9.2.2 Commands

9.2.2.1 Commands for S6b DSMIPv6 Authorization Procedures

9.2.2.1.1 Diameter-EAP-Request (DER) Command

The Diameter-EAP-Request (DER) command, indicated by the Command-Code field set to 268 and the "R" bit set in the Command Flags field, is sent from a PGW to a 3GPP AAA server. The Command Code value and the ABNF are re-used from the IETF RFC 5778 [11].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY, 16777272 >
                             < Session-Id >
                             [ DRMP ]
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             { Auth-Request-Type }
                             [ RAT-Type ]
                             [ User-Name ]
                             [ Service-Selection ]
                             { EAP-Payload }
                             [ MIP6-Feature-Vector ]
                             [ MIP6-Agent-Info ]
                             [ QoS-Capability ]
                             [ Visited-Network-Identifier ]
                             [ MIP-Careof-Address ]
                             [ AAA-Failure-Indication ]
                             *[ Supported-Features ]
                             [DER-S6b-Flags]
                             [ UE-Local-IP-Address]
                             ...
                             *[ AVP ]
```

9.2.2.1.2 Diameter-EAP-Answer (DEA) Command

The Diameter-EAP-Answer (DEA) command, indicated by the Command-Code field set to 268 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PGW. The Command Code value and the ABNF are re-used from the IETF RFC 5778 [11].

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY, 16777272 >
                          < Session-Id >
                          [ DRMP ]
                          { Auth-Application-Id }
                          { Auth-Request-Type }
                          { Result-Code }
                          { Origin-Host }
                          { Origin-Realm }
                          [ User-Name ]
                          [ EAP-Payload ]
                          [ EAP-Master-Session-Key ]
                          [ Mobile-Node-Identifier ]
                          [ APN-Configuration ]
                          [ MIP6-Agent-Info ]
                          [ MIP6-Feature-Vector ]
                          [ 3GPP-Charging-Characteristics ]
                          *[ QoS-Resources ]
                          *[ Redirect-Host ]
                          [ Trace-Info ]
                          *[ Supported-Features ]
                          ...
                          *[ AVP ]
```

9.2.2.2 Commands for S6b PMIPv6, GTPv2 or DSMIPv6 Authorization Procedures

9.2.2.2.1 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from the PDN GW to the 3GPP AAA Server. The Command Code value and ABNF are

re-used from the IETF RFC 4005 [4] AA-Request command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

NOTE: This command is used for the S6b Authorization Procedure for PMIPv6 or GTPv2, and also for the S6b Service Authorization Information Update procedure for PMIPv6, GTPv2 or DSMIPv6 following a previous RAR/RAA command exchange initiated by the 3GPP AAA Server.

```
<AA-Request> ::=    < Diameter Header: 265, REQ, PXY, 16777272 >
                                < Session-Id >
                                [ DRMP ]
                                { Auth-Application-Id }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                { Auth-Request-Type }
                                [ User-Name ]
                                [ MIP6-Agent-Info ]
                                [ MIP6-Feature-Vector ]
                                [ Visited-Network-Identifier ]
                                [ QoS-Capability ]
                                [ Service-Selection ]
                                [ OC-Supported-Features ]
                                [ Origination-Time-Stamp ]
                                [ Maximum-Wait-Time ]
                                *[ Supported-Features ]
                                [ Emergency- Services ]
                                ...
                                *[ AVP ]
```

9.2.2.2.2 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from the 3GPP AAA Server to the PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 4005 [4] AA-Answer command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

NOTE: This command is used for the S6b Authorization Procedure for PMIPv6 or GTPv2, and also for the S6b Service Authorization Information Update procedure for PMIPv6, GTPv2 or DSMIPv6 following a previous RAR/RAA command exchange initiated by the 3GPP AAA Server.

```
<AA-Answer> ::= < Diameter Header: 265, PXY, 16777272 >
                                < Session-Id >
                                [ DRMP ]
                                { Auth-Application-Id }
                                { Auth-Request-Type }
                                { Result-Code }
                                { Origin-Host }
                                { Origin-Realm }
                                ...
                                [ MIP6-Feature-Vector ]
                                [ Session-Timeout ]
                                [ APN-Configuration ]
                                [ QoS-Resources ]
                                [ AN-Trusted ]
                                *[ Redirect-Host ]
                                [ Trace-Info ]
                                [ OC-Supported-Features ]
                                [ OC-OLR ]
                                *[ Load ]
```

*[Supported-Features]
...
*[AVP]

9.2.2.3 Commands for PDN GW Initiated Session Termination

9.2.2.3.1 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58] Session-Termination-Request command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

```
<Session-Termination-Request> ::=  < Diameter Header: 275, REQ, PXY, 16777272 >
                                   < Session-Id >
                                   [ DRMP ]
                                   { Auth-Application-Id }
                                   { Origin-Host }
                                   { Origin-Realm }
                                   { Destination-Realm }
                                   { Termination-Cause }
                                   [ User-Name ]
                                   [ OC-Supported-Features ]
                                   …
                                   *[ AVP ]
```

9.2.2.3.2 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA server to a PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::=  < Diameter Header: 275, PXY, 16777272 >

                                  < Session-Id >
                                  [ DRMP ]
                                  { Result-Code }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  [ OC-Supported-Features ]
                                  [ OC-OLR ]
                                  *[ Load ]
                                  *[ AVP ]
```

9.2.2.4 Commands for 3GPP AAA Server Initiated Session Termination

9.2.2.4.1 Abort-Session-Request (ASR) Command

The Abort-Session-Request (ASR) command, indicated by the Command-Code field set to 274 and the "R" bit set in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to a PDN GW. The ABNF is based on the one in IETF RFC 4005 [4].

```
< Abort-Session-Request > ::=  < Diameter Header: 274, REQ, PXY, 16777272 >
                               < Session-Id >
                               [ DRMP ]
                               { Origin-Host }
                               { Origin-Realm }
                               { Destination-Realm }
                               { Destination-Host }
                               { Auth-Application-Id }
                               [ User-Name ]
                               [ Auth-Session-State ]
                               …
```

*[AVP]

9.2.2.4.2 Abort-Session-Answer (ASA) Command

The Abort-Session-Answer (ASA) command, indicated by the Command-Code field set to 274 and the "R" bit cleared in the Command Flags field, is sent from a PDN GW to a 3GPP AAA Server/Proxy. The ABNF is based on the one in IETF RFC 4005 [4].

```
< Abort-Session-Answer > ::= < Diameter Header: 274, PXY, 16777272 >
                             < Session-Id >
                             [ DRMP ]
                             { Result-Code }
                             { Origin-Host }
                             { Origin-Realm }
                             …
                             *[ AVP ]
```

9.2.2.4.3 Session-Termination-Request (STR) Command

The Session-Termination-Request (STR) command, indicated by the Command-Code field set to 275 and the "R" bit set in the Command Flags field, is sent from an PDN GW to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58] Session-Termination-Request command.

```
<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777272 >
                                  < Session-Id >
                                  [ DRMP ]
                                  { Origin-Host }
                                  { Origin-Realm }
                                  { Destination-Realm }
                                  { Auth-Application-Id }
                                  { Termination-Cause }
                                  [ User-Name ]
                                  [ OC-Supported-Features ]
                                  …
                                  *[ AVP ]
```

9.2.2.4.4 Session-Termination-Answer (STA) Command

The Session-Termination-Answer (STA) command, indicated by the Command-Code field set to 275 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server/Proxy to an PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 6733 [58] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777272 >
                                 < Session-Id >
                                 [ DRMP ]
                                 { Result-Code }
                                 { Origin-Host }
                                 { Origin-Realm }
                                 [ OC-Supported-Features ]
                                 [ OC-OLR ]
                                 *[ Load ]
                                 *[ AVP ]
```

9.2.2.5 Commands for S6b MIPv4 FACoA Authorization Procedures

9.2.2.5.1 AA-Request (AAR) Command

The AA-Request (AAR) command, indicated by the Command-Code field set to 265 and the "R" bit set in the Command Flags field, is sent from a PDN GW to a 3GPP AAA Server. The Command Code value and ABNF are re-used from the IETF RFC 4005 [4] AA-Request command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

```
<AA-Request> ::=    < Diameter Header: 265, REQ, PXY, 16777272 >
                                < Session-Id >
                                [ DRMP ]
                                { Auth-Application-Id }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                { Auth-Request-Type }
                                [ User-Name ]
                                [ MIP6-Agent-Info ]
                                [ MIP6-Feature-Vector ]
                                [ Visited-Network-Identifier ]
                                [ QoS-Capability ]
                                [ Service-Selection ]
                                *[ Supported-Features ]
                                [MIP-MN-HA-SPI]
                                [ OC-Supported-Features ]
                                ...
                                *[ AVP ]
```

9.2.2.5.2 AA-Answer (AAA) Command

The AA-Answer (AAA) command, indicated by the Command-Code field set to 265 and the "R" bit cleared in the Command Flags field, is sent from a 3GPP AAA Server to a PDN GW. The Command Code value and ABNF are re-used from the IETF RFC 4005 [4] AA-Answer command. New AVPs are added using the *[AVP] extension mechanism in the original ABNF.

```
<AA-Answer> ::= < Diameter Header: 265, PXY, 16777272 >
                                < Session-Id >
                                [ DRMP ]
                                { Auth-Application-Id }
                                { Auth-Request-Type }
                                { Result-Code }
                                { Origin-Host }
                                { Origin-Realm }
                                [ OC-Supported-Features ]
                                [ OC-OLR ]
                                *[ Load ]
                                ...
                                [ MIP6-Feature-Vector ]
                                [ Session-Timeout ]
                                [ APN-Configuration ]
                                [ QoS-Resources ]
                                *[ Redirect-Host ]
                                *[ Supported-Features ]
                                [MIP-Session-Key]
                                ...
                                *[ AVP ]
```

9.2.2.6 Commands for S6b Service Authorization Information Update Procedures

9.2.2.6.1 Re-Auth-Request (RAR) Command

The Diameter Re-Auth-Request (RAR) command shall be indicated by the Command-Code field set to 258 and the "R" bit set in the Command Flags field and is sent from a 3GPP AAA Server or 3GPP AAA Proxy to a PDN-GW. The ABNF for the RAR command shall be as follows:

```
< Re-Auth-Request > ::=  < Diameter Header: 258, REQ, PXY, 16777272 >
                         < Session-Id >
                         [ DRMP ]
                         { Origin-Host }
                         { Origin-Realm }
                         { Destination-Realm }
                         { Destination-Host }
                         { Auth-Application-Id }
                         { Re-Auth-Request-Type }
                         [ User-Name ]
                         [RAR-Flags ]
                         ...
                         *[ AVP ]
```

9.2.2.6.2 Re-Auth-Answer (RAA) Command

The Diameter Re-Auth-Answer (ASA) command shall be indicated by the Command-Code field set to 258 and the "R" bit cleared in the Command Flags field and is sent from a PDN-GW to a 3GPP AAA Server or 3GPP AAA Proxy. The ABNF for the RAA commands shall be as follows:

```
< Re-Auth-Answer > ::=  < Diameter Header: 258, PXY, 16777272 >
                        < Session-Id >
                        [ DRMP ]
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        [ User-Name ]
                        ...
                        *[ AVP ]
```

9.2.3 Information Elements

9.2.3.0 General

The following clauses describes the Diameter AVPs defined for the S6b interface protocol in the different modes of operation (DSMIPv6, PMIPv6/GTPv2, MIPv4…).

For all AVPs which contain bit masks and are of the type Unsigned32, bit 0 shall be the least significant bit. For example, to get the value of bit 0, a bit mask of 0x00000001 should be used.

9.2.3.1 S6b DSMIPv6 procedures

9.2.3.1.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in DSMIPv6 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

Table 9.2.3.1.1/1: Diameter S6b AVPs for DSMIPv6

				AVP Flag rules			
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**
MIP6-Agent-Info	486	9.2.3.2.2	Grouped	M			V,P
MIP6-Feature-Vector	124	9.2.3.2.3	Unsigned64	M			V,P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
RAR-Flags	1522	9.2.3.1.5	Unsigned32	V			M,P
QoS-Capability	578	9.2.3.2.4	Grouped	M			V,P
QoS-Resources	508	9.2.3.2.5	Grouped	M			V,P
Trace-Info	1505	8.2.3.13	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
Trust-Relationship-Update	1515	9.2.3.1.4	Enumerated	V			M,P
AAA-Failure-Indication	1518	8.2.3.21	Unsigned32	V			M,P
DER-S6b-Flags	1523	9.2.3.7	Unsigned32	V			M,P
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 [58].							
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.							

9.2.3.1.2 Visited-Network-Identifier

The Visited-Network-Identifier AVP contains an identifier that helps the home network to identify the visited network (e.g. the visited network domain name). The Vendor-Id shall be set to 10415 (3GPP).

The AVP shall be encoded as:

mnc<MNC>.mcc<MCC>.3gppnetwork.org

If MNC consists of only 2 digits, a leading digit "0" shall be added to the MNC value (e.g., if MNC=15 and MCC=234, the value of Visited-Network-Identifier shall be "mnc015.mcc234.3gppnetwork.org").

9.2.3.1.3 Void

9.2.3.1.4 Void

9.2.3.1.5 RAR-Flags

The RAR-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be as defined in table 9.2.3.1.5/1:

Table 9.2.3.1.5/1: RAR-Flags

Bit	Name	Description
0	Trust-Relationship-Update-indication	This bit, when set, indicates to the PDN GW that the 3GPP AAA server only initiates the re-authorization procedure send the trust relationship to the PDN GW, and the PDN GW shall not perform any authorization procedure towards the UE.
1	P-CSCF Restoration Request	This bit, when set, shall indicate to the PDN GW that the 3GPP AAA Server requests the execution of the HSS-based P-CSCF restoration procedures for WLAN, as described in 3GPP TS 23.380 [52] clause 5.6.
NOTE: Bits not defined in this table shall be cleared by the sender and discarded by the recever of the command.		

9.2.3.2 S6b PMIPv6 or GTPv2 procedures

9.2.3.2.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in PMIPv6 or GTPv2 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

Table 9.2.3.2.1/1: Diameter S6b AVPs for PMIPv6 or GTPv2

				AVP Flag rules			
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**
MIP6-Agent-Info	486	9.2.3.2.2	Grouped	M			V,P
MIP6-Feature-Vector	124	9.2.3.2.3	Unsigned64	M			V,P
QoS-Capability	578	9.2.3.2.4	Grouped	M			V,P
QoS-Resources	508	9.2.3.2.5	Grouped	M			V,P
Trace-Info	1505	8.2.3.13	Grouped	V			M,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
Visited-Network-Identifier	600	9.2.3.1.2	OctetString	M,V			P
Origination-Time-Stamp	1536	9.2.3.2.6	Unsigned64	V			M,P
Maximum-Wait-Time	1537	9.2.3.2.7	Unsigned32	V			M,P
Emergency- Services	1538	7.2.3.5	Unsigned32	V			M,P
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 [58].							
NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.							

9.2.3.2.2 MIP6-Agent-Info

The MIP6-Agent-Info AVP contains the PDN GW identity or (for the chained S2 - PMIP based S8 case) the Serving GW address information. This AVP is defined in IETF RFC 5447 [6]. The identity of PDN GW is either an IP address transported in MIP-Home-Agent-Address or an FQDN transported in MIP-Home-Agent-Host. The PDN GW may use its IP address if a single IP address can be used for all Access Networks and protocols towards the PDN GW. In all other cases the PDN GW shall use its FQDN. MAG/AAA/HSS shall use FQDN if known. The grouped AVP has the following grammar:

```
MIP6-Agent-Info ::= < AVP Header: 486 >
                    *2[ MIP-Home-Agent-Address ]
                    [ MIP-Home-Agent-Host ]
                    [ MIP6-Home-Link-Prefix ]
                    *[ AVP ]
```

NOTE: The AVP MIP6-Home-Link-Prefix is not used in S6b, but it is included here to reflect the complete IETF definition of the grouped AVP.

