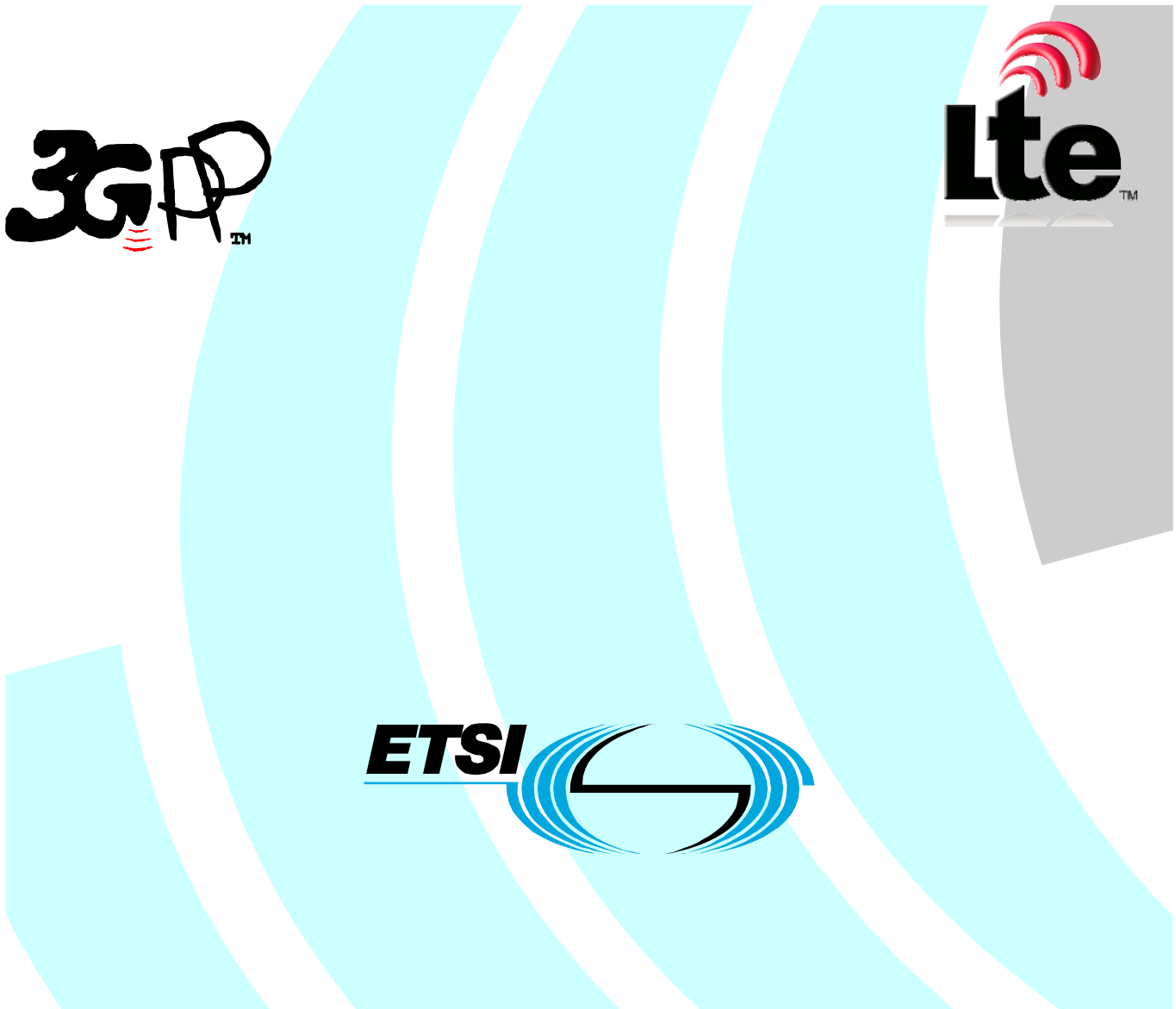
ETSI TS 129 273 V8.2.0 (2009-06)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Evolved Packet System (EPS);
3GPP EPS AAA interfaces
(3GPP TS 29.273 version 8.2.0 Release 8)



Reference
RTS/TSGC-0429273v820

Keywords
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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

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

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

Foreword

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, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

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

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.

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 will also cover H2 reference point defined in I-WLAN mobility.

1 Scope

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

The present document is applicable to:

- 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 H2 reference point between the 3GPP AAA Server and the HA.
- The SWm reference point between the 3GPP AAA Server/Proxy and the ePDG.

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 Draft draft-korhonen-dime-pmip6-04: "Diameter Proxy Mobile IPv6: Support For Mobility Access Gateway and Local Mobility Anchor to Diameter Server Interaction Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", work in progress.

[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] IETF RFC 3588: "Diameter Base Protocol".

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

[9] IETF Draft draft-ietf-dime-qos-attributes-05: "Quality of Service Attributes for Diameter", work in progress.

[10] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[11] IETF Draft draft-ietf-dime-mip6-split-12: "Diameter Mobile IPv6: Support for Home Agent to Diameter Server Interaction", work in progress.

[12] 3GPP TS 23.327: "Mobility between 3GPP-Wireless Local Area Network (WLAN) Interworking and 3GPP Systems".

[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] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[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 over Gx reference point".

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

[25] 3GPP2 X.P0057: "EUTRAN – eHRPD Interworking".

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

[27] IETF Draft draft-arkko-eap-aka-kdf-05: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", work in progress

[28] IETF Draft draft-ietf-mip6-bootstrapping-integrated-06: "MIP6-bootstrapping for the Integrated Scenario", work in progress.

[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] 3GPP TS 33.234: "Wireless Local Area Network (WLAN) interworking security".

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

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

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].

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 "Cat." column. For the correct handling of the Information Element according to the category type, see the description detailed in section 6 of the 3GPP TS 29.228 [22].

Editor's Note: new Diameter Command Codes shall be defined if the existing ABNF is modified in any other way than adding new AVPs using the *[AVP] extensibility possibility (if available in the existing ABNF). This shall be checked when the specification is stable and about to be completed.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Editor"s Note: To be completed or section removed.

3.3 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].

EPC	Evolved Packet Core
ePDG	Evolved Packet Data Gateway
FACoA	Foreign Agent Care-of-Address
LMA	Local Mobility Anchor
MAG	Mobile Access Gateway
MIPv4	Mobile IP version 4
NAS	Network Access Server
PBU	Proxy Binding Update
PMIP/PMIPv6	Proxy Mobile IP version 6
RRP	MIPv4 Registration Reply
RRQ	MIPv4 Registration Request
SGW	Serving Gateway

4 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. 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 section 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.

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.

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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP-payload	M	Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE is required in this case.
UE Layer-2 address	Calling-Station-ID	M	Carries the Layer-2 address of the UE.
Access Type	RAT-Type	O	Contains the untrusted non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	O	Contains the access network identifier used for key derivation at the HSS. (See 3GPP TS 24.302 [26] for all possible values) It is included if the non-3GPP access network selects EAP-AKA' authentication method.

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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication.
Result code	Result-Code / Experimental-Result	M	Result of the operation. Result codes are as in Diameter Base Protocol (IETF RFC 3588 [7]). Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which contains 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	Charging duration
Pairwise Master Key	EAP-Master-Session-Key	C	Shall be sent if Result-Code AVP is set to DIAMETER_SUCCESS.
3GPP AAA Server Name	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 identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or one occurrence of this information element.
Trust Relationship Indicator	AN-Trusted	M	This AVP contains the 3GPP AAA Server's decision on handling the non-3GPP access network trusted or untrusted. For the SWa case, the value 'UNTRUSTED' shall be used.

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 authentication method shall be selected based on the presence of the Access Network Identity: if this information element is present, EAP-AKA' method is used; otherwise, EAP-AKA method is used

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.

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.

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 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 trusted non-3GPP access, indicating that both re-authentication and re-authorization of the user is needed. Upon receipt of such a request, the trusted 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 3588 [7]. 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 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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
Re-Auth Request Type	Re-Auth–Request-Type	M	This information element defines whether the user is to be authorized only or authenticated and authorized. AUTHORIZE_AUTHENTICATE shall be required 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 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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15] and formatted as defined in clause 19 of 3GPP TS 23.003 [14].
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. 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 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 formatted as defined in clause 19 of 3GPP TS 23.003 [14].
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 authorized only or authenticated and authorized. AUTHORIZE_AUTHENTICATE shall be required in this case.

Table 4.1.2.4.1/2: 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 formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP payload	M	This IE shall contain the Encapsulated EAP payload used for UE-3GPP AAA Server mutual authentication.
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 (IETF RFC 3588 [7]). The Experimental-Result AVP shall be used for SWa errors. This is a grouped AVP which contains 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 IE shall contain the maximum number of seconds the user session should remain active.
Accounting Interim Interval	Accounting Interim-Interval	O	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).