9.2.3.2.3 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP contains a 64 bit flags field of supported mobility capabilities of the NAS. This AVP is defined in IETF RFC 5447 [6]. The NAS may include this AVP in a request message to indicate the mobility capabilities of the NAS to the 3GPP AAA server. Similarly, the Diameter server may include this AVP in an answer message to inform the NAS about which of the NAS indicated capabilities are supported or authorized by the 3GPP AAA Server.

Following capabilities are supported on S6b reference point in PMIPv6 or GTPv2 mode:

- PMIP6_SUPPORTED
- IP4_HOA_SUPPORTED
- GTPv2_SUPPORTED

9.2.3.2.4 QoS-Capability

The QoS-Capability AVP contains a list of supported Quality of Service profile templates (and therefore the support of the respective parameter AVPs). This AVP is defined in IETF RFC 5777 [9].

9.2.3.2.5 QoS-Resources

The QoS-Resources AVP includes a description of the Quality of Service resources for policing traffic flows. This AVP is defined in IETF RFC 5777 [9].

9.2.3.2.6 Origination-Time-Stamp

The Origination-Time-Stamp is of type Unsigned64. It indicates the UTC time when the originating entity initiated the request. It shall contain the number of milliseconds since 00:00:00 on 1 January 1900 UTC.

NOTE: This AVP contains the same numeric value, in milliseconds, as received over the GTPv2 protocol from the originating entity (see 3GPP TS 29.274 [38], clause 8.119).

9.2.3.2.7 Maximum-Wait-Time

The Maximum-Wait-Time is of type Unsigned32. It indicates the number of milliseconds since the Origination-Time-Stamp during which the originator of a request waits for a response. See 3GPP TS 29.274 [38].

9.2.3.3 S6b Re-used Diameter AVPs

Table 9.2.3.3/1: S6b re-used Diameter AVPs

Attribute Name	Reference	Comments
Supported-Features	3GPP TS 29.229 [24]	
Feature-List-ID	3GPP TS 29.229 [24]	See clause 9.2.3.4
Feature-List	3GPP TS 29.229 [24]	See clause 9.2.3.5
MIP-Careof-Address	IETF RFC 5778 [11]	
UE-Local-IP-Address	3GPP TS 29.212 [23]	
OC-Supported-Features	IETF RFC 7683 [47]	See clause 8.2.3.22
OC-OLR	IETF RFC 7683 [47]	See clause 8.2.3.23
DRMP	IETF RFC 7944 [53]	See clause 8.2.3.25
Load	IETF RFC 8583 [54]	See clause 8.2.3.26
NOTE 1: The M-bit settings for re-used AVPs override those of the defining specifications that are referenced. Values include: "Must set", "Must not set". If the M-bit setting is blank, then the defining specification applies. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.		

9.2.3.4 Feature-List-ID AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. For this release, the Feature-List-ID AVP value shall be set to 1 for the S6b application.

9.2.3.5 Feature-List AVP

The syntax of this AVP is defined in 3GPP TS 29.229 [24]. A null value indicates that there is no feature used by the S6b application. The meaning of the bits shall be as defined in table 9.2.3.5/1.

Table 9.2.3.5/1: Features of Feature-List-ID 1 used in S6b

Feature bit	Feature	M/O	Description
0	P-CSCF Restoration for WLAN	O	Support of P-CSCF Restoration for WLAN This feature is applicable to the AAR/AAA and RAR/RAA command pairs over the S6b interface, when the PDN GW supports the execution of the P-CSCF restoration procedures for WLAN for the related IMS PDN connection as described in 3GPP TS 23.380 [52] clause 5.6. If the PDN-GW does not indicate support of this feature in a former AAR command, the 3GPP AAA Server shall not send a RAR command requesting the execution of the HSS-based P-CSCF restoration procedures for WLAN,
Feature bit: The order number of the bit within the Supported-Features AVP, e.g. "1". Feature: A short name that can be used to refer to the bit and to the feature. M/O: Defines if the implementation of the feature is mandatory ("M") or optional ("O"). Description: A clear textual description of the feature.			

Features that are not indicated in the Supported-Features AVPs within a given application message shall not be used to construct that message.

9.2.3.6 S6b MIPv4 FACoA procedures

9.2.3.6.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in MIPv4 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

Table 9.2.3.6.1/1: Diameter S6b AVPs for MIPv4 FACoA

				AVP Flag rules			
Attribute Name	**AVP Code**	**Clause defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**
MIP6-Agent-Info	486	9.2.3.6.2	Grouped	M			V,P
MIP6-Feature-Vector	124	9.2.3.6.3	Unsigned64	M			V,P
QoS-Capability	578	9.2.3.6.4	Grouped	M			V,P
QoS-Resources	508	9.2.3.6.5	Grouped	M			V,P
MIP-MN-HA-SPI	491	9.2.3.6.6	Unsigned32	M			V,P
MIP-Session-Key	343	9.2.3.6.7	OctetString	M			V,P
Service-Selection	493	5.2.3.5	UTF8String	M			V,P
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 [58]. NOTE 2: If the M-bit is set for an AVP and the receiver does not understand the AVP, it shall return a rejection. If the M-bit is not set for an AVP, the receiver shall not return a rejection, whether or not it understands the AVP. If the receiver understands the AVP but the M-bit value does not match with the definition in this table, the receiver shall ignore the M-bit.							

9.2.3.6.2 MIP6-Agent-Info

The MIP6-Agent-Info AVP contains the PDN GW identity. This AVP is defined in IETF RFC 5447 [6]. The identity of PDN GW is either an IP address transported in MIP-Home-Agent-Address or an FQDN transported in MIP-Home-Agent-Host. The PDN GW may use its IP address if a single IP address can be used for all Access Networks and protocols towards the PDN GW. In all other cases the PDN GW shall use its FQDN. The FA/3GPP AAA Server/HSS shall use FQDN if known. The grouped AVP has the following grammar:

```
MIP6-Agent-Info ::= < AVP Header: 486 >
                    *2[ MIP-Home-Agent-Address ]
                    [ MIP-Home-Agent-Host ]
                    [ MIP6-Home-Link-Prefix ]
                    *[ AVP ]
```

NOTE: The AVP MIP6-Home-Link-Prefix is not used in S6b, but it is included here to reflect the complete IETF definition of the grouped AVP.

9.2.3.6.3 MIP6-Feature-Vector

The MIP6-Feature-Vector AVP contains a 64 bit flags field of supported mobility capabilities of the NAS. This AVP is defined in IETF RFC 5447 [6]. The NAS may include this AVP in a request message to indicate the mobility capabilities of the NAS to the 3GPP AAA Server. Similarly, the Diameter server may include this AVP in an answer message to inform the NAS about which of the NAS indicated capabilities are supported or authorized by the 3GPP AAA Server.

Following capabilities are supported on S6b reference point in MIPv4 FACoA mode:

- MIP4_SUPPORTED

9.2.3.6.4 QoS-Capability

The QoS-Capability AVP contains a list of supported Quality of Service profile templates (and therefore the support of the respective parameter AVPs). This AVP is defined in IETF RFC 5777 [9].

9.2.3.6.5 QoS-Resources

The QoS-Resources AVP includes a description of the Quality of Service resources for policing traffic flows. This AVP is defined in IETF RFC 5777 [9].

9.2.3.6.6 MIP-MN-HA-SPI

The MIP-MN-HA-SPI AVP contains the index of the security association between the Mobile Node and the HA. This AVP is defined in IETF RFC 5778 [11].

9.2.3.6.7 MIP-Session-Key

The MIP-Session-Key AVP contains the MN-HA shared key. This AVP is defined in IETF RFC 4004 [18].

9.2.3.7 DER-S6b-Flags

The DER-S6b-Flags AVP is of type Unsigned32 and it shall contain a bit mask. The meaning of the bits shall be asdefined in table 9.2.3.7/1:

Table 9.2.3.7/1: DER-S6b-Flags

Bit	Name	Description
0	Initial-Attach-Indicator	This bit, when set, indicates that a UE performs the Initial Attach procedure from non-3GPP access network. When not set, it indicates that a UE performs the Handover procedure.
NOTE:	Bits not defined in this table shall be cleared by the sender and discarded by the receiver of the command.	

9.2.4 Session Handling

The Diameter protocol between the PDN-GW and the 3GPP AAA Server or the 3GPP AAA Proxy shall always keep session state, and use the same Session-Id parameter for the lifetime of each Diameter session.

A Diameter session shall identify a PDN Connection for a given user and an APN, while the PDN Connection is kept alive in the non-3GPP access. When the PDN Connection is either disconnected on the non-3GPP access, or handed over to the 3GPP access, the diameter session shall be terminated. In order to indicate that the session state is to be maintained, the Diameter client and server shall not include the Auth-Session-State AVP, either in the request or in the response messages (see IETF RFC 6733 [58]).

10 Result-Code and Experimental-Result Values

10.1 General

This clause defines result code values that shall be supported by all Diameter implementations that conform to this specification.

10.2 Success

Result codes that fall within the Success category shall be used to inform a peer that a request has been successfully completed. The Result-Code AVP values defined in Diameter base protocol (IETF RFC 6733 [58]) shall be applied.

10.3 Permanent Failures

10.3.1 General

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request has failed, and should not be attempted again. The Result-Code AVP values defined in Diameter base protocol (IETF RFC 6733 [58]) shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

10.3.2 DIAMETER_ERROR_USER_UNKNOWN (5001)

This result code shall be sent by the HSS to indicate that the user identified by the IMSI is unknown (see 3GPP TS 29.229 [24]).

10.3.3 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED (5003)

This result code shall be sent by the HSS to indicate that there is currently no 3GPP AAA Server registered for the user (see 3GPP TS 29.229 [24]).

10.3.4 DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)

This result code shall be sent by the HSS to indicate that the subscriber is not allowed to roam in a certain non-3GPP V-PLMN (see 3GPP TS 29.229 [24]).

10.3.5 DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED (5005)

This result code shall be sent by the HSS to indicate that the node identity trying to be registered by a 3GPP AAA Server is already registered for a specific user (see 3GPP TS 29.229 [24]).

10.3.6 DIAMETER_ERROR_USER_NO_NON_3GPP_SUBSCRIPTION (5450)

This result code shall be sent by the HSS to indicate that no non-3GPP subscription is associated with the IMSI.

10.3.7 DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION (5451)

This result code shall be sent by the 3GPP AAA Server to indicate that the requested APN is not included in the user's profile, and therefore is not authorized for that user.

10.3.8 DIAMETER_ERROR_RAT_TYPE_NOT_ALLOWED (5452)

This result code shall be sent by the HSS to indicate the RAT type the UE is using is not allowed for the IMSI.

10.3.9 DIAMETER_ERROR_LATE_OVERLAPPING_REQUEST (5453)

This result code shall be sent by the 3GPP AAA Server to indicate that the incoming request collides with an existing session which has a more recent time stamp than the time stamp of the new request.

10.3.10 DIAMETER_ERROR_TIMED_OUT_REQUEST (5454)

This result code shall be sent by the 3GPP AAA Server to indicate that the incoming request is known to have already timed out at the originating entity.

10.3.11 DIAMETER_ERROR_ILLEGAL_EQUIPMENT (5554)

This result code shall be sent by the 3GPP AAA Server or 3GPP AAA Proxy to indicate that the Mobile Equipment used is not acceptable to the network (e.g. the Mobile Equipment is on the prohibited list of the EIR).

10.4 Transient Failures

10.4.1 General

Result codes that fall within the transient failures category shall be used to inform a peer that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future. The Result-Code AVP values defined in Diameter base protocol (IETF RFC 6733 [58]) shall be applied. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and the Result-Code AVP shall be absent.

There are no Transient Error codes defined in this specification.

11 3GPP AAA Server/Proxy – EIR

11.1 Functionality

11.1.1 General

The definition of the reference point between the 3GPP AAA Server or 3GPP AAA Proxy and the EIR and its functionality is specified in clauses 7.2 and 16.2 in 3GPP TS 23.402 [3].

The 3GPP AAA Server/Proxy – EIR reference point is used to check the Mobile Equipment's identity status (e.g. to check that it has not been stolen, or, to verify that it does not have faults).

11.1.2 Procedures Description

11.1.2.1 ME Identity Check

11.1.2.1.1 General

The Mobile Equipment Identity Check Procedure shall be used between the 3GPP AAA Server and the EIR if the TWAN or ePDG is in the HPLMN, or between the 3GPP AAA Proxy and the EIR if the TWAN or ePDG is in the VPLMN, to check the Mobile Equipment's identity status (e.g. to check that it has not been stolen, or, to verify that it does not have faults).

The Diameter Identity of the EIR is locally configured in the 3GPP AAA Server and 3GPP AAA Proxy.

This procedure is mapped to the commands ME-Identity-Check-Request/Answer (ECR/ECA) in the Diameter application specified in clause 7 of 3GPP TS 29.272 [29].

Table 11.1.2.1.1/1 specifies the involved information elements for the request.

Table 11.1.2.1.1/2 specifies the involved information elements for the answer.

Table 11.1.2.1.1/1: ME Identity Check Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Terminal Information	Terminal-Information	M	This information element shall contain the information about the used mobile equipment i.e. the IMEI. Within this Information Element, only the IMEI and the Software-Version AVPs shall be used on the 3GPP AAA Server/Proxy – EIR interface.
IMSI	User-Name (See IETF RFC 6733 [58])	O	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [3], clause 2.2.

Table 11.1.2.1.1/2: ME Identity Check Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
Result	Result-Code / Experimental-Result	M	This IE shall contain the result of the operation. The Result-Code AVP shall be used to indicate success / errors as defined in the Diameter base protocol (see IETF RFC 6733 [58]). The Experimental-Result AVP shall be used for errors. This is a grouped AVP which shall contain the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP. The following errors are applicable in this case: - Unknown equipment
Equipment Status	Equipment-Status	C	This information element shall contain the status of the requested mobile equipment as defined in 3GPP TS 22.016 [13]. It shall be present if the result of the ME Identity Check is DIAMETER_SUCCESS.

11.1.2.1.2 3GPP AAA Server Detailed Behaviour

The 3GPP AAA Server shall make use of this procedure to check the ME identity, if the 3GPP AAA Server is configured to check the IMEI with the EIR and if the ePDG or TWAN is in the HPLMN.

Terminal-Information, when sent by the 3GPP AAA Server to the EIR, shall contain the IMEI AVP, and it may contain also the Software-Version AVP.

IMSI may be sent together with Terminal Information to the EIR for operator-determined purposes.

When receiving the ME Identity Check answer from the EIR, the 3GPP AAA Server shall check the result code and the equipment status. Dependent upon the result, the 3GPP AAA Server shall determine whether to continue or stop the authentication and authorization procedure, see clause 5.1.2.1 and 7.1.2.1.

11.1.2.1.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy shall make use of this procedure to check the ME identity, if the 3GPP AAA Proxy is configured to check the IMEI with the EIR and if the ePDG or TWAN is in the VPLMN.

Terminal-Information, when sent by the 3GPP AAA Proxy to the EIR, shall contain the IMEI AVP, and it may contain also the Software-Version AVP.

IMSI may be sent together with Terminal Information to the EIR for operator-determined purposes.

When receiving the ME Identity Check answer from the EIR, the 3GPP AAA Proxy shall check the result code and the equipment status. Dependent upon the result, the 3GPP AAA Server shall determine whether to continue or stop the authentication and authorization procedure, see clause 5.1.2.1 and 7.1.2.1.

11.1.2.1.4 EIR Detailed Behaviour

See clause 6.2.1.3 of 3GPP TS 29.272 [29].

11.2 Protocol Specification

11.2.1 General

The 3GPP AAA Server/Proxy – EIR reference point shall be based on Diameter, as defined in IETF RFC 6733 [58]. It shall be defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

The Diameter application used over the 3GPP AAA Server/Proxy – EIR reference point is the S13/S13' Diameter application, and the application identifier is 16777252 (allocated by IANA).

11.2.2 Commands

11.2.2.1 ME Identity Check

11.2.2.1.1 ME-Identity-Check-Request (ECR) Command

See clause 7.2.19 of 3GPP TS 29.272 [29].

11.2.2.1.2 ME-Identity-Check-Answer (ECA) Command

See clause 7.2.20 of 3GPP TS 29.272 [29].

11.2.3 Information Elements

11.2.3.1 General

The following table specifies the Diameter AVPs re-used by the 3GPP AAA Server/Proxy - EIR interface protocol from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their use for the 3GPP AAA Server/Proxy – EIR interface.

Any other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported. The AVPs from Diameter base protocol specified in IETF RFC 6733 [58] are not included in table 11.2.3.1/1, but they may be re-used for the 3GPP AAA Server/Proxy - EIR protocol.

Table 11.2.3.1/1: Diameter AVPs re-used for the 3GPP AAA Server/Proxy – EIR interface

Attribute Name	Reference	Comments	M-bit
Terminal-Information	3GPP TS 29.272 [29]		
User-Name	IETF RFC 6733 [58]		
Equipment-Status	3GPP TS 29.272 [29]		

11.2.4 Session Handling

The Diameter sessions between the 3GPP AAA Server and the EIR, and between the 3GPP AAA Proxy and the EIR, shall be handled as specified for the Diameter sessions between the MME and the EIR in clause 7.1.4 of 3GPP TS 29.272 [29].

Annex A (informative): Trusted WLAN authentication and authorization procedure

A.1 General

This clause provides example call flows for the Trusted WLAN authentication and authorization procedure.

Call flows for TSCM or SCM for Non-seamless WLAN Offload are not represented as they can be easily derived from the normative part of this specification.

This Annex is informative and the normative descriptions in this specification and in 3GPP TS 33.402 [19] prevail over the descriptions in this Annex if there is any difference.

A.2 Call Flow for SCM and EPC-routed access

A.2.1 Successful call flow

Figure Annex A.2-1 describes a successful call flow for SCM and EPC-routed access, i.e. with S2a connectivity being granted to the UE.

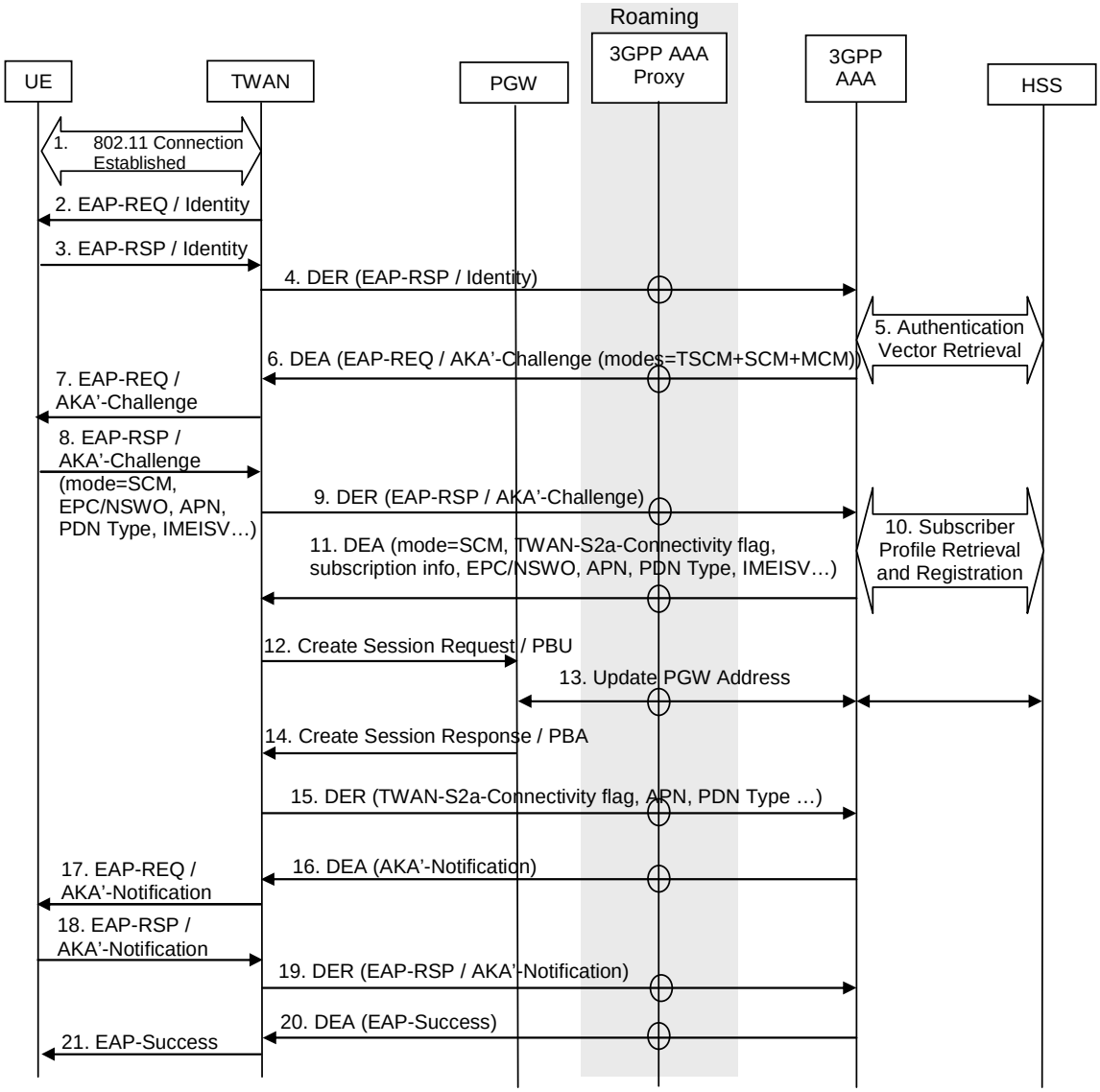

Figure Annex A.2-1: TWAN Authentication and Authorization Procedure for SCM and EPC routed access – successful case

1. A connection is established between the UE and the TWAN, using a specific procedure based on IEEE 802.11 [40].

2. The TWAN sends an EAP Request/Identity to the UE.

3. The UE sends an EAP Response/Identity message to the TWAN.

4. The TWAN forwards the EAP payload received from the UE to the 3GPP AAA Server and also indicates the supported TWAN connection modes in the DER message. The routing path may include one or several 3GPP AAA proxies for roaming case.

5. The 3GPP AAA Server retrieves authentication vectors for the UE from the HSS.

6. The 3GPP AAA Server sends an EAP Request/AKA'-Challenge in which it also indicates to the UE the TWAN connection modes supported by the network (e.g. TSCM, SCM and MCM) and in which it also requests the UE to provide its Mobile Equipment Identity. The Result-Code AVP in the DEA message is set to DIAMETER_MULTI_ROUND_AUTH. The TWAN-S2a-Connectivity Indicator is not set in the DEA-Flags AVP.

7. The TWAN forwards the EAP payload to the UE.

8. The UE sends the EAP Response/AKA'-Challenge in which it also indicates the requested connection mode. If the UE requests SCM and an EPC-routed access, the UE also indicates the requested APN, PDN type, Initial Attach/Handover indication and/or PCO. The user's Mobile Equipment Identity is also included, if available and if requested by the 3GPP AAA Server.

9. The TWAN forwards the EAP payload to 3GPP AAA Server.

10. If the 3GPP AAA Server successfully authentifies the UE, the 3GPP AAA Server downloads the user's subscription information from the HSS.

11. If the 3GPP AAA Server authorizes the SCM for EPC access for the UE, the 3GPP AAA Server includes the UE requested APN, PDN type, Initial Attach/Handover indication and/or PCO in the DEA message with the Result-Code AVP set to DIAMETER_MULTI_ROUND_AUTH. The 3GPP AAA Server also sets the TWAN-S2a-Connectivity Indicator in the DEA-Flags AVP to request the TWAN to proceed with the establishment of the S2a connectivity. The 3GPP AAA Server also includes the user's Mobile Equipment Identity, if available.

12. The TWAN sends a Create Session Request/PBU message to the PDN GW to initiate the S2a tunnel establishment.

13. The PDN GW informs the 3GPP AAA Server/HSS of its PDN GW identity and the APN corresponding to the UE's PDN Connection.

14. The PDN GW returns a Create Session Response/PBA message to the TWAN, including the IP address(es) allocated for the UE.

15. The TWAN includes the provided Connectivity Parameters received from the PDN GW and sets the TWAN-S2a-Connectivity Indicator in the DER-Flags AVP in the DER message to the 3GPP AAA Server. The 3GPP AAA Server ignores the EAP payload included in the DER message.

16. The 3GPP AAA Server includes the PDN connectivity parameters in the AKA'-Notification and sends the DEA message to the TWAN. The Result-Code AVP in the DEA message is set to DIAMETER_MULTI_ROUND_AUTH. The TWAN-S2a-Connectivity Indicator is not set in the DEA-Flags AVP.

17. The TWAN forwards the EAP payload to the UE.

18-19. The UE responds with an EAP-RSP/AKA'-Notification message that the TWAN forwardsto the 3GPP AAA Server.

20-21. The 3GPP AAA Server sends an EAP Success message that the TWAN forwards to the UE. The Result-Code AVP in the DEA message is set to DIAMETER_SUCESS. The subscription information need not to be included in the DEA message (if not changed).

A.2.2 Unsuccessful call flow

Figure Annex A.2-2 describes an unsuccessful call flow for SCM and EPC-routed access, where S2a connectivity can not been granted to the UE due to an overload condition in the network for the APN requested by the UE.

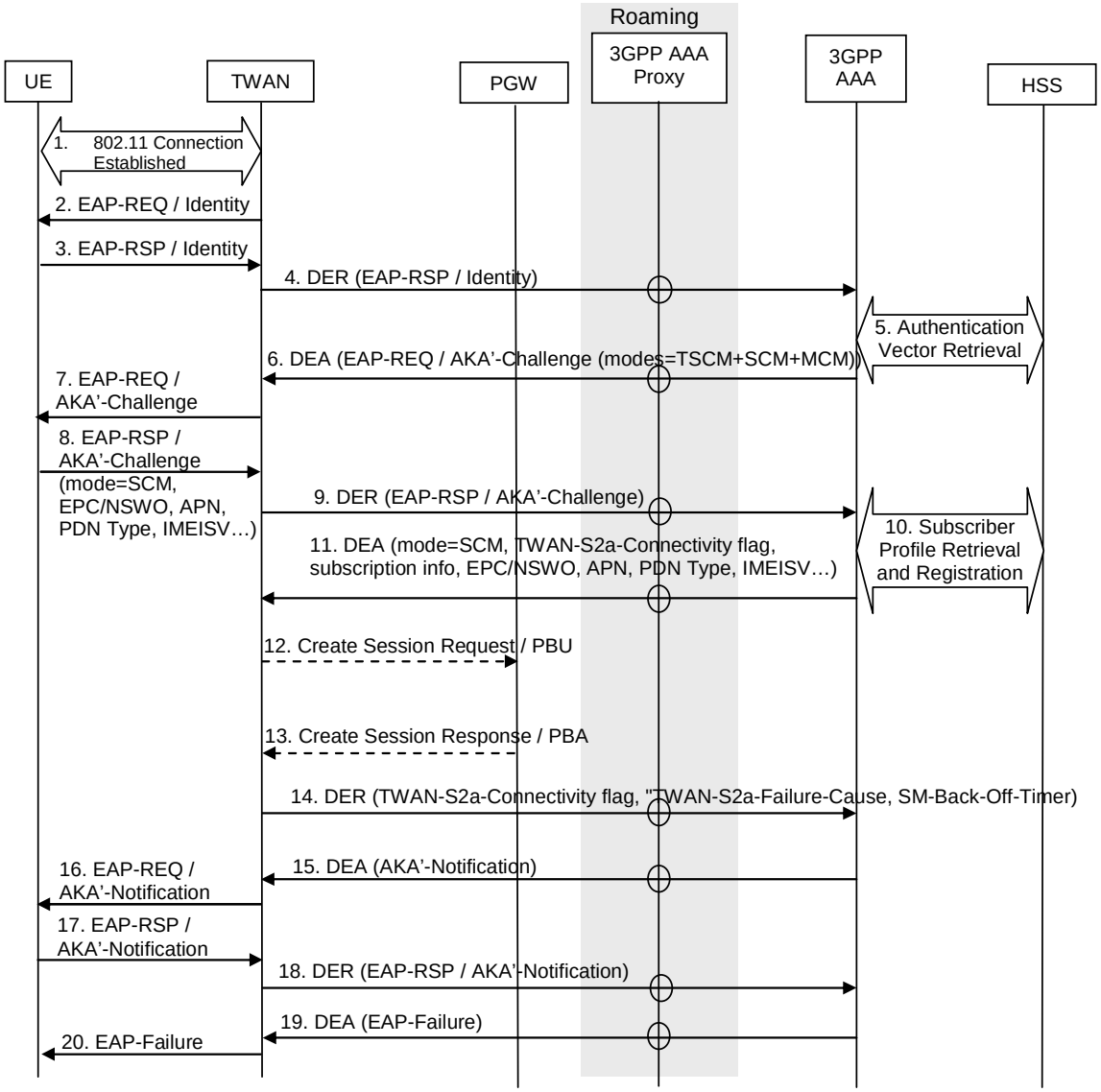

Figure Annex A.2-2: TWAN Authentication and Authorization Procedure for SCM and EPC routed access – UE request rejected with a Session Management back-off timer.

1. to 11. Same as Figure Annex A.2-1.

12. The TWAN sends a Create Session Request/PBU message to the PDN GW to initiate the S2a tunnel establishment, or skips this step and goes directly to step 14 if it is already aware of an overload condition for the requested APN and the UE request cannot be served by another PGW and if it decides to reject this UE request.

13. The PDN GW rejects the UE request, possibly including overload control information.

14. The TWAN rejects the request due to an overload condition for the APN requested by the UE. The TWAN returns the cause "insufficient resources" and provides a Session Management back-off timer to be sent to the UE. The TWAN also sets the TWAN-S2a-Connectivity Indicator in the DER-Flags AVP in the DER message to the 3GPP AAA Server. The 3GPP AAA Server ignores the EAP payload included in the DER message.

15. The 3GPP AAA Server forwards the Session Management back-off timer received from the TWAN encapsulated in the AKA'-Notification and sends the DEA message to the TWAN. The Result-Code AVP in the DEA message is set to DIAMETER_MULTI_ROUND_AUTH. The TWAN-S2a-Connectivity Indicator is not set in the DEA-Flags AVP.