4.2 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 section 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 NAS to a 3GPP AAA Server.

```
< Diameter-EAP-Request > ::=      < Diameter Header: 268, REQ, PXY >
                                  < Session-Id >
                                  { Auth-Application-Id }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  { Destination-Realm }
                                  { Auth-Request-Type }
                                  { EAP-Payload }
                                  [ User-Name ]
                                  [ Calling-Station-Id ]
                                  [ RAT-Type ]
                                  …
                                  [ ANID ]
                                  …
                                  *[ 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 >
                                 { 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]
…
*[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 IP 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 >
{ 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 >
{ 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

5 STa Description

5.1 Functionality

5.1.1 General

The STa reference point is defined between a non-3GPP IP access network and the 3GPP AAA Server or between a non-3GPP IP 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 IP 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 IP 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 IP 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, MIPv4 FA-CoA mode related mobility parameters in a case the UE attaches to the EPC using the S2a reference point.

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 both PMIPv6 and MIPv4 FA-CoA mode 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 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 may provide information on its PMIPv6 capabilities to the 3GPP AAA Server.

For a trusted non-3GPP access, the 3GPP AAA Server may perform IP mobility mode selection. The 3GPP AAA Server may provide to the trusted non-3GPP GW an indication if either PMIPv6 or local IP address assignment shall be used

During the STa Access Authentication and Authorization procedure the trusted non-3GPP GW shall provide information on the Access Network Identity to the 3GPP AAA Server.

During the STa Access Authentication and Authorization procedure the AAA Server may provide a Home Agent IPv6 address (and optionally IPv4 address) or FQDN to the trusted non-3GPP GW. This is needed if the DHCPv6 option for Home Agent address discovery is chosen (see TS 24.303 [13] and IETF Draft draft-ietf-mip6-bootstrapping-integrated [28]). If the Home Agent IPv6 address or FQDN is not included in the final Authentication and Authorization Answer by the AAA server, the trusted non-3GPP GW shall not assign the Home Agent via DHCPv6.

The User-Name AVP may contain a decorated NAI (as defined in 3GPP TS 23.003 [14]) in a roaming case. 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 defined in 3GPP TS 23.234 [21] and 3GPP TS 23.003 [14].

For both PMIPv6 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 Gateway identity for each of the already allocated PDN Gateway(s) with the corresponding PDN information is provided to the trusted non-3GPP system. The PDN Gateway identity is a FQDN and/or IP address of the PDN GW. If a FQDN is provided, the trusted non-3GPP system shall derive it to IP address according to the selected mobility management protocol.

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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP-payload	M	Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE is required in this case.
UE Layer-2 address	Calling-Station-ID	M	Carries 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 Draft draft-ietf-dime-qos-attributes [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. The PMIP6_SUPPORTED flag shall be set if the non-3GPP access supports PMIPv6 (see IETF Draft draft-korhonen-dime-pmip6 [2]). The flag MIP6_INTEGRATED shall be set if DHCPv6 based Home Agent address discovery is supported as defined in IETF RFC 5447 [6].
Access Type	RAT-Type	M	Contains the non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	M	Contains 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	O	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	This information element contains the APN the user wants to connect to (if available).
Terminal Information	Terminal-Information	O	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.

Editor"s Note: It is FFS if other MIP6-Feature-Vector AVP flags than those listed could be used.

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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication.
Result code	Result-Code / Experimental Result Code	M	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 contains 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	Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	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 PMIPv6 is used, the non-3GPP access network was decided to be trusted 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 when constructing the PDN GW FQDN upon which to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if PMIPv6 is used 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. When PMIPv6 is used 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, this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes. The AGW knows if PMIPv6 is used or if a local IP address 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 PMIPv6 is used, 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 (IPv4, IPv6 or IPv4v6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - APN-AMBR When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included: - HA-APN - Authorized 3GPP QoS profile - PDN GW identity
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 the Result-Code AVP is set to DIAMETER_SUCCESS. It shall contain a AAA/HSS authorized set of mobility capabilities to the trusted non-3GPP access network, if dynamic mobility mode selection is done. The PMIP6_SUPPORTED or ASSIGN_LOCAL_IP flag shall be set by the 3GPP AAA server to mandate which 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 PMIPv6 or MIPv4 is used and the Result-Code AVP is set to DIAMETER_SUCCESS and shall contain an AAA/HSS assigned identity (i.e. IMSI in EPC root NAI format as defined in 3GPP TS 23.003 [14]) to be used by the MAG in subsequent PBUs as the MN-ID or MIPv4 RRQs as the MN-NAI identifying the user in the EPS network. The node in the trusted non-3GPP access network receiving this IE may ignore it, if the node has already acquired equivalent information through other access network specific means.
3GPP AAA Server Name	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 identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). 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	This information element contains the type of charging method to be applied to the user (see 3GPP TS 29.061 [31]).
UE AMBR	AMBR	C	This Information Element contains 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.

Editor"s Note: It is FFS whether filtering rules need to be returned to NAS.

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 GW 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 SWx authentication response indicates that:

- The user does not exist, then the 3GPP AAA Server shall respond the non-3GPP GW 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 GW 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 GW 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 GW with the Result-Code set to DIAMETER_REDIRECT_INDICATION and the Redirect-Host set to the Diameter identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response from the HSS).

- Any other error occurred, then the error code DIAMETER_UNABLE_TO_COMPLY shall be returned to the Non-3GPP GW.

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: 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 local breakout may be used for some of the APN connections of the user and

- The appropriate trust relationship exists between the HPLMN and VPLMN operators.

The 3GPP AAA Server shall identify the possibility for local breakout based on the VPLMN-Dynamic-Address-Allowed AVPs in the user's subscription profile; If the PDN GW may be allocated in the VPLMN for any of the subscribed APNs, local breakout is considered to be possible.

If the 3GPP AAA Server has decided to take the received trust relationship indicator into account, it shall combine its own decision (taken as described above) with the received trust relationship indicator in a way that the final decision shall be "trusted" only if both initial decisions were "trusted"; otherwise, the final decision shall be "untrusted"

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].

SWx interface to obtain the user's subscription profile authorization data 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: The network operator can configure this e.g. according to the roaming agreements with the non-3GPP AN operator or with VPLMN operator.

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 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 (EAP-Request/AKA-Challenge) 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 subclauses. Otherwise, the SWa authentication and authorization procedure is executed as described in clause 4.1.2.1.

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 if the user is barred to use the subscribed APNs. If it is so, then the Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED

3) Check RAT-Type AVP. If

   - the access type indicates any value not described in 3GPP TS 29.212 [23] or

   - the received RAT-Type is listed in the user's disallowed RAT-Types,

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

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

4) Check if the user has a subscription for the requested 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:

   - 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 flag indicates to the 3GPP AAA server whether the trusted non-3GPP GW supports PMIPv6 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 PMIPv6 should be used, the PMIP6_SUPPORTED flag shall be set in the response to indicate the PMIPv6 support of the UE to the trusted non 3GPP GW. 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 trusted non 3GPP GW that a local IP address should be assigned. The 3GPP AAA server shall not set the PMIP6_SUPPORTED and ASSIGN_LOCAL_IP flags both at the same time in the response.

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

Once the Authentication and Authorization procedure successfully finishes, the 3GPP AAA Server shall download, together with authentication data, the list of authorized APN"s and the authorized mobility protocols in the authentication and authorization response from the HSS (see SWx procedure in Section 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.

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.

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 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 GW.
- 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: For exampe, 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.

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).

5.1.2.1.4 Trusted non-3GPP GW Detailed Behaviour

The Trusted non-3GPP GW 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 PMIPv6 is used, at successful completion of the procedure, the trusted non-3GPP GW shall store the non-3GPP user data received from the 3GPP AAA Server. The trusted non-3GPP GW 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.

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 GW has received the PGW identity in form of the FQDN from the 3GPP AAA server, then the trusted non-3GPP GW may obtain the IP address of the Home Agent functionality of that PGW as described in 3GPP TS 29.303 [34].

5.1.2.2 HSS/AAA Initiated Detach on STa

5.1.2.2.1 General

This procedure is used to communicate between the 3GPP AAA/HSS and the the trusted non-3GPP access network to indicate that the 3GPP AAA/HSS has decided that a specific UE shall be detached from accessing the EPC. 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 RFC 3588 [7]. 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 contains the permanent identity of the user (i.e. IMSI in EPC root NAI format as defined in 3GPP TS 23.003 [14]).
Auth-Session-State	Auth-Session-State	O	This information element indicates to the Non-3GPP GW 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	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 contains 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	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.

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 GW. If it does require a STR from the Non-3GPP 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.

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.

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 GW 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 GW.

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 GW onto the 3GPP AAA Server and shall return an STA command to the non-3GPP 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 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 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 Non-3GPP GW.

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 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). 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. Upon receipt of such a request, the trusted non-3GPP access 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 3588 [7]. 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 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 to retrieve the subscriber profile from the HSS. This procedure may be initiated at any time by the Trusted non-3GPP GW 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 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.

NOTE 1: After receiving the authorization answer, the trusted 3GPP GW 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.

The STa Re-Authentication procedure shall be used between the 3GPP AAA Server and the trusted non-3GPP access 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 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 3588 [7]. 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 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.

NOTE 2: If the re-authentication of the user is not successful, the trusted non-3GPP access will release all the active PDN connections of theuser. After a successful authentication and authorization procedure, the trusted 3GPP GW 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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
Re-Auth Request Type	Re-Auth–Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. 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 is 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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
Result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which contains 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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
Request-Type	Auth-Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. In this case, it shall have the value: AUTHORIZE_ONLY
Routing Information	Destination-Host	M	The 3GPP AAA Server name is obtained from the Origin-Host AVP of a previously received message.

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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for STa errors. This is a grouped AVP which contains 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 3588 [7].
Accounting Interim Interval	Acct-Interim-Interval	O	Charging duration.
APN-OI replacement	APN-OI-Replacement	C	This AVP shall indicate the domain name to replace the APN-OI when constructing the PDN GW FQDN upon which to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if PMIPv6 is used 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. When PMIPv6 is used, 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, 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 GW knows if PMIPv6 is used or if a local IP address 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 PMIPv6 is used, 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 (IPv4, IPv6 or IPv4v6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included: - HA-APN - Authorized 3GPP QoS profile - PDN GW identity
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]).
UE AMBR	AMBR	C	This Information Element contains 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".

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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP-payload	M	Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	Defines 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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in clause 19 of 3GPP TS 23.003 [14].
EAP payload	EAP payload	M	Encapsulated EAP payload used for UE- 3GPP AAA Server mutual authentication.
Result code	Result-Code / Experimental Result Code	M	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 contains 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 3588 [7].
Accounting Interim Interval	Accounting Interim-Interval	O	Charging duration.
Pairwise Master Key	EAP-Master-Session-Key	C	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 PMIPv6 is used 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 when constructing the PDN GW FQDN upon which to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if PMIPv6 is used 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 and the Result-Code AVP is set to DIAMETER_SUCCESS. When PMIPv6 is used 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, this AVP shall only be present if DHCP based Home Agent discovery is used and contain the Home Agent Information for discovery purposes. The AGW knows if PMIPv6 is used or if a local IP address 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 PMIPv6 is used, the following information elements per APN may be included: - APN - Authorized 3GPP QoS profile - User IP Address (IPv4 and/or IPv6) - Allowed PDN types (IPv4, IPv6 or IPv4v6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed - APN-AMBR When DSMIPv6 with HA discovery based on DHCPv6 is used, the following information elements per Home Agent may be included: - HA-APN - Authorized 3GPP QoS profile - PDN GW identity
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]).
UE AMBR	AMBR	C	This Information Element contains 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".

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 GW, 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 chapter 5.1.2.1.2.

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 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 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 subclauses 8.1.2.2.2.1 and 8.1.2.2.2.2.

- De-register the user from the HSS, as described in subclauses 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 GW 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 GW 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 GW 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 GW 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.

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 shall detach the user from the non-3GPP access network and release all resources.

5.1.2.4 Non-3GPP IP 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 Base IETF RFC 3588[7] STR and STA commands

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 contains the identity of the user (i.e. IMSI in EPC root NAI format as defined in 3GPP TS 23.003 [14]).
Termination Cause	Termination-Cause	M	Contains 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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for S6b errors.

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 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.

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.

5.2 Protocol Specification

5.2.1 General

The STa reference point shall be based on Diameter, as defined in IETF RFC 3588 [7] 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 Draft draft-korhonen-dime-pmip6 [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 Draft draft-korhonen-dime-pmip6 [2] and the NAS to AAA interface functionality defined in IETF RFC 5447 [6].

The MAG 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 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 Draft draft-korhonen-dime-pmip6 [2].