16. The TWAN forwards the EAP payload to the UE.

17-18. The UE responds with an EAP-RSP/AKA'-Notification message that the TWAN forwards to the 3GPP AAA Server.

19-20. The 3GPP AAA Server sends an EAP Failure message that the TWAN forwards to the UE. The Result-Code AVP in the DEA message is set to DIAMETER_UNABLE_TO_COMPLY.

A.2.3 Call flow with IMEI check in VPLMN

Figure Annex A.2-3 describes a roaming call flow for SCM and EPC-routed access, with IMEI check performed in the VPLMN.

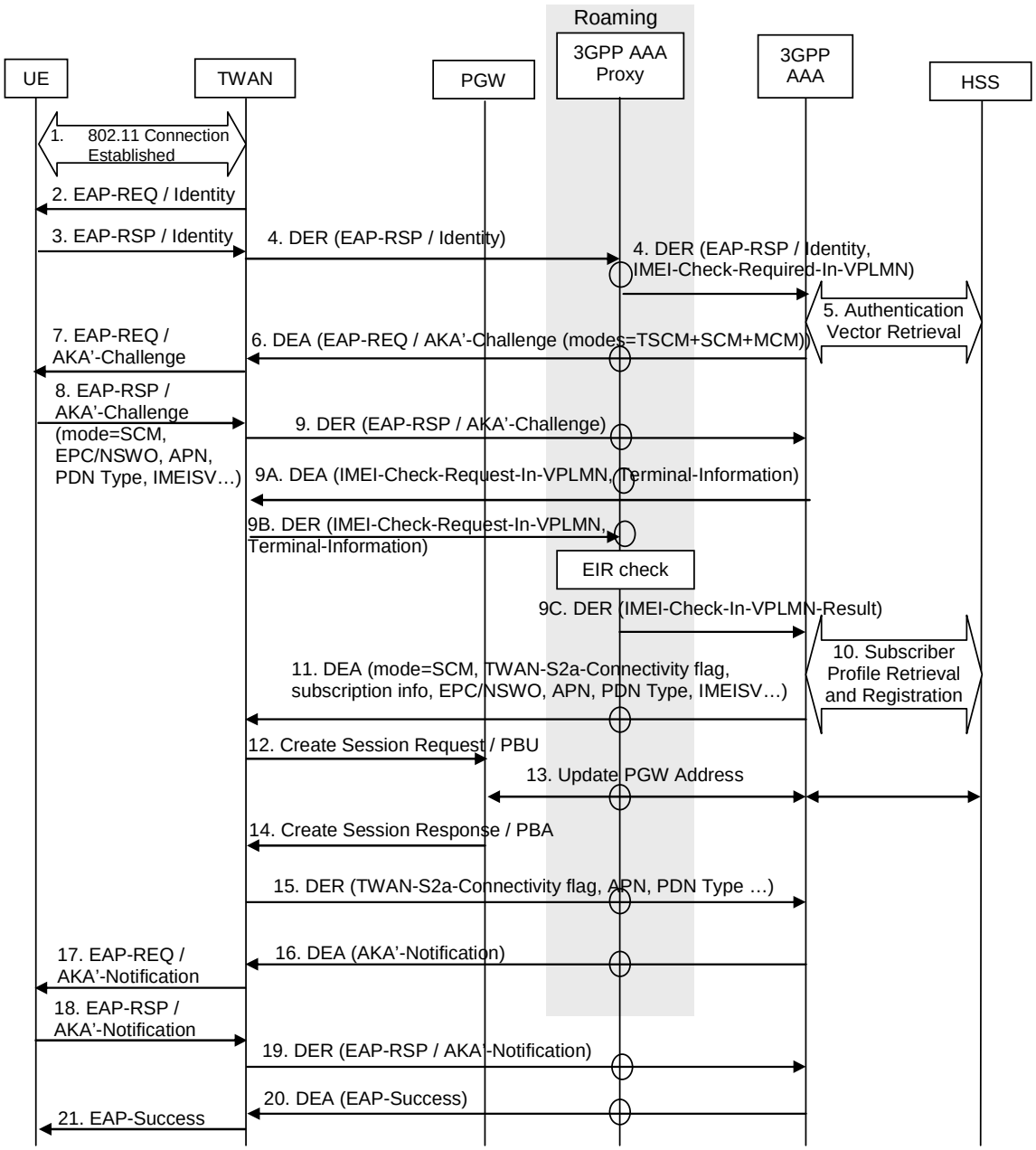

Figure Annex A.2-3: TWAN Authentication and Authorization Procedure for SCM and EPC routed access, with IMEI check performed in the VPLMN

1. to 3. Same as Figure A.2-1.

4. If IMEI check is required by operator policy, the 3GPP AAA Proxy sets the IMEI-Check-Required-In-VPLMN bit in the DER-Flags AVP.

5. to 9. Same as Figure A.2-1.

9A. The 3GPP AAA Server requests the VPLMN to perform the IMEI check by setting the IMEI-Check-Request-In-VPLMN bit in the DEA-Flags AVP and including the Terminal-Information AVP in the DEA message.

9B. The TWAN returns the IMEI-Check-Request-In-VPLMN flag in the DER-Flags AVP and the Terminal-Information AVP to the 3GPP AAA Proxy.

9C. The 3GPP AAA Proxy performs the IMEI check in the VPLMN and forwards the DER to the 3GPP AAA Server, replacing the IMEI-Check-Request-In-VPLMN bit in the DER-Flags AVP by the IMEI-Check-In-VPLMN-Result AVP.

10. to 21. Same as Figure A.2-1 if the IMEI check in VPLMN was successful.

Otherwise the 3GPP AAA Server sends an EAP Failure message that the TWAN forwards to the UE. The Result-Code AVP in the DEA message is set to DIAMETER_ERROR_ILLEGAL_EQUIPMENT.

A.3 Call Flow for MCM for EPC-routed access and/or NSWO

A.3.1 Successful call flow

Figure Annex A.3-1 describes a successful call flow for MCM, for EPC-routed access and/or Non-seamless WLAN offload.

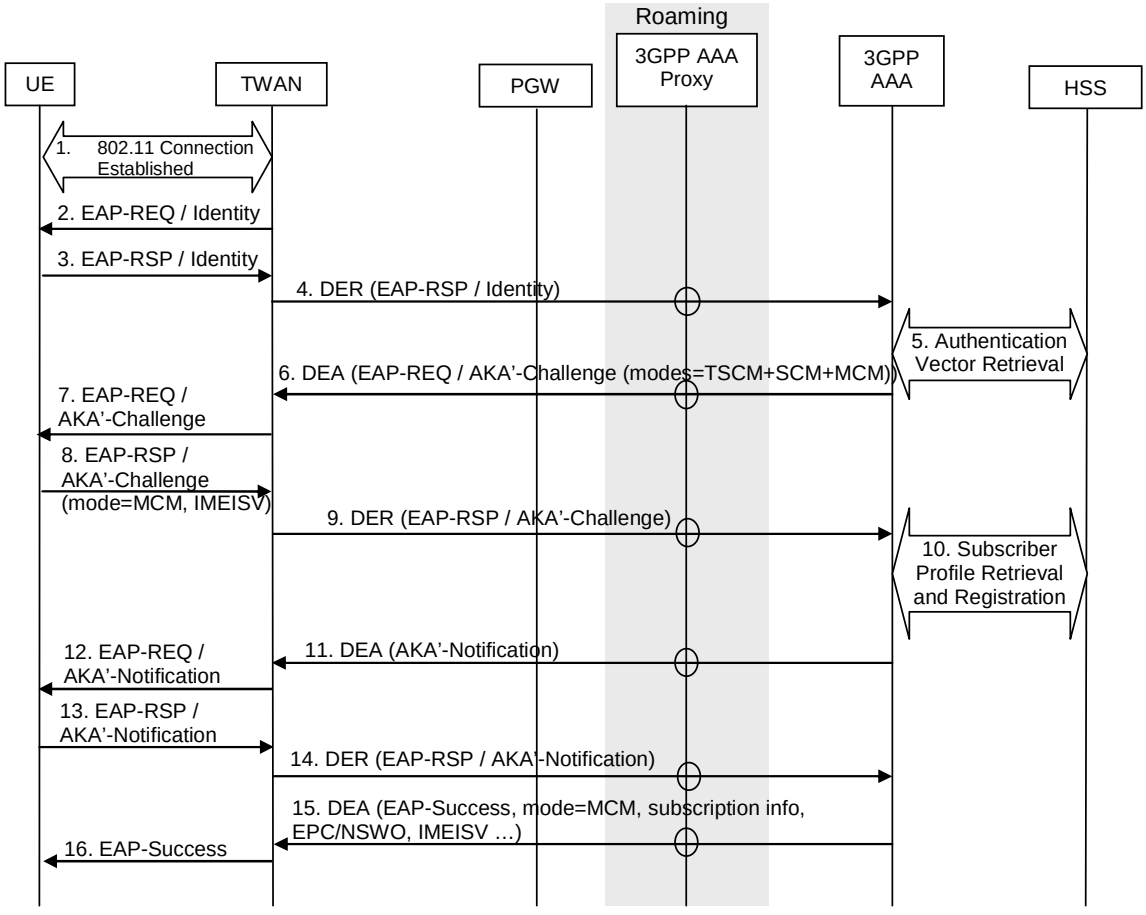

Figure Annex A.3-1: TWAN Authentication and Authorization Procedure for MCM – successful case

1. A connection is established between the UE and the TWAN, using a specific procedure based on IEEE 802.11 [40].

2. The TWAN sends an EAP Request/Identity to the UE.

3. The UE sends an EAP Response/Identity message to the TWAN.

4. The TWAN forwards the EAP payload received from the UE to the 3GPP AAA Server and also indicates the supported TWAN connection modes in the DER message. For MCM, the TWAN also provides the TWAG's control plane IPv4 and/or IPv6 addresses to be used by the UE for WLCP if the MCM is selected. The routing path may include one or several 3GPP AAA proxies for roaming case.

5. The 3GPP AAA Server retrieves authentication vectors for the UE from the HSS.

6. The 3GPP AAA Server sends an EAP Request/AKA'-Challenge in which it also indicates to the UE the TWAN connection modes supported by the network (e.g. TSCM, SCM and MCM) and, for MCM, the WLCP transport(s) supported by the TWAN (i.e. IPv4 and/or IPv6), and in which it also requests the UE to provide its Mobile Equipment Identity. The Result-Code AVP in the DEA message is set to DIAMETER_MULTI_ROUND_AUTH. The TWAN-S2a-Connectivity Indicator is not set in the DEA-Flags AVP.

7. The TWAN forwards the EAP payload to the UE.

8. The UE sends the EAP Response/AKA'-Challenge in which it also indicates the requested connection mode. In this example, the UE requests the MCM. The user's Mobile Equipment Identity is also included, if available and if requested by the 3GPP AAA Server.

9. The TWAN forwards the EAP payload to the 3GPP AAA Server.

10. If the 3GPP AAA Server successfully authentifies the UE, the 3GPP AAA Server downloads the user's subscription information from the HSS.

11. The 3GPP AAA Server includes the information required for the MCM in the AKA'-Notification as specified in 3GPP TS 24.302[26] (e.g. NSWO authorization, TWAG control plane address) and sends the DEA message to the TWAN. The Result-Code AVP in the DEA message is set to DIAMETER_MULTI_ROUND_AUTH. The TWAN-S2a-Connectivity Indicator is not set in the DEA-Flags AVP.

12. The TWAN forwards the EAP payload to the UE.

13-14. The UE responds with an EAP-RSP/AKA'-Notification message that the TWAN forwardsto the 3GPP AAA Server.

15-16. The 3GPP AAA Server sends an EAP Success message that the TWAN forwards to the UE. The Result-Code AVP in the DEA message is set to DIAMETER_SUCCESS. The DEA message also indicates to the TWAN the selected connected mode (MCM), the user's subscription information, whether the user is authorized for EPC and/or non-seamless WLAN offload, the WLCP key for WLCP signalling protection, and the user's Mobile Equipment Identity if it is available.

    Dependent on the authorizations received from the 3GPP AAA server, the UE may subsequently initiate the establishement of PDN connections to access the EPC and/or proceeed with non-seamless WLAN offload.

A.3.2 Call flow with IMEI check in VPLMN

Figure Annex A.3-x describes a roaming call flow for MCM, for EPC-routed access and/or Non-seamless WLAN offload, with IMEI check performed in the VPLMN.

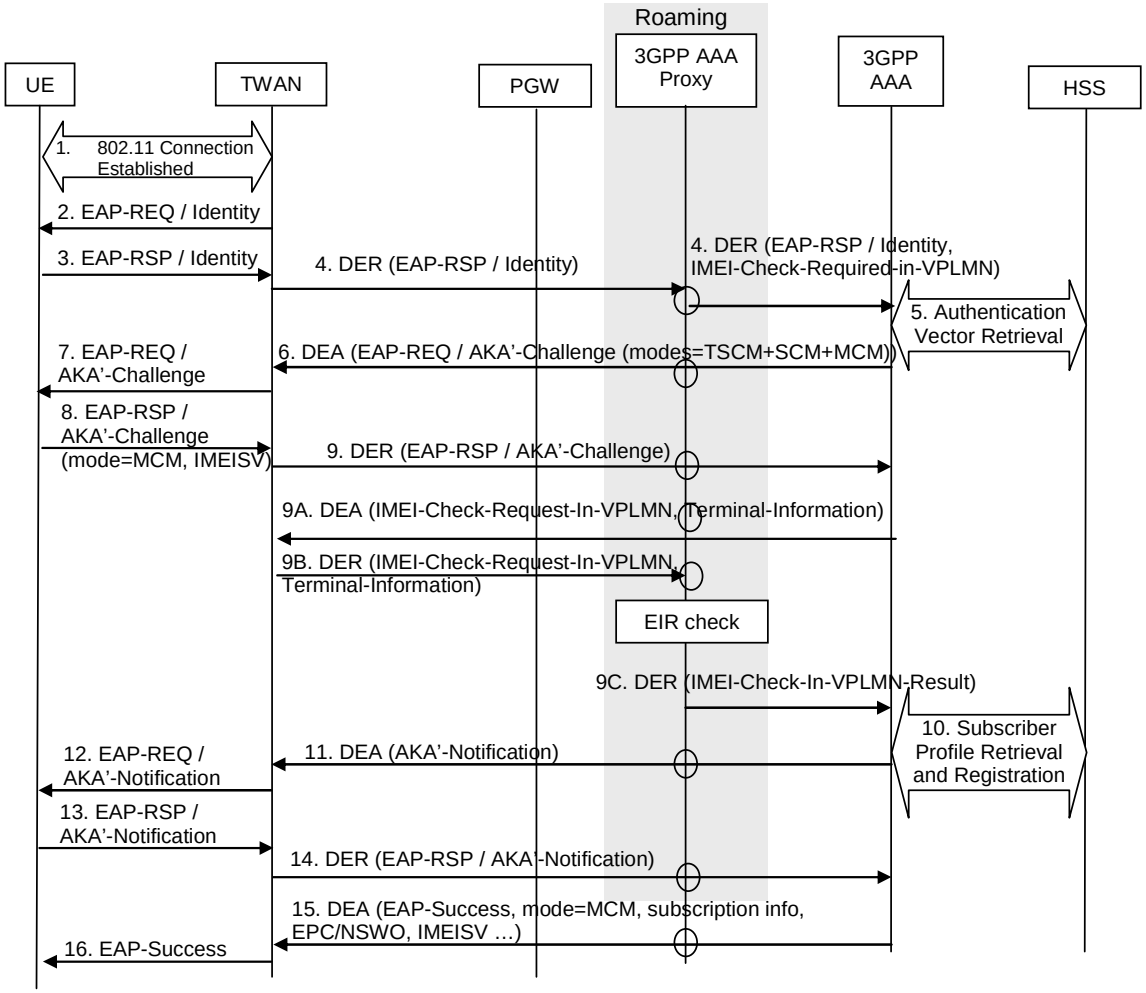

Figure Annex A.3-x: TWAN Authentication and Authorization Procedure for MCM, with an IMEI check in the VPLMN

1. to 3. Same as Figure A.3-1.

4. If IMEI check is required by operator policy, the 3GPP AAA Proxy sets the IMEI-Check-Required-In-VPLMN bit in the DER-Flags AVP.

5. to 9. Same as Figure A.3-1.

9A. The 3GPP AAA Server requests the VPLMN to perform the IMEI check by setting the IMEI-Check-Request-In-VPLMN bit in the DEA-Flags AVP and including the Terminal-Information AVP in the DEA message.

9B. The TWAN returns the IMEI-Check-Request-In-VPLMN flag in the DER-Flags AVP and the Terminal-Information AVP to the 3GPP AAA Proxy.

9C. The 3GPP AAA Proxy performs the IMEI check in the VPLMN and forwards the DER to the 3GPP AAA Server, replacing the IMEI-Check-Request-In-VPLMN bit in the DER-Flags AVP by the IMEI-Check-In-VPLMN-Result AVP.

10. to 16. Same as Figure A.3-1 if the IMEI check in VPLMN was successful.

Otherwise the 3GPP AAA Server sends an EAP Failure message that the TWAN forwards to the UE. The Result-Code AVP in the DEA message is set to DIAMETER_ERROR_ILLEGAL_EQUIPMENT.

A.4 Call Flow for TSCM and EPC-routed access

Figure Annex A.4-1 describes a successful call flow for TSCM for EPC-routed access, i.e with S2a connectivity being granted to the UE.

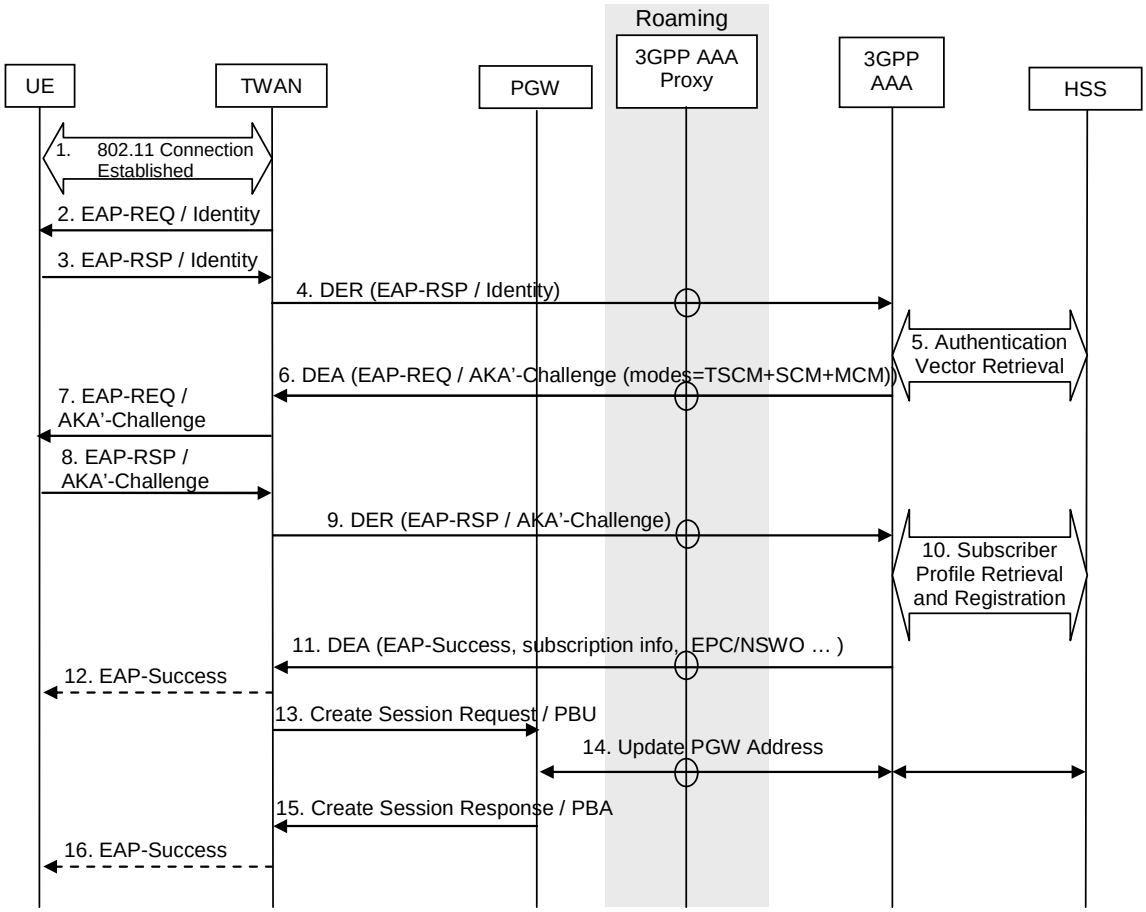

Figure Annex A.4-1: TWAN Authentication and Authorization Procedure for TSCM – successful case

1. A connection is established between the UE and the TWAN, using a specific procedure based on IEEE 802.11 [40].
2. The TWAN sends an EAP Request/Identity to the UE.
3. The UE sends an EAP Response/Identity message to the TWAN.
4. The TWAN forwards the EAP payload received from the UE to the 3GPP AAA Server and also indicates the supported TWAN connection modes in the DER message. The routing path may include one or several 3GPP AAA proxies for roaming case.
5. The 3GPP AAA Server retrieves authentication vectors for the UE from the HSS.
6. The 3GPP AAA Server sends an EAP Request/AKA'-Challenge in which it also indicates to the UE the TWAN connection modes supported by the network (e.g. TSCM, SCM and MCM). The Result-Code AVP in the DEA message is set to DIAMETER_MULTI_ROUND_AUTH. The TWAN-S2a-Connectivity Indicator is not set in the DEA-Flags AVP.
7. The TWAN forwards the EAP payload to the UE.
8. The UE sends the EAP Response/AKA'-Challenge. In this example, the UE does not signal any requested connection mode in that message, which indicates a request for TSCM.
9. The TWAN forwards the EAP payload to the 3GPP AAA Server.

10. If the 3GPP AAA Server successfully authentifies the UE, the 3GPP AAA Server downloads the user's subscription information from the HSS.

11. The 3GPP AAA Server sends an EAP Success message that the TWAN forwards to the UE in step 12 or 16. The Result-Code AVP in the DEA message is set to DIAMETER_SUCCESS. The DEA message also contains the user's subscription information, whether the user is authorized for EPC and/or non-seamless WLAN offload. The 3GPP AAA Server does not signal any selected TWAN connection mode in the DEA message, which indicates to the TWAN that TSCM is selected.

12. The TWAN forwards the EAP Success message to the UE, when using layer 3 attach trigger.

13. The TWAN sends a Create Session Request/PBU message to the PDN GW to initiate the S2a tunnel establishment (assuming EPC access has been authorized).

14. The PDN GW informs the 3GPP AAA Server/HSS of its PDN GW identity and the APN corresponding to the UE's PDN Connection.

15. The PDN GW returns a Create Session Response/PBA message to the TWAN, including the IP address(es) allocated for the UE.

16. The TWAN forwards the EAP Success message to the UE, when using layer 2 attach trigger.

Annex B (normative): Diameter overload control mechanism

B.1 General

IETF RFC 7683 [47] specifies a Diameter overload control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

Depending on regional/national requirements and network operator policy, priority traffic (e.g., MPS) shall be the last to be throttled and shall be exempted from throttling due to Diameter overload control up to the point where requested traffic reduction cannot be achieved without throttling the priority traffic.

B.2 SWx interface

B.2.1 General

The Diameter overload control mechanism is an optional feature over the SWx interface.

It is recommended to make use of IETF RFC 7683 [47] on the SWx interface where, when applied, the 3GPP AAA server shall behave as a reacting node and the HSS as a reporting node.

B.2.2 HSS behaviour

The HSS requests traffic reduction from the 3GPP AAA server when it is in an overload situation, by including OC-OLR AVP in answer commands as described in IETF RFC 7683 [47].

The HSS identifies that it is in an overload situation by implementation specific means. For example, the HSS may take into account the traffic over the SWx interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources etc.

The HSS determines the specific contents of the OC-OLR AVP in overload reports and the HSS decides when to send OC-OLR AVPs by implementation specific means.

B.2.3 3GPP AAA server behaviour

The 3GPP AAA server applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [47].

Requested traffic reduction is achieved by the 3GPP AAA server by implementation specific means. For example, it may implement message throttling with prioritization.

The 3GPP AAA server, when requested to apply traffic reduction over the SWx interface, may request traffic reduction over the interfaces (e.g STa, SWm, S6b) towards the access nodes if the Diameter overload control mechanism is supported on these interfaces.

Annex C gives guidance on message prioritisation over the SWx interface.

B.3 STa interface

B.3.1 General

The Diameter overload control mechanism is an optional feature over the STa interface.

It is recommended to make use of the IETF RFC 7683 [47] over the STa interface where, when applied, the trusted non 3GPP access network shall behave as a reacting node and the 3GPP AAA server as a reporting node.

B.3.2 3GPP AAA server behaviour

The 3GPP AAA server requests traffic reduction from the trusted non 3GPP access network when it is in an overload situation, by including OC-OLR AVP in answer commands as described in IETF RFC 7683 [47].

The 3GPP AAA server identifies that it is in an overload situation by implementation specific means. For example, the 3GPP AAA server may take into account the traffic over the STa interfaces or other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources etc.

The 3GPP AAA server determines the specific contents of the OC-OLR AVP in overload reports and the 3GPP AAA server decides when to send OC-OLR AVPs by implementation specific means.

The 3GPP AAA server, when requested to apply traffic reduction over the SWx interface, may also request traffic reduction over the STa interfaces towards the trusted access networks nodes.

B.3.3 Trusted non 3GPP access network behaviour

The trusted non 3GPP access network applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [47].

Requested traffic reduction is achieved by the trusted non 3GPP access network by implementation specific means. For example, it may implement message throttling with prioritization.

Annex C gives guidance on message prioritisation over the STa interface.

B.4 S6b interface

B.4.1 General

The Diameter overload control mechanism is an optional feature over the S6b interface.

It is recommended to make use of the IETF RFC 7683 [47] over the S6b interface where, when applied, the PDN-GW shall behave as a reacting node and the 3GPP AAA server as a reporting node.

B.4.2 3GPP AAA server behaviour

The 3GPP AAA server requests traffic reduction from the PDN-GW when it is in an overload situation, by including OC-OLR AVP in answer commands, as described in IETF RFC 7683 [47].

The 3GPP AAA server identifies that it is in an overload situation by implementation specific means. For example, the 3GPP AAA server may take into account the traffic over the S6b interfaces and other interfaces, the level of usage of internal resources (CPU, memory), the access to external resources etc.

The 3GPP AAA server determines the specific contents of the OC-OLR AVP in overload reports and when the 3GPP AAA server decides when to send OC-OLR AVPs by implementation specific means.

The 3GPP AAA server, when requested to apply traffic reduction over the SWx interface, may also request traffic reduction over the S6b interfaces towards the PDN-GWs.

B.4.3 PDN-GW behaviour

The PDN-GW applies required traffic reduction received in answer commands to subsequent applicable requests, as per IETF RFC 7683 [47].Requested traffic reduction is achieved by the PDN-GW by implementation specific means. For example, it may implement message throttling with prioritization.

Annex C gives guidance on message prioritisation over the S6b interface.

B.5 SWa Interface

B.5.1 General

The Diameter overload control mechanism is an optional feature over the SWa interface.

It is recommended to make use of the IETF RFC 7683 [47] over the SWa interface where, when applied, the untrusted non-3GPP access network shall behave as a reacting node and the 3GPP AAA server as a reporting node.

B.5.2 3GPP AAA server behaviour

The 3GPP AAA server behaviour is the same as described in clause B.3.2 for STa by replacing:

- trusted non 3GPP access network by untrusted non 3GPP access network;
- STa by SWa.

B.5.3 untrusted non-3GPP access network behaviour

The untrusted non-3GPP access network behaviour is the same as described in clause B.3.3 for STa by replacing:

- trusted non 3GPP access network by untrusted non 3GPP access network;
- STa by SWa.

Annex C gives guidance on message prioritisation over the SWa interface.

B.6 SWm Interface

B.6.1 General

The Diameter overload control mechanism is an optional feature over the SWm interface.

It is recommended to make use of the IETF RFC 7683 [47] over the SWm interface where, when applied, the ePDG shall behave as a reacting node and the 3GPP AAA server as a reporting node.

B.6.2 3GPP AAA server behaviour

The 3GPP AAA server behaviour is the same as described in clause B.3.2 for STa by replacing

- trusted non 3GPP access network by ePDG;
- STa by SWm.

B.6.3 ePDG behaviour

The ePDG behaviour is the same as described in clause B.3.3 for STa by replacing:

- trusted non 3GPP access network by ePDG;
- STa by SWm.

Annex C gives guidance on message prioritisation over the SWm interface.

Annex C (Informative): Diameter overload control node behaviour

C.1 Introduction

Annex C gives guidance on the Diameter overload control node behaviours regarding message prioritisation over non 3GPP access interfaces.

C.2 Message prioritization over SWx

This clause gives an analysis of possible behaviours of the 3GPP AAA server regarding message prioritisation as guidance and for an informative purpose.

When the HSS is overloaded, the 3GPP AAA server will receive overload reports from the HSS requesting a reduction of the requests sent by the 3GPP AAA server. This will apply to MAR and SAR requests.

The 3GPP AAA server can consider some messages with a lower or a higher priority; lower priority messages will be candidates for throttling before higher priority messages.

The 3GPP AAA server can take into account if it has already registered the user:

- Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, when the 3GPP AAA Server has to apply traffic reduction;
- if the user is not already registered in the 3GPP AAA server and the user is not establishing a PDN connection for emergency services, the 3GPP AAA server gives a lower priority to the MAR command to be sent to the HSS. This will correspond to the following cases:
  - the user is not registered for non 3GPP access in the HSS and is doing an attach on a non 3GPP access;
  - the user is not registered for non 3GPP access in the HSS and is doing an handover from a 3GPP access; if the MAR command is throttled, the PDN connection will be then maintained in the 3GPP access;
  - the user is registered in the HSS but with another 3GPP AAA server, apart a restoration case (see further), this relates to a new session. There is nevertheless a limitation for an inter RAT mobility between non 3GPP accesses when such a MAR is throttled, this is considered as acceptable;
  - after a not throttled and successful MAR, the subsequent requests (SARs) have a higher priority, otherwise it would mean that the initial MAR command processed by the (overloaded) HSS has been useless. An example is the call flow described in Annex C;
  - if the user is registered in the 3GPP AAA server, the 3GPP AAA server gives a higher priority to the MAR or SAR commands to be sent to the HSS as to maintain the service to the user; nevertheless, if a SAR indicates a PGW_UPDATE and is related to an additional Diameter session over S6b for the user, so to establish an additional PDN connection, a lower priority may be given to this SAR;
- in a restoration procedure due to the failure of the old 3GPP AAA server, the new 3GPP AAA server is informed of such a restoration procedure by the presence of the AAA-Failure-Indication AVP in the request received from the access. As restoration procedures may be a source of a high signalling traffic and contribute to a HSS overload, the new 3GPP AAA server may give a lower priority to such MAR messages;
- the deregistration of the user by the 3GPP AAA server has a higher priority as releasing resources in the HSS.