```
< Diameter-EAP-Request > ::=      < Diameter Header: 268, REQ, PXY, 16777250 >
                                  < Session-Id >
                                  { Auth-Application-Id }
```

{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ 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]
…
*[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 Draft draft-korhonen-dime-pmip6 [2]. The ABNF also contains AVPs that are reused from IETF RFC 4072 [5].

< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY, 16777250 >
< Session-Id >
{ 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]

…
*[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 >
                                  { 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 >
                                 { 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 GW to a 3GPP AAA Server/Proxy. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command.

```
<Session-Termination-Request> ::=    < Diameter Header: 275, REQ, PXY, 16777250 >
                                     < Session-Id >
                                     { Origin-Host }
                                     { Origin-Realm }
                                     { Destination-Realm }
                                     { Auth-Application-Id }
                                     { Termination-Cause }
                                     [ User-Name ]
                                     …
                                     *[ 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 GW. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::=  < Diameter Header: 275, PXY, 16777250 >
                                  < Session-Id >
                                  { Result-Code }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  *[ 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-3GPPGW. ABNF for the RAR command is as follows:

```
< Re-Auth-Request > ::=     < Diameter Header: 258, REQ, PXY, 16777250 >
                            < Session-Id >
                            { 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 GW to a 3GPP AAA Server/Proxy. ABNF for the RAA commands is as follows:

```
< Re-Auth-Answer > ::=      < Diameter Header: 258, PXY, 16777250 >
                            < Session-Id >
                            { 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 GW to a 3GPP AAA Server/Proxy. The ABNF is re-used from the IETF Draft draft-korhonen-dime-pmip6 [2].

```
< AA-Request > ::=          < Diameter Header: 265, REQ, PXY, 16777250 >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Origin-Host }
                            { Origin-Realm }
                            { Destination-Realm }
                            { Auth-Request-Type }
                            [ Destination-Host ]
                            [ User-Name ]
                            [ Visited-Network-Identifier ]
                            [ RAT-Type ]
                            [ QoS-Capability ]
                            …
                            *[ 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 GW. The ABNF is re-used from the IETF Draft draft-korhonen-dime-pmip6 [2].

```
< AA-Answer > ::=           < Diameter Header: 268, PXY, 16777250 >
                            < Session-Id >
                            { 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]
…
*[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 IP 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 GW to a 3GPP AAA server. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Request command.

<Session-Termination-Request> ::= < Diameter Header: 275, REQ, PXY, 16777250 >
< Session-Id >
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
{ Auth-Application-Id }
{ Termination-Cause }
[User-Name]
…
*[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 GW. The Command Code value and ABNF are re-used from the IETF RFC 3588 [7] Session-Termination-Answer command.

<Session-Termination-Answer> ::= < Diameter Header: 275, PXY, 16777250 >
< Session-Id >
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
*[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 PMIPv6 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

Table 5.2.3.1/1: Diameter STa AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
APN-Configuration	1430	8.2.3.7	Grouped	M				No
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V	
QoS-Capability	tbd	5.2.3.4						
RAT-Type	1032	5.2.3.6	Enumerated	M,V	P			Y
Visited-Network-Identifier	600	9.2.3.1.2	UTF8String	M,V				No
ANID	1504	5.2.3.7	UTF8String	M, V				No
Service-Selection	tbd	5.2.3.5	UTF8String	M	P		V	No
Mobile-Node-Identifier	tbd	5.2.3.2	UTF8String	M	P		V	No
AN-Trusted	1503	5.2.3.9	Enumerated	M, V	P			No

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, do not need to be supported.

Table 5.2.3.1/2: STa re-used Diameter AVPs

Attribute Name	Reference	Comments
Accounting-Interim-Interval	IETF RFC 3588 [7]	
Auth-Request-Type	IETF RFC 3588 [7]	
Calling-Station-Id	IETF RFC 4005 [4]	
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 3588 [7]	
Session-Timeout	IETF RFC 3588 [7]	
User-Name	IETF RFC 3588 [7]	
Terminal-Information	3GPP TS 29.272 [29]	
MIP6-Agent-Info	draft-ietf-dime-mip6-integrated [6]	
APN-OI-Replacement	3GPP TS 29.272 [29]	

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

5.2.3.2 Mobile-Node-Identifier

The Mobile-Node-Identifier AVP (AVP Code TBD) 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.

The Mobile-Node-Identifier is defined on IETF Draft draft-korhonen-dime-pmip6-04 [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 GW (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 GW 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 GW 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 GW that PMIPv6 shall be used.

- ASSIGN_LOCAL_IP ()
  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 GW that the non-3GPP GW shall assign to the user a local IP address.

- MIP4_SUPPORTED
  This flag is set by the PDN GW. When this flag is set, it shows that MIPv4 mobility protocol is used on the S2a interface.

Editor"s Note: The value of the ASSIGN_LOCAL_IP and MIP4_SUPPORTED flag needs to be assigned by IANA.

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 may contain an APN that contains 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 Draft draft-ietf-dime-mip6-split [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 IP access network is to be handled as trusted.

UNTRUSTED (1)

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

5.2.4 Session Handling

The Diameter protocol between the non-3GPP Access Gateway 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 3588 [7]).

6 SWd Description

6.1 Functionality

6.1.1 General

For a general description of the SWd reference point refer to 3GPP TS 23.234 [21], Section 6.3.11.1 "General Description of the Wd Reference Point".

The functionality of the SWd reference point is to transport AAA messages similar to those provided in 3GPP TS 23.234 [21], Section 6.3.11.2 with the following exceptions:

- 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;
- Providing access scope limitation information to the access network based on the authorised services for each user (for example, IP address filters);
- 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.

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 GW 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 GW, 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.

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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
EAP payload	EAP-payload	M	Encapsulated EAP payload used for the UE – 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE is required in this case.
UE Layer-2 address	Calling-Station-ID	M	Carries 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 Draft draft-ietf-dime-qos-attributes [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. The PMIP6_SUPPORTED flag shall be set if the trusted non-3GPP access supports PMIPv6 (see IETF Draft draft-korhonen-dime-pmip6 [2]). The flag MIP6_INTEGRATED shall be set if DHCPv6 based Home Agent address discovery is supported as defined in IETF RFC 5447 [6].
Access Type	RAT-Type	M	Contains the trusted non-3GPP access network technology type that is serving the UE.
Access Network Identity	ANID	M	Contains 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	Identifier that allows the home network to identify the Visited Network.
APN Id	Service-Selection	O	This information element contains the APN the user wants to connect to (if available).
Terminal Information	Terminal-Information	O	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	This AVP expresses the trusted/untrusted decision about the non-3GPP IP access, from the VPLMN's point of view.

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 GW 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 GW, 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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
Request-Type	Auth-Req-Type	M	The following values are to 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	Identifier that allows the home network to identify the Visited Network.
Routing Information	Destination-Host	M	The 3GPP AAA Server name 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 Draft draft-ietf-dime-qos-attributes [9].
Access Type	RAT-Type	O	Contains 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 IP 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 subclauses 7.1.2.1.3 and 7.1.2.2.3 respectively.

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 PMIPv6 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 subclauses 9.1.2.1.4, 9.1.2.2.4, 9.1.2.3.4, and 9.1.2.4.4, respectively.

6.2 Protocol Specification

6.2.1 General

The SWd reference point shall be based on Diameter, as defined in IETF RFC 3588 [7] 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 Draft draft-korhonen-dime-pmip6 [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.

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 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 Draft draft-korhonen-dime-pmip6 [2].

```
< Diameter-EAP-Request > ::=    < Diameter Header: 268, REQ, PXY, 16777250 >
                                < Session-Id >
                                { Auth-Application-Id }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                { 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 ]
                                …
                                *[ 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 Draft draft-korhonen-dime-pmip6 [2]. The ABNF also contains AVPs that are reused from IETF RFC 4072 [5].

```
< Diameter-EAP-Answer > ::=     < Diameter Header: 268, PXY, 16777250 >
                                < Session-Id >
                                { 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]
…
*[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 subclauses 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 subclauses apply.

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

The ABNFs defined for the STa interface in clause 5.2.2.4 and in its subclauses 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 subclauses 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 subclauses 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 PMIPv6 mode, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

Table 5.2.3.1/1: Diameter STa AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
APN-Configuration	1430	8.2.3.7	Grouped	M				No
MIP6-Feature-Vector	tbd	5.2.3.3	Unsigned64	M			V	
QoS-Capability	tbd	5.2.3.4						
RAT-Type	1032	5.2.3.6	Enumerated	M,V	P			Y
Visited-Network-Identifier	600	9.2.3.1.3	UTF8String	M,V				No
ANID	1504	5.2.3.7	UTF8String	M, V				No
Service-Selection	tbd	5.2.3.5	UTF8String	M	P		V	No
Mobile-Node-Identifier	tbd	5.2.3.2	UTF8String	M	P		V	No
AN-Trusted	1503	5.2.3.9	Enumerated	M,V	P			No

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, do not need to be supported.

Table 5.2.3.1/2: STa re-used Diameter AVPs

Attribute Name	Reference	Comments
Accounting-Interim-Interval	IETF RFC 3588 [7]	
Auth-Request-Type	IETF RFC 3588 [7]	
Calling-Station-Id	IETF RFC 4005 [6]	
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 3588 [7]	
Session-Timeout	IETF RFC 3588 [7]	
User-Name	IETF RFC 3588 [7]	
Terminal-Information	3GPP TS 29.272 [29]	
APN-OI-Replacement	3GPP TS 29.272 [29]	

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

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 PMIPv6 related mobility parameters in a case the UE attaches to the EPC via the S2b 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 capabilities to the 3GPP AAA Server. The 3GPP AAA Server may perform IP mobility mode selection. The 3GPP AAA Server may provide to the ePDG an indication if either PMIPv6 or local IP address assignment shall be used.

Upon a successful authorization, when PMIPv6 is used, the 3GPP AAA server shall return PMIPv6 related information back to the ePDG. This information shall 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 Gateway 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 is ued, 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 protocol 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 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], formatted as defined in 3GPP TS 23.003 [14].
EAP payload	EAP-Payload	M	This information element shall contain the encapsulated EAP payload used for UE - 3GPP AAA Server mutual authentication
Authentication Request Type	Auth-Request-Type	M	This information element indicates whether authentication only or authentication and authorization are required. It shall have the value of AUTHORIZE_AUTHENTICATE.
APN	Service-Selection	C	This information element shall contain the APN for which the UE is requesting authorization. This AVP shall be present when the ePDG has received an APN from the UE in the IKEv2 signalling.
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.
Mobility features	MIP6-Feature-Vector		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 shall be set as defined in IETF Draft draft-korhonen-dime-pmip6 [2], if PMIPv6 is supported by ePDG. The MIP6_INTEGRATED flag shall be used to indicate to the 3GPP AAA server that the ePDG supports IKEv2 based Home Agent address discovery.

Table 7.1.2.1.1/2: Authentication and Authorization Answer

Information element name	Mapping to Diameter AVP	Cat.	Description
EAP payload	EAP-Payload	M	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	It 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.
Result code	Result-Code / Experimental-Result-Code	M	It shall contain the result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ.
3GPP AAA Server Name	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 identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). 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 shall be set to indicate that PMIPv6 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 when constructing the PDN GW FQDN upon which to perform a DNS resolution. See 3GPP TS 23.003 [3]. It shall only be included if PMIPv6 is used 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. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When PMIPv6 is used, the following information elements per APN may be included: - APN - User home IP Address (if static IPv4 and/or IPv6 is allocated to the UE's subscribed APN) - PDN GW identity (if the PDN connection was active in case of HO, if there is static PDN GW allocated to the UE's subscribed APN) - PDN GW allocation type - VPLMN Dynamic Address Allowed 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 In these cases, the following information elements shall be included: - HA-APN - PDN GW identity
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 PMIPv6 is used. It shall contain an AAA/HSS assigned identity (i.e. IMSI in EPC root NAI format as defined in 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. The ePDG receiving this IE may ignore it, if the ePDG has already acquired equivalent information from the UE.

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.

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 identity of the 3GPP AAA Server currently serving the user (as indicated 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 the user does not have non-3GPP access subscription, then 3GPP AAA Server shall respond to the non-3GPP GW 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.

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.

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) Check if there was request for an APN received. If not, AAA Server shall check, whether the user already has an active PDN connection to the default APN. If it is so, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. Otherwise, the default APN of the user is selected to be used during the actual authentication and authorization procedure.

4) Check if user has a subscription for the requested 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. 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 flag indicates to the 3GPP AAA server whether the ePDG supports PMIPv6 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 PMIPv6 should be used, the PMIP6_SUPPORTED flag shall be set in the response to indicate the PMIPv6 support of the UE to the

ePDG. 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: 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 and ASSIGN_LOCAL_IP flags both at the same time in the response.

Upon successful authentication and authorization, the 3GPP AAA Server shall return user data relevant to the APN as received from the HSS. The Result-Code shall be set to DIAMETER_SUCCESS.

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.

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.

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).

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.

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 PMIPv6 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 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].

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 section 7.1.2.5).

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).

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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
Diameter Session ID	Session-Id	M	This information element shall identify the session uniquely.
Request Type	Auth-Request-Type	M	This information element shall contain the type of request. It shall have the value AUTHORIZATION_ONLY (0).

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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14.]
Diameter Session ID	Session-Id	M	This information element shall identify the session uniquely.
Registration Result	Result-Code/ Experimental Result Code	M	It shall contain the result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or or as per in NASREQ.
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 and PGW Data	APN-Configuration	C	This information element shall only be sent if the Result-Code AVP is set to DIAMETER_SUCCESS. APN-Configuration is a grouped AVP, defined in 3GPP TS 29.272 [29]. When PMIPv6 is used, the following information elements per APN may be included: - APN - Authorized 3GPP QoS profile - Statically allocated User IP Address (IPv4 and/or IPv6) - PDN GW identity - PDN GW allocation type - VPLMN Dynamic Address Allowed 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 folowing information elements shall be included: - HA-APN - PDN GW identity
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]).
Session time	Session-Timeout	C	If the authorization succeeded, then this IE shall contain the time this authorization is valid for.