C.3 Message prioritisation over STa, SWm and SWa

This clause gives an analysis of possible behaviours of the trusted non 3GPP access network over STa, of the untrusted non 3GPP access network over SWa and of the ePDG over SWm regarding message prioritisation as guidance and for an informative purpose.

In the rest of the clause, a reacting node identifies:

- a trusted non 3GPP access network over STa;
- an untrusted non 3GPP access network over SWa;
- an ePDG over SWm.

As applying Diameter overload control over SWm and SWa may overlap, this is an operator policy to apply Diameter overload control either on SWm or on SWa or on both.

When the 3GPP AAA server is overloaded, the reacting node will receive overload reports from the 3GPP AAA server requesting a reduction of requests sent by the reacting node. This will apply to DER, STR (and also AAR for STa and SWm) commands.

The reacting node can consider some messages with a lower or a higher priority; lower priority messages will be candidates for throttling before higher priority messages. The reacting node can take into account the following considerations:

- Diameter requests related to PDN connections for emergency services have the highest priority. Depending on regional/national requirements and network operator policy, these Diameter requests are the last to be throttled, when the reacting node has to apply traffic reduction;
- if the user has no existing context in the reacting node and the user is not establishing a PDN connection for emergency services, the reacting node gives a lower priority to authentication and authorisation procedures, so to DER commands. This avoids adding new users on the 3GPP AAA server. There is nevertheless a consequence in limiting an inter RAT mobility between non 3GPP accesses when such a DER is throttled, this is considered as acceptable;
- if the initial request was not throttled, the subsequent requests have a higher priority, otherwise it would mean that the initial request processed by the (overloaded) 3GPP AAA server has been useless. An example is the call flow described in Annex A.2 for STa;
- If the user has an existing context in the reacting node, new requests have a higher priority so to maintain the service to the user;
- DER Requests (and also AAR for STa) resulting from the reception of a re-authentication re-authorisation procedure (or also re-authorisation procedure over STa) from the 3GPP AAA server have a higher priority, so to maintain the service to the user;
- The trusted non 3GPP access network has the possibility (see 5.1.2.3.1clause), at any time, to send a AAR command for check if there is any modification in the user authorization parameters previously provided by the 3GPP AAA Server. The trusted non 3GPP access network may defer such AAR requests to diminish the traffic without impacting the service to the user;
    - Session termination procedures initiated by the reacting node may have a higher priority as releasing resources in the 3GPP AAA server.

C.4 Message prioritization over S6b

This clause gives an analysis of possible behaviours of the PDN-GW regarding message prioritisation as guidance and for an informative purpose.

When the 3GPP AAA server is overloaded, the PDN-GW will receive overload reports from the 3GPP AAA server requesting a reduction of requests sent by the PDN-GW. This will apply to AAR and STR commands.

The PDN-GW can consider some messages with a lower or a higher priority; lower priority messages will be candidates for throttling before higher priority messages.

Following considerations can be taken into account:

- An important point to consider is that UEs accessing the PDN-GW via S2a or S2b have already been previously authorized to use the non 3GPP access (i.e. via STa or SWm or SWa). The AAR command over S6b following this initial authorisation has a higher priority, otherwise, if the AAR is throttled, it would mean that the initial authorisation procedure (and its process by the 3GPP AAA server) has been useless;

- An exception is in the Multi Connection Mode (MCM) (described in 3GPP TS 23.402 [3]), where after a first PDN connection being established, the UE requests the establishment of additional PDN connections. As the priority, when overload in the 3GPP AAA server, is to maintain the existing service in preference to setting up new services for the user, such AAR commands over S6b may have a lower priority;

- Traffic reduction over the STa or SWm or SWa interfaces with the throttling of new authentication authorisation procedures, results in diminishing requests for new PDN connections to the PDN-GW and diminishing the traffic over S6b;

- regarding the 3GGP AAA Server behaviour, it is better to request traffic reduction over the STa or SWm or SWa interfaces than over the S6b interface, so following the principle to request the traffic reduction as early and as close as possible to the traffic source (i.e. the UE);

- AAR Requests resulting from the reception of a re-authorisation procedure from the 3GPP AAA server have a higher priority, so to maintain the service to the user;

- the session termination procedures over S6b initiated by the PDN-GW resulting from a UE request may have a higher priority as releasing resources in the 3GPP AAA server.

Annex D (normative): Diameter message priority mechanism

D.1 General

IETF RFC 7944 [53] specifies a Diameter routing message priority mechanism that allows Diameter nodes to indicate the relative priority of Diameter messages. With this information, other Diameter nodes may leverage the relative priority of Diameter messages into routing, resource allocation, set the DSCP marking for transport of the associated Diameter message, and also abatement decisions when overload control is applied.

D.2 SWa, STa, SWd, SWm, SWx, S6b interfaces

The Diameter message priority mechanism is an optional feature which may apply on one or several of the SWa, STa, SWd, SWm, SWx, S6b interfaces.

It is recommended to make use of IETF RFC 7944 [53] over the SWa, STa, SWd, SWm, SWx, S6b interfaces of an operator network when the overload control defined in Annex C is applied on these interfaces.

A 3GPP functional entity supporting the Diameter message priority mechanism over an interface listed above shall comply with IETF RFC 7944 [53].

A 3GPP functional entity sending a request shall determine the required priority according to its policies. When priority is required, it shall include the DRMP AVP indicating the required priority level in the request it sends, and shall prioritise the request according to the required priority level.

When the 3GPP functional element receives the corresponding response, it shall prioritise the received response according to the priority level received within the DRMP AVP if present in the response, otherwise according to the priority level of the corresponding request.

When a 3GPP functional entity receives a request, it shall handle the request according to the received DRMP AVP priority level. For the response, it may modify the priority level received in the DRMP AVP according to its policies and shall handle the response according to the required priority level. If the required priority level is different from the priority level received in the request, it shall include the DRMP AVP in the response.

If:

- a 3GPP functional entity supports using the Diameter message priority mechanism for DSCP marking purposes,
- the transport network utilizes DSCP marking, and
- message-dependant DSCP marking is possible for the protocol stack transporting Diameter,

then the 3GPP functional entity shall set the DSCP marking for transport of the request or response according to the required priority level.

Diameter requests related to high priority traffic (e.g, MPS, emergency) shall contain a DRMP AVP with a high priority of which the level value is operator dependent.

When not-explicitly requested, the inclusion and priority value of the DRMP AVP in Diameter messages are implementation specific.

Annex E (informative): Untrusted WLAN authentication and authorization procedure

E.1 General

This clause provides example call flows for the Untrusted WLAN authentication and authorization procedure.

This Annex is informative and the normative descriptions in this specification and in 3GPP TS 33.402 [19] prevail over the descriptions in this Annex if there is any difference.

See clause 8.2.2 of 3GPP TS 33.402 [19] for details on the IKEv2 and EAP-AKA procedures. This clause focuses on the SWm, S6b and SWx signalling interactions.

E.2 Successful call flow

Figure Annex E.2-1 describes a successful Untrusted WLAN authentication and authorization call flow.

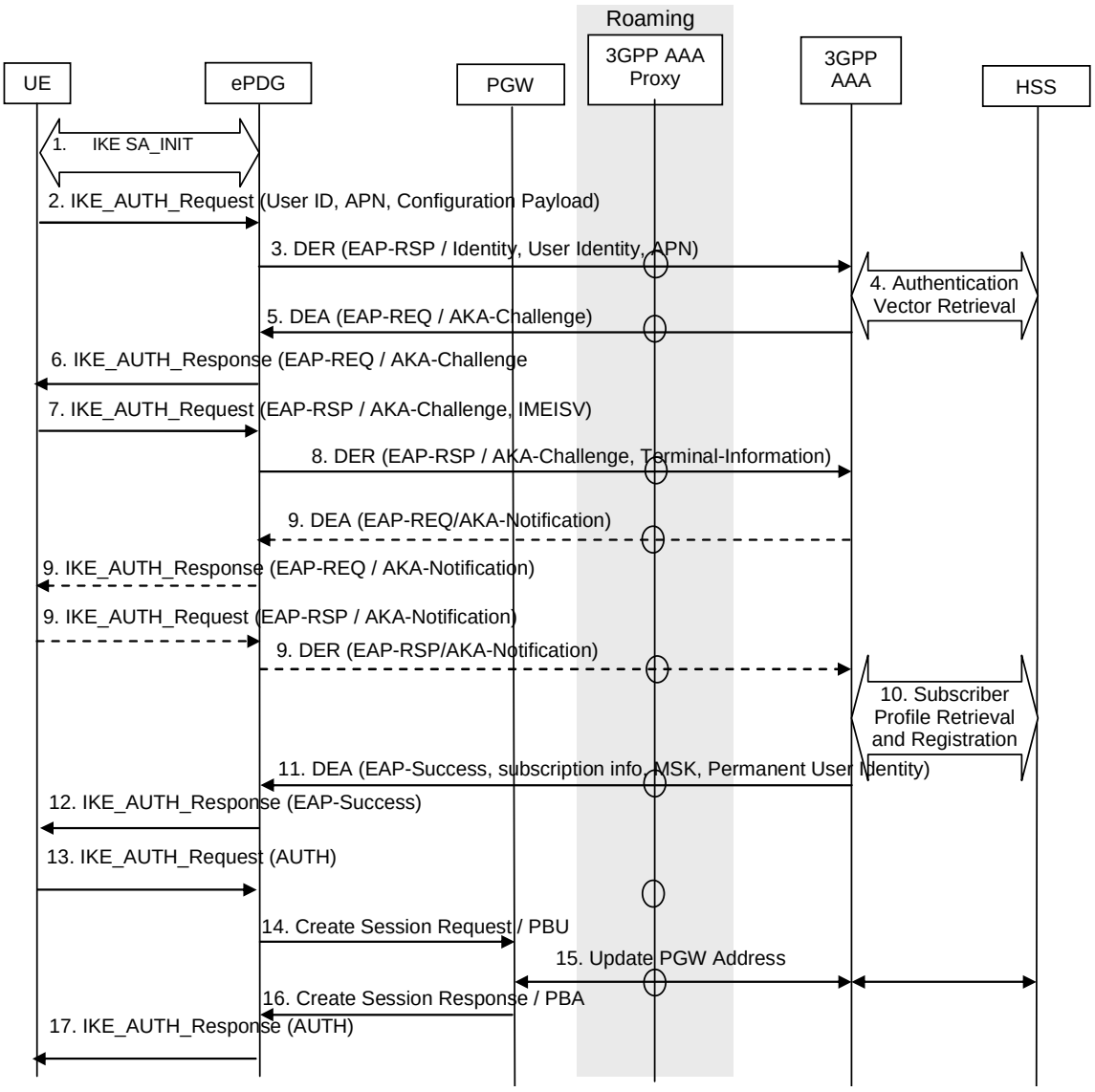

Figure Annex E.2-1: Untrusted WLAN Authentication and Authorization Procedure – successful case

3. The ePDG sends the EAP-RSP/Identity payload to the 3GPP AAA Server and also indicates the user identity and requested APN, if received from the UE.
4. The 3GPP AAA Server retrieves authentication vectors for the UE from the HSS.
5. The 3GPP AAA Server sends an EAP Request/AKA-Challenge.
6. The ePDG forwards the EAP payload to the UE and also requests the UE to provide its Mobile Equipment Identity if required.
8. The ePDG forwards the EAP payload to the 3GPP AAA Server. The user's Mobile Equipment Identity is also included, if available.
9. If dynamic IP mobility selection is executed, the selected mobility mode is sent to the UE in an AKA-Notification request.
10. If the 3GPP AAA Server successfully authentifies the UE, the 3GPP AAA Server downloads the user's subscription information from the HSS.
11. If the 3GPP AAA Server authorizes the access for the UE, the 3GPP AAA Server sends an EAP Success message that the ePDG forwards to the UE. The Result-Code AVP in the DEA message is set to DIAMETER_SUCESS. The subscription information, keying material and permanent user identity are also provided to the ePDG.
14. The ePDG sends a Create Session Request/PBU message to the PDN GW to initiate the S2b tunnel establishment.
15. The PDN GW informs the 3GPP AAA Server/HSS of its PDN GW identity and the APN corresponding to the UE's PDN Connection.
16. The PDN GW returns a Create Session Response/PBA message to the ePDG, including the IP address(es) allocated for the UE.
17. The IKEv2 negotiation completes. The ePDG provides the UE IP address to the UE.

E.3 Call flow with IMEI check in VPLMN

Figure Annex E.3-1 describes a roaming call flow, with IMEI check performed in the VPLMN.

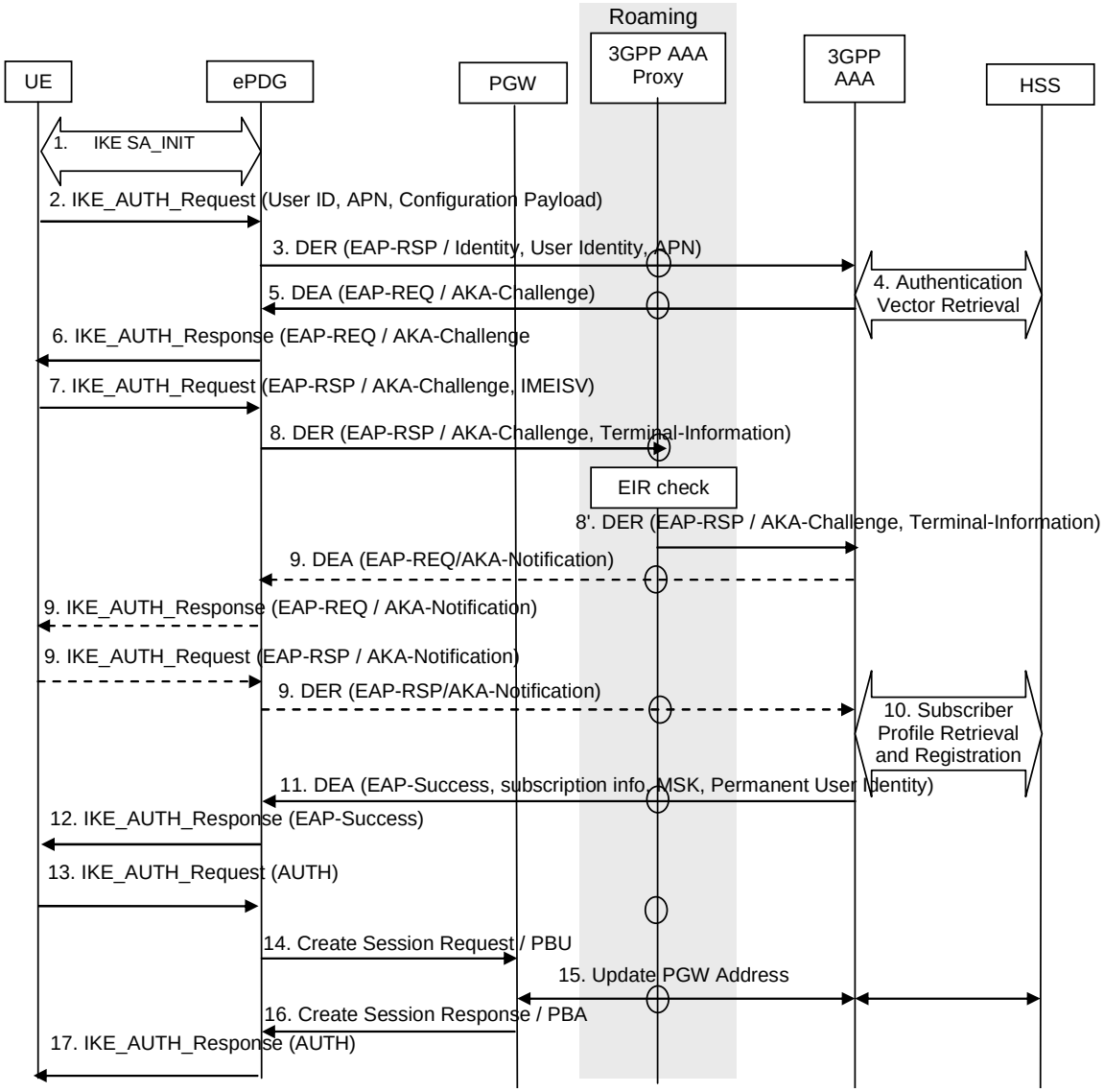

Figure Annex E.3-1: Untrusted WLAN Authentication and Authorization Procedure, with IMEI check performed in the VPLMN

1. to 5. Same as Figure E.2-1.