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. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2) Check whether the user is allowed to access the APN. If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

3) The 3GPP AAA Server shall return user data relevant to the APN as received from the HSS. The Result-Code shall be set to DIAMETER_SUCCESS.

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 Section 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.

7.1.2.2.3 3GPP AAA Proxy Detailed Behaviour

The 3GPP AAA Proxy shall be required to handle roaming cases in which the PDG 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).

7.1.2.2.4 ePDG Detailed Behaviour

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.

If PMIPv6 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 PMIPv6 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) and IKE_SA of the user.
- 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.
  - 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 PMIPv6 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 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].

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 Base IETF RFC 3588 [7] STR and STA commands

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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
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	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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
Auth-Session-State	Auth-Session-State	O	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	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 contains 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	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.

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.

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 command codes Re-Auth-Request and Re-Auth-Answer specified in IETF RFC 3588 [7]. 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 mapped to the Diameter command codes Re-Auth-Request (RAR) and Re-Auth-Answer (RAA) 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 identity of the user. The identity shall be represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
Re-Auth Request Type	Re-Auth-Request-Type	M	Defines whether the user is to be authenticated only, authorized only or both. AUTHORIZE_ONLY shall be set.
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 contains the identity of the user. The identity is represented in NAI form as specified in IETF RFC 4282 [15], formatted as defined in 3GPP TS 23.003 [14].
Result	Result-Code	M	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 3588 [7] 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.

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 3588 [7] 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 Draft draft-korhonen-dime-pmip6 [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 Draft draft-korhonen-dime-pmip6 [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 tbd.

Editor"s Note: A new application ID is needed to be applied for to IANA.

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 Draft draft-korhonen-dime-pmip6 [2].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY >
                             < Session-Id >
                             { Auth-Application-Id }
                             { Origin-Host }
                             { Origin-Realm }
                             { Destination-Realm }
                             { Auth-Request-Type }
                             { EAP-Payload }
                             [ User-Name ]
                             [ RAT-Type ]
                             [ Service-Selection ]
                             [ MIP6-Feature-Vector ]
                             [ QoS-Capability ]
                              [ Visited-Network-Identifier ]
                             …
                             *[ 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 Draft draft-korhonen-dime-pmip6 [2].

```
< Diameter-EAP-Answer > ::= < Diameter Header: 268, PXY >
                            < Session-Id >
                            { Auth-Application-Id }
                            { Auth-Request-Type }
                            { Result-Code }
                            { Origin-Host }
                            { Origin-Realm }
                            { EAP-Payload }
                             [ EAP-Master-Session-Key ]
                            [ APN-OI-Replacement ]
                             [ APN-Configuration ]
                             [ MIP6-Feature-Vector ]
                             [ Mobile-Node-Identifier ]
                             [ Session-Timeout ]
                            [MIP6-Agent-Info ]
                            *[ Redirect-Host ]
                            …
                            *[ 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 >
                        < Session-Id >
                        { Auth-Application-Id }
                        { Origin-Host }
                        { Origin-Realm }
                        { Destination-Realm }
                        { Auth-Request-Type }
                        [ User-Name ]
                        …
                        *[ 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 >
                        < Session-Id >
                        { Auth-Application-Id }
                        { Auth-Request-Type }
                        { Result-Code }
                        { Origin-Host }
                        { Origin-Realm }
                        [ User-Name ]
                        [ APN-Configuration ]
                         [ 3GPP-Charging-Characteristics ]
                        [ Session-Timeout ]
                        …
                        *[ 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 3588 [7], and is defined as follows:

```
< Session-Termination-Request > ::=     < Diameter Header: 275, REQ, PXY >
                                        < Session-Id >
                                        { Origin-Host }
                                        { Origin-Realm }
                                        { Destination-Realm }
                                        { Auth-Application-Id }
                                        { Termination-Cause }
                                        [ User-Name ]
                                        …
                                        *[ 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 3588 [7], and is defined as follows:

```
< Session-Termination-Answer > ::=      < Diameter Header: 275, PXY >
                                        < Session-Id >
                                        { Result-Code }
                                        { Origin-Host }
                                        { Origin-Realm }
                                        …
                                        *[ 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 >
                              < Session-Id >
                              { 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 >
                             < Session-Id >
                             { 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 3588 [7] Session-Termination-Request command.

```
<Session-Termination-Request> ::=  < Diameter Header: 275, REQ, PXY, 16777250 >
                                   < Session-Id >
                                   { Origin-Host }
                                   { Origin-Realm }
                                   { Destination-Realm }
                                   { Auth-Application-Id }
                                   { Termination-Cause }
                                   [ User-Name ]
                                   …
                                   *[ 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 3588 [7] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::=  < Diameter Header: 275, PXY, 16777250 >
                                  < Session-Id >
                                  { Result-Code }
                                  { Origin-Host }
                                  { Origin-Realm }
                                  *[ 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 >
                            < Session-Id >
                            { 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 >
                            < Session-Id >
                            { 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.

Table 7.2.3.1/1: Diameter SWm AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
APN-Configuration	1430	8.2.3.7	Grouped	M			V	No
Mobile-Node-Identifier	tbd	5.2.3.2	OctetString	M			V	
MIP6-Feature-Vector	124	5.2.3.3	Unsigned64	M			V	
QoS-Capability	tbd	9.2.3.2.4	Grouped	M			V	No
RAT-Type	1032	5.2.3.6	Enumerated	M,V	P			Y
Visited-Network-Identifier	600	9.2.3.1.2	UTF8String	M,V				No

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, do not need to be supported.

Table 7.2.3.1/2: SWm re-used Diameter AVPs

Attribute Name	Reference	Comments
Auth-Request-Type	IETF RFC 3588 [7]	
Called-Station-Id	IETF RFC 4005 [4]	
EAP-Master-Session-Key	IETF RFC 4072 [5]	
EAP-Payload	IETF RFC 4072 [5]	
Re-Auth-Request-Type	IETF RFC 3588 [7]	
Session-Timeout	IETF RFC 3588 [7]	
User-Name	IETF RFC 3588 [7]	
MIP6-Agent-Info	draft-ietf-dime-mip6-integrated [6]	
APN-OI-Replacement	3GPP TS 29.272 [29]	

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

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 PMIPv6 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 3588 [7]).

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 PMIPv6 related mobility parameters in the chained tunnel cases.

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 section 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 3588 [7])	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	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 indicates the number of authentication vectors requested
Authentication Data	SIP-Auth-Data-Item	C	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 is 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	Contains the access network identifier used for key derivation at the HSS. (See 3GPP TS 24. 302 [26] for all possible values). Shall be present if the Authentication Method is EAP-AKA".
Access Type	RAT-Type	M	Contains the radio access technology that is serving the UE. (See 3GPP TS 29.212 [23] for all possible values)
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 GW, in authentication and authorization request. The AVP shall be transparently forwarded by the 3GPP AAA server.

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 indicates the authentication method It shall contain one of the values EAP-AKA or EAP-AKA'. EAP-AKA' is specified in IETF Draft draft-arkko-eap-aka-kdf [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 indicates the authentication method It shall contain one of the values EAP-AKA or EAP-AKA'.
Authorization Information	SIP-Authorization	M	It shall contain the concatenation of nonce, as sent to the terminal, and auts, as received from the terminal. Nonce 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 IETF RFC 3588 [7])	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 indicates 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 contains 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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

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	It shall contain one of the values EAP-AKA or EAP-AKA'.
Authentication Information AKA	SIP-Authenticate	M	It 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	It 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. 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 RAT-Type AVP. 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 check the request type.

     - If the request indicates there is a synchronization failure, 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 identical, 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 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. The Result-Code shall be set to DIAMETER_SUCCESS.

       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.

If the 3GPPP AAA Server name received in the request is identical to the 3GPP AAA Server name stored in HSS, 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 3GPP AAA Server name. 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] and shall download Authentication-Data-Item stored 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.

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. When the 3GPP AAA Server is going to remove the access information for a non-3GPP user (i.e. the STa, SWm, S6b sessions are terminated) or when the OCS has initiated a disconnection, the 3GPP AAA Server informs the HSS about an ongoing disconnection process and the HSS de-registers the non-3GPP user.
- 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 PGW identity as a result of PDN connection establishment or PDN disconnection over the non-3GPP access.