6. If IMEI check is required by operator policy, the ePDG requests the UE to provide its Mobile Equipment Identity.

7. Same as Figure E.2-1.

8. The ePDG includes the Terminal-Information AVP in the DER command. If IMEI check is required by operator policy, the 3GPP AAA Proxy performs the IMEI check in the VPLMN. If the IMEI check allows to continue the authentication and authorization procedure, the 3GPP AAA Proxy forwards the DER to the 3GPP AAA Server (as shown in this figure). Otherwise the 3GPP AAA Proxy responds to the ePDG with the Experimental-Result-Code DIAMETER_ERROR_ILLEGAL_EQUIPMENT and sends a SWm Session Termination Request towards the 3GPP AAA Server.

9 to 17. Same as Figure E.2-1 if the IMEI check in VPLMN was successful.

Annex F (normative): Diameter load control mechanism

F.1 General

IETF RFC 8583 [54] specifies a Diameter overload control mechanism which includes the definition and the transfer of related AVPs between Diameter nodes.

F.2 SWx interface

F.2.1 General

The Diameter load control mechanism is an optional feature over the SWx interface.

It is recommended to make use of IETF RFC 8583 [54] on the SWx interface where, when applied, the 3GPP AAA server shall behave as a reacting node and the HSS as a reporting node.

F.2.2 HSS behaviour

The HSS may report its current load by including a Load AVP of type HOST in answer commands as described in IETF RFC 8583 [54].

The HSS calculates its current load by implementation specific means. For example, the HSS may take into account the traffic over the SWx interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The HSS determines when to send Load AVPs of type HOST by implementation specific means.

F.2.3 3GPP AAA server behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the 3GPP AAA server may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF RFC 8583 [54].

F.3 STa interface

F.3.1 General

The Diameter load control mechanism is an optional feature over the STa interface.

It is recommended to make use of the IETF RFC 8583 [54] over the STa interface where, when applied, the trusted non 3GPP access network shall behave as a reacting node and the 3GPP AAA server as a reporting node.

F.3.2 3GPP AAA server behaviour

The 3GPP AAA server may report its current load by including a Load AVP of type HOST in answer commands as described in IETF RFC 8583 [54].

The 3GPP AAA server calculates its current load by implementation specific means. For example, the 3GPP AAA server may take into account the traffic over the STa interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The 3GPP AAA server determines when to send Load AVPs of type HOST by implementation specific means.

F.3.3 Trusted non 3GPP access network behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the Trusted non 3GPP access network may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF RFC 8583 [54].

F.4 S6b interface

F.4.1 General

The Diameter load control mechanism is an optional feature over the S6b interface.

It is recommended to make use of the IETF RFC 8583 [54] over the S6b interface where, when applied, the PDN-GW shall behave as a reacting node and the 3GPP AAA server as a reporting node.

F.4.2 3GPP AAA server behaviour

The 3GPP AAA server may report its current load by including a Load AVP of type HOST in answer commands as described in IETF RFC 8583 [54].

The 3GPP AAA server calculates its current load by implementation specific means. For example, the 3GPP AAA server may take into account the traffic over the S6b interface or other interfaces, the level of usage of internal resources (e.g. CPU, memory), the access to external resources, etc.

The 3GPP AAA server determines when to send Load AVPs of type HOST by implementation specific means.

F.4.3 PDN-GW behaviour

When performing next hop Diameter Agent selection for requests that are routed based on realm, the PDN-GW may take into account load values from Load AVPs of type PEER received from candidate next hop Diameter nodes, as per IETF RFC 8583 [54].

F.5 SWa Interface

F.5.1 General

The Diameter load control mechanism is an optional feature over the SWa interface.

It is recommended to make use of the IETF RFC 8583 [54] over the SWa interface where, when applied, the untrusted non-3GPP access network shall behave as a reacting node and the 3GPP AAA server as a reporting node.

F.5.2 3GPP AAA server behaviour

The 3GPP AAA server behaviour is the same as described in clause F.3.2 for STa by replacing:

- trusted non 3GPP access network by untrusted non 3GPP access network;
- STa by SWa.

F.5.3 untrusted non-3GPP access network behaviour

The untrusted non-3GPP access network behaviour is the same as described in clause F.3.3 for STa by replacing:

- trusted non 3GPP access network by untrusted non 3GPP access network;
- STa by SWa.

F.6 SWm Interface

F.6.1 General

The Diameter load control mechanism is an optional feature over the SWm interface.

It is recommended to make use of the IETF RFC 8583 [54] over the SWm interface where, when applied, the ePDG shall behave as a reacting node and the 3GPP AAA server as a reporting node.

F.6.2 3GPP AAA server behaviour

The 3GPP AAA server behaviour is the same as described in clause F.3.2 for STa by replacing

- trusted non 3GPP access network by ePDG;
- STa by SWm.

F.6.3 ePDG behaviour

The ePDG behaviour is the same as described in clause F.3.3 for STa by replacing:

- trusted non 3GPP access network by ePDG;
- STa by SWm.

Annex G (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Cat	Subject/Comment	New
2008-12	CT#42	CP-080717				V2.0.0 approved in CT#42	8.0.0
2009-03	CT#43	CP-090051	0002	2		Clarification on QoS Resource on S6b	8.1.0
		CP-090051	0003	1		Context Identifier for Update or Removal of PDN GW	
		CP-090051	0007	-		Clarification on the S6b Authorization Procedure for DSMIPv6	
		CP-090051	0009	-		Clarification on DHCPv6/IKEv2 based HA discovery	
		CP-090051	0010	1		Clarification on AAA server authentication/authorization	
		CP-090051	0011	1		Difference of S6b and H2	
		CP-090051	0013	1		STR on HSS/AAA initiated detach over STa	
		CP-090051	0014	1		STR on 3GPP AAA Server initiated detach over SWm	
		CP-090051	0015	1		STR on 3GPP AAA Server initiated detach over S6b	
		CP-090051	0016	1		Multiple 3GPP AAA identities	
		CP-090051	0019	1		User-Name AVP contains only the IMSI	
		CP-090051	0020	-		Removal of APN-Barring-Type Reference	
		CP-090051	0021	1		Charging AVPs	
		CP-090051	0022	1		MIP6-Agent-Info Definition and Usage	
		CP-090051	0023	1		REAUTHENTICATION_FAILURE Correction	
		CP-090051	0025	1		Definition of Server-Assignment-Type values	
		CP-090051	0026	-		Multiple Occurrences of SIP-Auth-Data-Item AVP	
		CP-090051	0028	1		Using MIP6-Agent-Info for SGW address	
		CP-090051	0029	1		MIP6-Agent-Info corrections	
		CP-090051	0030	1		Trace activation in PDN GW over the SWx and S6b interfaces	
		CP-090051	0031	1		Signalling VPLMN Trust of non-3GPP AN	
		CP-090051	0033	-		Corrections in Visited Network Identifier definitions	
		CP-090051	0034	2		Service Authorization Information update on S6b when using DSMIP	
		CP-090051	0035	4		STa/SWa clarifications	
		CP-090051	0036	1		IP address authorization corrections	
		CP-090051	0037	2		SWm Authentication Correction	
		CP-090051	0039	1		SWm corrections - others	
		CP-090051	0040	3		SWm Service Authorization Information Update corrections	
		CP-090051	0041	5		Combined Authentication and authorization procedure on SWm	
		CP-090051	0042	2		S6b related corrections	
		CP-090051	0044	2		Corrections to S6b/HA clause 9	
		CP-090039	0045	3		User to HSS resolution	
		CP-090051	0080	1		Corrections to STR procedures for AAA_UNKNOWN_SESSION_ID	
		CP-090051	0081	1		Corrections to S6b STR procedures	
		CP-090236	0082	1		PDN GW update for Wildcard APN	
		CP-090051	0083	-		RFC 5447 References	
2009-06	CT#44	CP-090289	0084	1		Use of Access-Restriction-Data AVP	8.2.0
		CP-090289	0085	-		Difference between S6b and H2	
		CP-090289	0086	1		Corrections to 29.273	
		CP-090289	0087	1		Inclusion of static IP address	
		CP-090289	0088	1		Home Agent discovery	
		CP-090289	0090	-		Incorrect command for user profile updates	
		CP-090289	0092	1		Home Agent discovery	
		CP-090289	0093	1		Formatting of APN in Service-Selection AVP	
		CP-090289	0094	-		Update of AVP Codes	
		CP-090289	0096	1		STa/SWa separation correction	
		CP-090289	0097	-		SWa corrections	
		CP-090289	0098	1		STa re-authorization and re-authentication	
		CP-090289	0101	2		SWa re-authentication	
		CP-090289	0102	1		Adding APN-OI-Replacement	
		CP-090289	0103	2		HA reallocation clarification	
2009-09	CT#45	CP-090537	0105	2		Correction on APN-OI-Replacement	8.3.0
		CP-090537	0106	-		Correction on the Description of Mobility Features over S6b	
		CP-090537	0111	-		EAP-AKA' IETF RFC Reference	
		CP-090537	0112	-		Removal of Remaining Editor Notes	
		CP-090537	0113	1		MIP6_SPLIT flag removal	
		CP-090537	0108	3		Support of optimized idle mode mobility	
		CP-090537	0115	-		E-UTRAN - eHRPD Connectivity and Interworking Reference	
		CP-090537	0116	2		Detailed behaviour in error cases	
		CP-090537	0118	1		Application IDs	
		CP-090537	0119	-		Service-Selection AVP Code	

		CP-090537	0120	-		PDN-Type AVP	
		CP-090537	0121	1		Clarifications on PGW Handling on S6b/H2	
2009-09	CT#45	CP-090562	0117	1		Emergency Support in AAA interfaces	9.0.0
2009-12	CT#46	CP-090793	0122	2		APN level APN-OI-Replacement	
		CP-090774	0126	3		Correction of Allowed PDN Types	9.1.0
		CP-090774	0128	2		Incorrect HSS behaviour on deregistration	
		CP-090774	0130	2		MIP6 Agent Info	
		CP-090774	0132			Nonce	
		CP-090774	0136	-		3GPP AAA Server detailed behaviour at HSS Initiated Update of User Profile	
		CP-090774	0140	2		Static PDN GW	
		CP-090787	0141			Removal of Definition of APN-Configuration	
		CP-090774	0143	1		PGW deregistration via S6b	
		CP-090774	0145	1		Add Supported-Features AVP to STa/SWa	
		CP-090774	0147	-		Add Supported-Features AVP to SWm	
		CP-090774	0149	-		Add Supported-Features AVP to SWx	
		CP-090774	0151	-		Add Supported-Features AVP to S6b	
		CP-090774	0153	1		Correction of Application ID	
		CP-090774	0155	1		Error Handling	
		CP-090774	0157	-		HSS/AAA-Initiated Disconnection	
2010-03	CT#47	CP-10024	0163	1		Correction in Subscription-ID	9.2.0
		CP-10024	0165	-		NAI decoration and realm-based routing clarifications	
		CP-10024	0167	-		IETF References update	
		CP-10024	0169	-		Permanent User Identity	
		CP-10024	0171	1		Static PDN GW	
		CP-10024	0173	-		QoS AVP Codes	
		CP-10024	0175	-		Indication of PLMN ID of the selected PGW	
		CP-10044	0176	-		Context-Identifier in Registration Request	
2010-06	CT#48	CP-100290	0179	1		Corrections on Session Termination between the PGW and the AAA	9.3.0
		CP-100277	0180	-		Corrections to implementation of CR 128 and CR 175	
		CP-100277	0181	-		PGW Identity upon successful authorization on SWm	
2010-06	CT#48	CP-100443	0184	-		Ambiguity of Presence Conditions of IEs and AVP ABNF	9.4.0
		CP-100457	0188	-		IETF References	
		CP-100457	0189	1		SWm missing AVPs	
2010-09	CT#49	CP-100603	0187	1		Removal of Invalid Reference	10.0.0
2010-12	CT#50	CP-100679	0197	1		Correcting PDN GW behaviour for S6b	10.1.0
		CP-100698	0194	1		Update APN and PDN GW in the 3GPP AAA Server on SWx	
		CP-100698	0195	1		Update APN and PDN GW in Non-3GPP IP Access over the STa & SWm interfaces	
		CP-100686	0196	3		SWm and S6b procedures for GTP based S2b	
		CP-100707	0200	-		MIP6 Feature Vector flags assignment	
		CP-100707	0203	-		SWx AVP Bits Definition	
		CP-100707	0206	-		Visited-Network-Identifier Data Type	
2011-03	CT#51	CP-110051	0210	1		Usage of Auth-Request-Type in response messages	10.2.0
		CP-110073	0208	2		Correction on PGW PLMN ID	
2011-06	CT#52	CP-110359	0214	1		Trace-Depth-List correction	10.3.0
		CP-110359	0217	1		MIPv4 security parameters on the STa and S6b interfaces	
		CP-110359	0221	1		PGW Update	
		CP-110359	0223	1		APN Configuration for SWx	
		CP-110360	0219	-		Authentication Timeout	
2011-12	CT#54	CP-110778	0227	1		S6b session handling after handover to 3GPP access	10.4.0
		CP-110778	0235	1		Incorrect access name on SWa	
		CP-110793	0228	5		Correction on Trust Relationship Indication	
		CP-110793	0238	-		Implementation Error of CR 196 R3	
2011-12	CT#54	CP-110812	0225	4		SWx Restoration	11.0.0
2012-03	CT#55	CP-120016	0257	1		Wrong Command Code in STa AA-Answer	11.1.0
		CP-120020	0251	2		Authorize the requested home address types	
		CP-120020	0260	-		Content of Service-Selection AVP	
		CP-120040	0245	1		Wildcard APN in the user subscription	
		CP-120040	0253	-		Permanent User Identity in SWm Authentication and Authorization Answer	
		CP-120040	0255	-		Encoding of Visited-Network-Identifier AVP	
		CP-120040	0256	-		Re-Authorization Errors	
		CP-120042	0254	1		Permanent User Identity at SWa	
		CP-120044	0240	1		PDN GW reallocation based on UE's location	
2012-06	CT#56	CP-120225	0243	3		Trust Relationship Indication	11.2.0
		CP-120238	0264	-		S6b procedures for GTP based S2a	
		CP-120247	0265	2		Missing IE in TS 29.273	
		CP-120247	0266	-		Emergency scenario for STa interface	
		CP-120247	0267	2		Visited Network Identifier	
		CP-120247	0278	1		Network Name	
		CP-120238	0268	6		STa & SWd procedures for GTP S2a & Trusted WLAN access	

		CP-120238	0269	1		Default APN for 'Trusted WLAN access'	
		CP-120238	0270	3		Informing Serving SSID to the AAA Server	
		CP-120238	0271	1		Avoiding registration of PDN-GW identity for TWAN	
		CP-120238	0275	1		Clarifications on TWAN behaviour	
		CP-120237	0273	2		PDN GW selection for S2c during tunnel establishment	
2012-09	CT#57	CP-120441	0285	-		Update of IETF draft status to RFC	11.3.0
		CP-120447	0287	2		PGW selection in eHRPD for SIPTO	
		CP-120461	0272	3		Recovering from AAA Server failure	
		CP-120474	0279	1		Transport Access Type AVP for BBAI	
		CP-120477	0280	1		NSWO-Capability & NSWO-Authorization AVPs	
		CP-120477	0281			Access Type for TWAN access	
		CP-120656	0292	1		Reference list correction to align with the corrected TS 29.212 title	
2012-12	CT#58	CP-120711	0307	1		Removal of AVP Encryption	11.4.0
		CP-120733	0293	-		Repeat information for Trusted non-3GPP access network	
		CP-120733	0300	5		Matching WLAN-ID between Selected WLAN ID and TWAN Access Info	
		CP-120733	0301	1		Update of draft-ietf-radext-ieee802ext reference	
		CP-120747	0294	-		Correction on Auth-Request-Type	
		CP-120747	0295	-		Description of Result IE	
		CP-120728	0297	2		Information Elements for SWa interface	
		CP-120728	0299	1		Session ID in the SWm Authorization procedure	
		CP-120750	0302	1		Trace Info for PGW	
		CP-120750	0303	1		Add the definition of trace-reference	
		CP-120741	0309	2		Use of Flag instead of Enumerated AVPs	
2013-03	CT#59	CP-130022	0314	2		About EAP-AKA' challenge message	11.5.0
		CP-130022	0315	1		TWAN Authorization when HE-SSID is not provided	
		CP-130022	0317	-		Missing P-Bit settings in Information Element tables	
		CP-130022	0316	-		Presence condition of PGW-ID AVP in S6b AAR command	
2013-06	CT#60	CP-130288	0313	3		New DER-S6b-flags on S6b interface	11.6.0
		CP-130288	0325	1		MIP4 supported flag	
		CP-130288	0323	1		3GPP AAA Proxy behavior	
		CP-130288	0321	1		Definition of HA-APN	
		CP-130288	0320	2		Trust relationship for PGW	
		CP-130293	0318	2		UE local IP address for SWm or S6b	
2013-06	CT#60	CP-130381	0326	1		EAP-AKA clarification	12.0.0
		CP-130381	0319	2		Clarification for Routing Policies	
2013-09	CT#61	CP-130459	0333	1		Category of Authentication Data Information Element in SWx/MAR command	12.1.0
		CP-130472	0329	2		Add 3GPP AAA Proxy detailed Behaviour on SWa	
		CP-130472	0331	1		Correction on IP Mobility Mode Selection function	
		CP-130461	0327	2		Clarification on provision of HA information for DHCP-based HA discovery on STa	
		CP-130461	0332	-		Applicability of IP Filters and Routing Policies functionality on EPC	
2013-12	CT#62	CP-130602	0351	-		EAP Payload	12.2.0
		CP-130640	0338	-		Clarification on Trust Relationship Indicator	
		CP-130640	0339	1		MIP6-Agent-Info over the S6b interface	
		CP-130640	0346	-		Clarification of M-bit handling	
		CP-130640	0354	1		Reflective QoS for BBF convergence	
		CP-130606	0341	-		IMSI for BBF in trusted S2c case	
		CP-130616	0343	4		NSWO via the trusted WLAN	
		CP-130616	0345	1		VPLMN trust relationship indicator	
		CP-130616	0356	1		EPC Access Authorization	
		CP-130633	0353	1		PGW update on SWx	
2014-03	CT#63	CP-140023	0366	1		Replacement of IETF WLAN AVPs	12.3.0
		CP-140033	0361	-		Incorrect Diameter commands	
		CP-140033	0363	1		Condition for sending APN Information	
		CP-140030	0364	1		Retrieval of Network Provided Location Information via HSS	
		CP-140033	0367	-		RAT Type correction	
2014-06	CT#64	CP-140247	0368	-		STa Authentication for Trusted WLAN access	12.4.0
		CP-140253	0369	4		IMSI for BBF convergence	
		CP-140253	0370	1		Reflective QoS in BBF architecture	
		CP-140252	0373	2		Civic Address Encoding	
		CP-140252	0377	-		TWAN-BSSID AVP re-naming	
		CP-140243	0374	3		Diameter overload over SWx	
		CP-140243	0375	3		Diameter overload over STa and S6b	
2014-09	CT#65	CP-140510	0379	2		Session Management back-off timer for UE in Single-Connection mode	12.5.0
		CP-140516	0381	2		Remove TS 23.234 from TS 29.273	
		CP-140516	0382	1		Remove TS 29.234 from TS 29.273	
		CP-140519	0383	1		Circuit ID in NetLoc-TWLAN	

2014-12	CT#66	CP-140771	0385	-		Correct wrong references to 3GPP specifications that define Diameter experimental result codes 5001 to 5005	12.6.0
		CP-140771	0397	3		Restricted RAT Types	
		CP-140784	0386	1		WLCP key for WLCP signalling protection	
		CP-140784	0387	1		TWAN authentication and authorization call flows for MCM and TSCM	
		CP-140784	0398	1		Back-off timer refers to Tw1	
		CP-140790	0389	3		Diameter Overload over SWm and SWa	
		CP-140754	0394	2		Leading Digit of User-Name AVP	
		CP-140757	0396	-		Incorrect implementation of CR on EAP-Payload	
2015-03	CT#67	CP-150021	0401	1		Usage of decorated NAI	12.7.0
		CP-150021	0404	1		Clarification of user de-registration	
2015-06	CT#68	CP-150276	0416	1		Correction of the type of the Redirect-Host AVP	12.8.0
		CP-150250	0407	-		Repeated SWm session for default APN	
2015-06						Implemented Rel-13 CRs removed (0410r1, 0417r1, 0418r1, 0405r1)	12.8.1
2015-06	CT#68	CP-150268	0410	1		The value of SM-Back-Off-Timer	13.0.0
		CP-150268	0417	1		Clarification on the S6b Service Authorization Information Update procedure for DSMIPv6	
		CP-150268	0418	1		Removing EPC before Root NAI	
		CP-150268	0405	1		PDN GW Identity	
2015-09	CT#68	CP-150455	0422	1		IMEI(SV) signalling for untrusted WLAN access	13.1.0
		CP-150455	0423	2		IMEI(SV) signalling for trusted WLAN access	
		CP-150455	0424	1		IMEI(SV) signalling during Non-3GPP IP Access Registration	
		CP-150442	0425	1		3GPP AAA Server sends an ASR command to clean up possible hanging resources	
		CP-150442	0426	3		Overlapping transaction over S6b	
		CP-150451	0427	1		Default access type for SCM	
		CP-150447	0428	-		Reference to a wrong clause in TS 23.008	
2015-12	CT#70	CP-150770	0429	5		Emergency PDN connection over untrusted WLAN access	13.2.0
		CP-150770	0430	3		Network provided WLAN Location Information for PDN connection establishment over S2b	
		CP-150764	0431	1		UE local IP address in Authentication and Authorization Request over SWm	
		CP-150780	0433	3		P-CSCF Restoration for WLAN over SWx	
		CP-150780	0434	5		Authorisation procedure with the extended P-CSCF restoration mechanism for WLAN	
		CP-150787	0435	-		Transfer of IMEI from 3GPP AAA Server to HSS over SWx	
		CP-150773	0436	3		Multiple accesses to a PDN connection not allowed for SCM	
		CP-150748	0438	-		Visited-Network-Identifier for untrusted WLAN	
		CP-150748	0443	2		Blocking TWAN access to EPC	
		CP-150782	0439	1		Handling of S6b Authorization Request without Origination Timestamp	
		CP-150846	0440	4		Diameter message priority over non 3GPP access	
		CP-150759	0444	1		Reference to DOIC updated with IETF RFC 7683	
2016-03	CT#71	CP-160035	0446	-		Remove the default access AVP	13.3.0
		CP-160042	0447	-		Extension on TWAN-S2a-Failure-Cause	
		CP-160042	0448	1		Authorize the UE requested APN	
		CP-160037	0449	-		Correction of CR implementation on Emergency PDN connection over untrusted WLAN access	
		CP-160037	0450	1		ePDG retrieval of WLAN Location Information	
		CP-160153	0452	2		Result-Codes for P-CSCF Restoration	
2016-06	CT#72	CP-160220	0453	1		RAT type not allowed	13.4.0
2016-06	CT#72	CP-160220	0454	1		Wildcard APN for SWx and S6b	13.4.0
2016-06	CT#72	CP-160220	0455	2		Clarification on the use of SAR message when AAA has no profile	13.4.0
2016-06	CT#72	CP-160220	0456	1		Wildcard authorized APN in TWAN	13.4.0
2016-06	CT#72	CP-160220	0457	2		APN information over S6b	13.4.0
2016-06	CT#72	CP-160231	0458	-		Removal of NBIFOM reference	13.4.0
2016-06	CT#72	CP-160223	0459	2		Incorrect usage of term "Untrusted WLAN" when RAT type is not known	13.4.0
2016-09	CT#73	CP-160418	0463	-		APN subscription check in the STa authentication and authorization procedure	13.5.0
2016-09	CT#73	CP-160418	0465	1		Transferring AAA identifier from the ePDG/TWAN to the PGW	13.5.0
2016-09	CT#73	CP-160436	0461	1		3GPP AAA Server/Proxy – EIR reference point	14.0.0
2016-09	CT#73	CP-160436	0462	2		STa and SWm extensions for IMEI check	14.0.0
2016-12	CT#74	CP-160674	0466	2		Destination-Host correction on STa & SWm	14.1.0
2016-12	CT#74	CP-160674				3GPP AAA Server behaviour in the user profile updated procedure	14.1.0
2016-12	CT#74	CP-160674	0489	1		Handling of Undefined bit in DER-Flags	14.1.0
2016-12	CT#74	CP-160679	0468	4		Handover of Emergency PDN Connections	14.1.0
2016-12	CT#74	CP-160679	0471	1		IMEI check for Emergency Attach over WLAN	14.1.0
2016-12	CT#74	CP-160679	0473	1		Emergency services over untrusted WLAN for unauthenticated or unauthorized UEs	14.1.0

2016-12	CT#74	CP-160679	0474	2		Support of Emergency sessions over Trusted WLAN	14.1.0
2016-12	CT#74	CP-160682	0469	1		Missing IMEI-Check-In-VPLMN-Result AVP	14.1.0
2016-12	CT#74	CP-160682	0477	1		IMEI check call flow for untrusted WLAN	14.1.0
2016-12	CT#74	CP-160657	0476	1		APN-Configuration AVP format for Non-3GPP accesses	14.1.0
2016-12	CT#74	CP-160681	0484	2		Load Control	14.1.0
2016-12	CT#74	CP-160653	0486	-		Renaming of Emergency-Indication AVP	14.1.0
2016-12	CT#74	CP-160664	0491	-		Correction to change IETF drmp draft version to official RFC 7944	14.1.0
2016-12	CT#74	CP-160651	0492	-		Discontinuation of the I-WLAN feature	14.1.0
2017-03	CT#75	CP-170050	0493	1		DIAMETER_ERROR_ILLEGAL_EQUIPMENT code	14.2.0
2017-03	CT#75	CP-170044	0494	1		Emergency-Info AVP in Non-3GPP IP Access Registration response	14.2.0
2017-03	CT#75	CP-170049	0495	1		Addition of ERP support for TWAN Interworking	14.2.0
2017-03	CT#75	CP-170037	0496	1		Bit ordering in Diameter AVPs used as bit-masks	14.2.0
2017-03	CT#75	CP-170037	0497	1		Handling of AAA Failure Indication over SWa	14.2.0
2017-03	CT#75	CP-170037	0498	1		SWm Behaviour after Failed Re-Authorization	14.2.0
2017-03	CT#75	CP-170048	0499	1		Update of reference for the Diameter base protocol	14.2.0
2017-03	CT#75	CP-170048	0500	1		Handling of the Vendor-Specific-Application-Id	14.2.0
2017-06	CT#76	CP-171033	0466	1		NAI for emergency services over WLAN access to EPC	14.3.0
2017-06	CT#76	CP-171018	0503	1		Support for signaling transport level packet marking	14.3.0
2017-06	CT#76	CP-171035	0505	1		Only ERP Implicit Bootstrapping mode is supported in Rel-14	14.3.0
2017-06	CT#76	CP-171042	0507	-		Definition of Origination-Time-Stamp AVP	14.3.0
2017-09	CT#77	CP-172019	0509	1		Emergency sessions over untrusted WLAN with an unauthenticated IMSI	14.4.0
2017-09	CT#77	CP-172015	0511	-		PGW selection for WLAN with deployed DCNs	14.4.0
2017-09	CT#77	CP-172013	0514	-		Correction of DRMP Procedures	14.4.0
2017-09	CT#77	CP-172023	0508	-		MIP6-Feature-Vector over SWx	15.0.0
2017-09	CT#77	CP-172023	0512	3		External-ID in non-3GPP subscription profile	15.0.0
2017-12	CT#78	CP-173026	0515	-		Authorization procedure initiated by ePDG	15.1.0
2018-06	CT#80	CP-181123	0518	-		Full-Network-Name and Short-Network-Name AVPs	15.2.0
2019-03	CT#83	CP-190032	0519	1		Mobility between EPC/ePDG and 5GS	15.3.0
2019-09	CT#85	CP-192094	0521	2		draft-ietf-dime-load published as RFC 8583	15.4.0
2020-03	CT#87e	CP-200047	0522	-		APN-OI-Replacement not applicable for Emergency services	16.0.0
2020-06	CT#88e	CP-201053	0523	-		APN-OI-Replacement	16.1.0
2020-09	CT#89e	CP-202043	0525	1		AAA Deregistration	16.2.0
2021-03	CT#91e	CP-210027	0526	1		Use of Inclusive Language	17.0.0
2021-09	CT#93e	CP-212053	0528	1	D	Editorial correction on WLAN Location Information AVP name	17.1.0
2022-03	CT#95e	CP-220040	0529	1	F	29.273 Addition of MPS statement to Annex B	17.2.0
2022-03	CT#95e	CP-220053	0530	-	B	Non-Seamless WLAN offload in 5GS	17.2.0
2022-06	CT#96	CP-221030	0531	1	F	NSWO in 5GS	17.3.0
2022-09	CT#97e	CP-222034	0533	-	F	Corrections for NSWO in 5GS	17.4.0
2022-12	CT#98e	CP-223048	0535	1	F	Correcting a label in SUCI in NAI format	17.5.0
2023-03	CT#98e	CP-230079	0538	1	F	Stage 2 alignments for Non-seamless WLAN offload in 5GS	17.6.0

History

Document history		
V17.2.0	May 2022	Publication
V17.3.0	July 2022	Publication
V17.4.0	October 2022	Publication
V17.5.0	January 2023	Publication
V17.6.0	April 2023	Publication