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 3588 [7])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Server Assignment Type	Server-Assignment-Type	M	Type of procedure the 3GPP AAA Server requests in the HSS. When this IE contains REGISTRATION value, the HSS performs a registration of the non-3GPP user. When this IE contains USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / AUTHENTICATION_FAILURE the HSS de-registers the non-3GPP user. When this IE contains AAA_USER_DATA_REQUEST value, the HSS downloads the subscriber user profile towards the 3GPP AAA Server as part of 3GPP AAA Server initiated profile download request, but no registration is performed. When this IE contains PGW_UPDATE value, the HSS checks if the stored 3GPP AAA server name is the currently registered 3GPP AAA server for this same user and updates the PGW identity for the non-3GPP user. Any other value is 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 is 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 is included with the suitable HSS address and it is stored in the 3GPP AAA Server for further usage.
PGW identity	MIP6-Agent-Info	C	This IE contains the PDN GW identity reallocated and is included if the Server-Assignment-Type is set to PGW_UPDATE. When notifying the HSS about removal of PDN GW for an APN, then this AVP shall not be included.
Context Identifier	Context-Identifier	O	This parameter shall identify the APN for the reallocated or removed PDN GW, and it may be included if it is available and the Server-Assignment-Type is set to PGW_UPDATE.
APN Id	Service-Selection	C	This information element contains the APN, and it shall be included if 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 3588 [7])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Registration result	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which contains 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	Relevant user profile. Section 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 contains 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.

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. Check the Server Assignment Type value received in the request:

   - If it indicates REGISTRATION, the HSS shall check that the 3GPP AAA Server name stored for the subscriber matches the 3GPP AAA Server name received in the request, 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 APN context of the Wildcard APN.

   - If it indicates USER_DEREGISTRATION / ADMINISTRATIVE_DEREGISTRATION / REAUTHENTICATION_FAILURE, the HSS shall remove the 3GPP AAA Server name previously assigned for the 3GPP 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.

   - If it indicates AAA_USER_DATA_REQUEST, 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, and it matches the 3GPP AAA Server address received in the 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 there is a 3GPP AAA Server already serving the user, and it does not match the 3GPP AAA Server address received in the request, the HSS shall return the old 3GPP AAA Server address to the requester 3GPP AAA Server. The Result-Code shall be set to DIAMETER_SUCCESS.

       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 to the entity that requested the authentication the 3GPP AAA Server name where to address the new request. The redirect shall be limited only to that specific request.

     - If there is not a 3GPP AAA Server serving the user, the HSS shall return an error, setting the Result-Code to DIAMETER_UNABLE_TO_COMPLY in the Response command.

   - If it indicates PGW_UPDATE, the HSS shall check that the 3GPP AAA Server name stored for the subscriber matches the 3GPP AAA Server name received in the request, store the PGW identity (if it is received in the command) or delete the existing PGW identity (if it is not 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. If the APN corresponding to the PGW identity is not present in the subscription but a wild card APN is present in the subscription, the HSS shall store the new PDN GW for an APN if present in the request or delete the stored PDN GW for an APN and the APN itself if the PDN GW Identity IE is not 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 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.

Once the 3GPP AAA server has received the user profile data as a result of successful registration to the HSS, the 3GPP AAA server shall create appropriate routing policies and IP filtering information according to the retrieved operator defined barring information. These routing policies and IP filtering information are used for the subsequent authorizations by the MAG functionality in the trusted 3GPP/IP access, or ePDG or PGW. 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 AAA shall not store this APN data beyond the lifetime of the UE sessions related to the specific APN and the AAA shall delete them upon disconnection of the UE.

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 3588 [7])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
Reason for de-registration	Deregistration-Reason	M	The HSS shall send to the 3GPP AAA server a reason for the de-registration. The de-registration reason is 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	The 3GPP AAA server name is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server,

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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

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. 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.

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] and 3GPP TS 32.422 [32], 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.

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.

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 3588 [7])	M	This information element shall contain the user IMSI, formatted according to 3GPP TS 23.003 [14], clause 2.2.
User profile	Non-3GPP-User-Data	M	Updated user profile. Section 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	The 3GPP AAA Server name is obtained from the Origin-Host AVP, which is received from the 3GPP AAA Server

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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for SWx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

8.1.2.3.2 HSS Detailed behaviour

The HSS shall make use of this procedure to update relevant user profile in the 3GPP AAA server, or activate / deactivate subscriber and equipment trace in the PDN GW.

8.1.2.3.3 3GPP AAA Server Detailed behaviour

The 3GPP AAA server shall overwrite, for the subscriber identity indicated in the request, current information with the information received from the HSS, except in the error situations detailed in table 8.1.2.3.3/1.

After a successful user profile download, the 3GPP AAA server shall initiate re-authentication procedure as described in sub-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 3GPP IP Access then the 3GPP AAA server shall initiate a re-authorization procedure as described in sub-clause 5.1.2.3.

Following a successful user profile download, the 3GPP AAA server shall apply routing policies and IP filtering information as described in clause 8.1.2.2.2. . As multiple authorization sessions may exist for the user (see section 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.

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.

8.2 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 XXX.

Editor's Note: A new application Id needs to be requested from IANA.

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 section 8.1.2.1.

Message Format

```
< Multimedia-Auth-Request > ::=  < Diameter Header: 303, REQ, PXY, XXX >
                                 < Session-Id >
                                 { 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 ]
                                 …
                                 *[ 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 section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

Message Format

```
< Multimedia-Auth-Answer > ::=  < Diameter Header: 303, PXY, XXX >
                                < Session-Id >
                                { 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 ]
                                …
                                *[ AVP ]
```

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 section 8.1.2.3.

Message Format

```
< Push-Profile-Request > ::=    < Diameter Header: 305, REQ, XXX >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Host }
                                { Destination-Realm }
                                { User-Name }
                                [ Non-3GPP-User-Data ]…
                                *[ 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 section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

Message Format

```
< Push-Profile-Answer > ::=     < Diameter Header: 305, PXY, YYY >
                                < Session-Id >
                                { Vendor-Specific-Application-Id }
                                [ Result-Code ]
                                [ Experimental-Result ]
                                { Auth-Session-State }
                                { Origin-Host }
                                { Origin-Realm }
                                …
                                *[ AVP ]
```

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 section 8.1.2.2.2.

Message Format

```
< Server-Assignment-Request > ::=     < Diameter Header: 301, REQ, PXY, XXX >
                                      < Session-Id >
```

{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
[Service-Selection]
[Context-Identifier]
[MIP6-Agent-Info]
{ User-Name}
{ Server-Assignment-Type }
…
*[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 or user profile download procedure. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

Message Format

< Server-Assignment-Answer > ::= < Diameter Header: 301, PXY, YYY >
< Session-Id >
{ 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]
…
*[AVP]

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 section 8.1.2.2.3.

Message Format

<Registration-Termination-Request> ::= < Diameter Header: 304, REQ, PXY, XXX >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
{ Deregistration-Reason }
…
*[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 section 6.2 of 3GPP TS 29.229 [24] in addition to the values defined in RFC 3588 [7].

Message Format

```
<Registration-Termination-Answer> ::=  < Diameter Header: 304, PXY, XXX >
                                       < Session-Id >
                                       { Vendor-Specific-Application-Id }
                                       [ Result-Code ]
                                       [ Experimental-Result ]
                                       { Auth-Session-State }
                                       { Origin-Host }
                                       { Origin-Realm }
                                       …
                                       *[ AVP ]
```

8.2.3 Information Elements

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 ]
                        *[ AVP ]
```

The AMBR included in this grouped AVP shall include the AMBR associated to the user"s subscription (UE-AMBR).

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. In that specific case, the Trace-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 IMSI and MSISDN values. This grouped AVP shall set the sub-AVP Subscription-Id-Type to value "END_USER_E164" or to value "END_USER_IMSI" and shall set the sub-AVP Subscription-Id-Data to the MSISDN value.

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 barring of 3GPP - non-3GPP interworking subscription. The following values are defined:

NON_3GPP_SUBSCRIPTION_ALLOWED (0)

The subscriber has non-3GPP subscription to access EPC network.

NON_3GPP_SUBSCRIPTION_BARRED (1)

The subscriber has no non-3GPP subscription to access EPC 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

This AVP is defined is chapter 5.2.3.6 and it shall include thef access technology types not allowed for the user.

8.2.3.6 Session-Timeout

The Session-Timeout AVP is of type Unsigned32. It is defined in IETF RFC 3588 [7] 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].

MIP6-Agent-Info is defined in section 9.2.3.2.2.

PDN-Type is defined in 3GPP TS 29.272 [29].

Served-Party-IP-Address is defined in 3GPP TS 32.299 [30].

3GPP-Charging-Characteristics is defined in 3GPP TS 29.061 [31].

The AVP format shall conform as follows:

```
APN-Configuration ::=   < AVP Header: 1430 10415 >
                        { Context-Identifier }
                        { Service-Selection }
                        { PDN-Type }
                        *2[ Served-Party-IP-Address ]
                        [ MIP6-Agent-Info ]
                        [ PDN-GW-Allocation-Type]
                        [ VPLMN-Dynamic-Address-Allowed ]
                        [ EPS-Subscribed-QoS-Profile ]
                        [ 3GPP-Charging-Characteristics ]
                        [ AMBR ]
                        *[ Specific-APN-Info ]
                        *[ AVP ]
```

The AMBR included in this grouped AVP shall include the AMBR associated to this specific APN configuration (APN-AMBR).

The Specific-APN-Info contains the APN which is not present in the subscription context but the UE is authorized to connect to and the identity of the registered PDN-GW. For details, see 3GPP TS 29.272 [29].

8.2.3.8 ANID

The ANID AVP is defined in chapter 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.

8.2.3.13 Trace-Info

The Trace-Data 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.

8.2.3.14 Trace-Data

The Trace-Data AVP is of type Grouped. The Diameter AVP is defined 3GPP TS 29.272 [29], while its contents is defined in 3GPP TS 32.422 [32].

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 3588 [7]. 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 3588 [7]. 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 shall forward the Diameter request directly to the 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 and H2 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 reference point in the PMIPv6 mode, the S6b reference point is used to update the 3GPP AAA server or the 3GPP AAA proxy with the PDN-GW address information. 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 H2 reference point is defined between the 3GPP AAA Server and the HA. The definition of the reference point and its functionality is given in 3GPP TS 23.327 [12].

NOTE: The H2 interface is a subset of the S6b interface in the sense that only the DSMIPv6 procedures and the respective AVPs are implemented. Therefore, in the context of DSMIPv6 the procedures described in this specification apply to both S6b and H2.

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 Draft draft-ietf-dime-mip6-split [11].

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 contains the identity of the user
Authentication Request Type	Auth-Request-Type	M	Defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_AUTHENTICATE is required in this case.
EAP Payload	EAP-Payload	M	Encapsulated payload for UE – 3GPP AAA Server mutual authentication
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This IE shall be present if the PDN GW is not in the UE's home network.
Access Type	RAT-Type	C	This Information Element contains 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 contains the address of the selected PGW for the UE and the corresponding PDN connection. It includes the FQDN and/or IPv6 address(es) of the selected PDN GW for the APN 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 informs the 3GPP AAA Server about the used mobility protocol. The MIP6_SPLIT flag shall be set.
APN	Service-Selection	O	Contains the APN information extracted from the IKE_AUTH message. Includes 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	If included in the request message, indicates 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.

Table 9.1.2.1/2: Authentication and Authorization Answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
EAP Payload	EAP-Payload	M	Encapsulated payload for UE – 3GPP AAA Server mutual authentication
Master Session Key	EAP-Master-Session-Key	C	Keying material for protecting the communication between the UE and PDN GW. Present if result code is success.
Result Code	Result-Code / Experimental-Result-Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ. The Result-Code DIAMETER_MULTI_ROUND_AUTH is used in the responses that trigger further requests from the PDN GW and DIAMETER_SUCCESS is included at the successful completion of the authentication and authorization procedure. Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which contains 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 Draft draft-ietf-dime-mip6-split [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. The MIP6_SPLIT flag shall be set.
Current User Identity	Mobile-Node-Identifier	M	Contains the UE identity.
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 and PDN GW 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) - PGW identity - Allowed PDN type (IPv4, IPv6 or IPv4v6) - APN-AMBR If the 3GPP AAA server has retrieved a PGW identity from the HSS, it shall include it in this AVP.
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 contains 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 includes 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 is set to 0.
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]).
3GPP AAA Server Name	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 identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). 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 is 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 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-List - Trace-Event-List - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List: if this AVP is not present, trace report generation is requested for all interfaces listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW (3)". If this AVP is not included, trace activation in PDN GW is required.

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].

The PDN GW shall utilize the downloaded APN configuration data, among others, to decide whether the user's request for an IPv4 home address shall be accepted or rejected.

If 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].

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]. For H2, the 3GPP AAA server shall process the DER message according to 3GPP TS 33.234 [33].

Upon successful completion, a DIAMETER_SUCCESS shall be returned to indicate successful authentication procedure and authentication information shall be returned. 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 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 identity of the 3GPP AAA Server currently serving the user (as indicated in the 3GPP-AAA-Server-Name AVP returned in the SWx authentication response 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.

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).

9.1.2.2 Authorization Procedures when using PMIPv6

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.

The PDN GW shall update its address information to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time.

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 Draft draft-korhonen-dime-pmip6 [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	Set to the NAI identifier of the UE as specified in 3GPP TS 23.003 [14].
Authentication Request Type	Auth-Request-Type	M	Defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY is required in this case.
PDN GW Identity	MIP6-Agent-Info	O	This IE contains the address and possibly the FQDN of the selected PDN GW for the UE and the corresponding PDN connection
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDN GW is not in the UE's home network.
Mobility features	MIP6-Feature-Vector	M	Contains the mobility features supported by the PDN GW. The PMIP6_SUPPORTED flag shall be set.
APN	Service-Selection	M	Contains the APN information extracted from the PBU.
QoS capabilities	QoS-Capability	O	If included in the request message, it indicates 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.

Table 9.1.2.2.1/2: Authorization answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result code	Result-Code	M	Result of the operation. The possible values of the Result-Code AVP are defined in IETF RFC 3588 [7]. Set to DIAMETER_SUCCESS if the authorization of a MAG or the update to the PDN GW address succeeded. Set to DIAMETER_AUTHORIZATION_REJECTED is the authorization of a new MAG or the update of the PDN GW address failed.
Authorized mobility features	MIP6-Feature-Vector	C	The 3GPP AAA Server shall insert this AVP if the authorization was successful. The PMIP6_SUPPORTED flag shall be set.
Session time	Session-Timeout	C	If the authorization succeeded, then this IE contains 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 including the following information elements: - APN - Authorized 3GPP QoS profile - APN-AMBR
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 includes 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 is set to 0.
3GPP AAA Server Name	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 identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). 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 is included 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-List - Trace-Event-List - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List: if this AVP is not present, trace report generation is requested for all interfaces listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW (3)". If this AVP is not included, trace activation in PDN GW is required.

9.1.2.2.2 PDN GW Detailed Behaviour

Upon receipt of a PBU message from the MAG, 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 etc.

The PDN GW shall include in the request the APN where the user shall be connected to.

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 MAG, for instance) shall not include it again.

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 proceed to connect the user to the specified APN, and will send the PBA message to the MAG.

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].

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 update the PDN GW information for the APN for the UE on the HSS.

The 3GPP AAA Server must 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, then the3GPP AAA Server shall include the Service-Selection AVP in the authorization answer and set the Result-Code to DIAMETER_SUCCESS.
  - 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 data from the HSS as specified for the SWx reference point. 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 identity of the 3GPP AAA Server currently serving the user (as indicated 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 GW may have sent PBU without authorizing the user.

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, and therefore the mobility session established for this PDN connection is to be removed.

The procedure shall be initiated by the PDN GW and removes PDN GW information from the 3GPP AAA server. These procedures are based on the reuse of Diameter Base IETF RFC 3588 [7] STR and STA commands.

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 contains the identity of the user.
Termination Cause	Termination-Cause	M	Contains the reason for the disconnection.

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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for S6b errors.

9.1.2.3.2 PDN GW Detailed Behaviour

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 contains the identity of the user.
Auth-Session-State	Auth-Session-State	O	This information element indicates 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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which contains 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 contains 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	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, the PDN GW shall initiate a termination procedure for the associated PDN connection, and shall release any resource allocated to it.

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

3GPP 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 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.

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. This procedure is based on the reuse of Diameter Base IETF RFC 3588 [7] RAR and RAA commands. The information element content for these messages is shown in tables 9.1.2.2.1/1 and 9.1.2.2.1/2.

2. After receiving the re-authorization request, the PDN GW invokes for the indicated APN. The authorization procedure for PMIPv6 is described in the section 9.1.2.2 (Service Authorization). Tables 9.1.2.2.1/3 and 9.1.2.2.1/4 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 contains the identity of the user
Request Type	Re-Auth-Request-Type	M	Defines whether re-authentication or re-authorization is required. AUTHORIZE_ONLY is required in this case.

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	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 9.1.2.5/3: Authorization Request when using DSMIPv6

Information Element Name	Mapping to Diameter AVP	Cat.	Description
User identity	User-Name	M	This information element contains the identity of the user
Authentication Request Type	Auth-Request-Type	M	Defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY is required in this case.
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDN GW is not in the UE's home network.
Access Type	RAT-Type	M	Contains the non-3GPP access network technology type that is serving the UE.
PDN GW Identity	MIP6 -Agent-Info	M	This IE contains the address of the selected PGW for the UE and the corresponding PDN connection. It includes the FQDN and/or IP address(es) of the selected PDN GW for the APN that the user shall be connected to.
APN	Service-Selection	O	Contains the APN information extracted from the IKE_AUTH message. Includes 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, indicates to the 3GPP AAA server that the PGW capable of downloading a static QoS profile for the UE. The PGW includes this IE only during UE the initial attach.

Table 9.1.5.1/4: Authorization Answer when using DSMIPv6

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result Code	Result-Code / Experimental-Result-Code	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol or as per in NASREQ. 1xxx should be used for multi-round, 2xxx for success. Experimental-Result AVP shall be used for S6b errors. This is a grouped AVP which contains 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 Draft draft-ietf-dime-mip6-split [11], then the 3GPP AAA server is indicating to the PGW that it shall initiate a HA switch procedure towards the UE.
Current User Identity	Mobile-Node-Identifier	M	Contains the UE identity in EPS.
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 and PDN GW 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) - PDN GW identity. - PDN GW allocation type - VPLMN Dynamic Address Allowed If the PDN GW Identity (MIP6-Agent-Info AVP) is present and the Result-Code AVP is set to DIAMETER_SUCCESS_RELOCATE_HA, then the 3GPP AAA Server is indicating to the PDN GW that it shall initiate a HA switch procedure towards the UE. The address of the assigned PDN GW is defined in the MIP-Home-Agent-Address AVP.
Session Time	Session-Timeout	C	If the authentication and authorization succeeded, then this IE contains the time this authorization is valid for.
QoS resources	QoS-Resources	C	If the authentication and authorization succeeded, then the 3GPP AAA server includes 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 is set to 0. This IE contains the QoS Profile authorized by the 3GPP AAA server for the requested APN based on the subscribed QoS parameters.
Trace information	Trace-Info	C	This AVP is 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-List - Trace-Event-List - Trace-Collection-Entity The following AVPs may also be included in the Trace-Data AVP: - Trace-Interface-List: if this AVP is not present, trace report generation is requested for all interfaces listed in 3GPP TS 32.422 [32] - Trace-NE-Type-List, with the only allowed value being "PDN GW (3)". If this AVP is not included, trace activation in PDN GW is required.

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.

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, the PDN GW shall perform an authorization procedure as described in section 9.1.2.2.
   - 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.
3. If it indicates AUTHORIZE_AUTHENTICATE, Result-Code shall be set to DIAMETER_INVALID_AVP_VALUE.

When receiving the authorization request, 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 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].

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 address information to the 3GPP AAA Server and HSS. Static QoS profile information may also be downloaded at the same time.

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	Set to the NAI identifier of the UE as specified in 3GPP TS 23.003 [14].
Authentication Request Type	Auth-Request-Type	M	Defines whether the UE is to be authenticated only, authorized only or both. AUTHORIZE_ONLY is required in this case.
PDN GW Identity	MIP6-Agent-Info	O	This IE contains the address and possibly the FQDN of the selected PDN GW for the UE and the corresponding PDN connection
Visited Network Identifier	Visited-Network-Identifier	C	Identifier that allows the home network to identify the Visited Network. This AVP shall be present if the PDN GW is not in the UE's home network.
Mobility features	MIP6-Feature-Vector	M	Contains the mobility features supported by the PDN GW. The MIP4_SUPPORTED flag shall be set
APN	Service-Selection	M	Contains the APN information extracted from the PBU.
QoS capabilities	QoS-Capability	O	If included in the request message, it indicates 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.

Table 9.1.2.6.1/2: Authorization answer

Information Element Name	Mapping to Diameter AVP	Cat.	Description
Result code	Result-Code	M	Result of the operation. The possible values of the Result-Code AVP are defined in IETF RFC 3588 [7]. Set to DIAMETER_SUCCESS if the authorization of a MAG or the update to the PDN GW address succeeded. Set to DIAMETER_AUTHORIZATION_REJECTED is the authorization of a new MAG or the update of the PDN GW address failed.
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 contains 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 includes 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 is set to 0.
3GPP AAA Server Name	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 identity of the 3GPP AAA Server currently serving the user. The node receiving this IE shall behave as defined in the Diameter Base Protocol (IETF RFC 3588 [7]). The command shall contain zero or one occurrence of this information element.

9.1.2.6.2 PDN GW Detailed Behaviour

Upon receipt of a RRQ message from the MAG, 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 etc.

The PDN GW shall include in the request the APN where the user shall be connected to.

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 MAG, for instance) shall not include it again.

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 proceed to connect the user to the specified APN, and will send the PBA message to the MAG.

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. Optionally, it may retrieve user data for the subscriber for the APN and shall return it in the AAA response to the PDN GW.

The 3GPP AAA Server must check that the user exists. If not, the 3GPP AAA Server shall use the procedures defined for the SWx interface to retrieve the user profile, including the list of authorized APNs for that user.

If the HSS returns DIAMETER_SUCCESS, and the APN requested by the PDN GW is included in the list of authorized APNs, then the same status code shall be returned to the PDN GW to indicate successful authorization.

If the HSS returns DIAMETER_SUCCESS, but 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 HSS returns DIAMETER_ERROR_USER_UNKNOWN, the 3GPP AAA Server shall return the same error to the PDN GW.

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 3588 [7] 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 Draft draft-korhonen-dime-pmip6 [2], which defines a Diameter extensions and application for PMIPv6 MAG to AAA and LMA to AAA interfaces.
- IETF Draft draft-ietf-dime-qos-attributes [9], which defines attribute value pairs to convey QoS information between Diameter peers.

The LMA to 3GPP AAA server or the LMA to 3GPP AAA proxy communication shall use the LMA to AAA interface functionality defined in IETF Draft draft-korhonen-dime-pmip6 [2] to update the 3GPP AAA server with PDN GW identity, and optionally to retrieve mobility related parameters and static QoS profiles.

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 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, draft-ietf-dime-mip6-split [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 Draft draft-ietf-dime-mip6-split [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 or HA shall act as the NAS, as described in 3GPP TS 33.234 [10].

Editor"s Note: The Application Id to be advertised over the S6b reference point is to be assigned by IANA.

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 Draft draft-ietf-dime-mip6-split [11].

```
< Diameter-EAP-Request > ::= < Diameter Header: 268, REQ, PXY >
                             < Session-Id >
                             { 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 ]
                             ...
                            *[ 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 Draft draft-ietf-dime-mip6-split [11].

```
<Diameter-EAP-Answer> ::= < Diameter Header: 268, PXY >
                          < Session-Id >
                          { Auth-Application-Id }
                          { Auth-Request-Type }
                          { Result-Code }
                          { Origin-Host }
                          { Origin-Realm }
                          [ User-Name ]
                          [ EAP-Payload ]
                          [ EAP-Master-Session-Key ]
                          [ Mobile-Node-Identifier ]
                          [ APN-Configuration ]
                          [ MIP6-Agent-Info ]
                          [ MIP6-Feature-Vector ]
                          [ 3GPP-Charging-Characteristics ]
                          *[ QoS-Resources ]
                          *[ Redirect-Host ]
                          [ Trace-Info ]
                          ...
                          *[ AVP ]
```

9.2.2.2 Commands for S6b PMIPv6 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 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 >
                          < Session-Id >
                          { Auth-Application-Id }
                          { Origin-Host }
                          { Origin-Realm }
                          { Destination-Realm }
                          { Auth-Request-Type }
                          [ User-Name ]
                          [ MIP6-Agent-Info ]
                          [ MIP6-Feature-Vector ]
                          [ QoS-Capability ]
                          [ Service-Selection ]
                          ...
                          *[ 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 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 >
                         < Session-Id >
                         { Auth-Application-Id }
                         { Auth-Request-Type }
                         { Result-Code }
                         { Origin-Host }
                         { Origin-Realm }
                         ...
                         [ MIP6-Feature-Vector ]
                         [ Session-Timeout ]
                         [ QoS-Resources ]
                         *[ Redirect-Host ]
                         [ Trace-Info ]
                         ...
                         *[ 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 3588 [7] 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 >
                                     < Session-Id >
                                     { Auth-Application-Id }
                                     { Origin-Host }
                                     { Origin-Realm }
                                     { Destination-Realm }
                                     { Termination-Cause }
                                     [ User-Name ]
                                     …
                                     *[ 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 3588 [7] Session-Termination-Answer command.

```
<Session-Termination-Answer> ::=     < Diameter Header: 275, PXY >
                                     < Session-Id >
                                     { Result-Code }
                                     { Origin-Host }
                                     { Origin-Realm }
                                     *[ 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 >
                                 < Session-Id >
                                 { 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 >
                                < Session-Id >
                                { 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 3588 [7] Session-Termination-Request command.

```
<Session-Termination-Request> ::=   < Diameter Header: 275, REQ, PXY, 16777250 >
                                < Session-Id >
                                { Origin-Host }
                                { Origin-Realm }
                                { Destination-Realm }
                                { Auth-Application-Id }
                                { Termination-Cause }
                                [ User-Name ]
                                …
                                *[ 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 3588 [7] Session-Termination-Answer command.

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

9.2.2.5 Commands for S6b MIPv4 Authorization Procedures

9.2.2.5.1 AA-Request (AAR) Command

The ABNFs definition for the PMIP mobility protocol in clause 9.2.2.2.1 applies.

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 >
                            < Session-Id >
                            { Origin-Host }
                            { Origin-Realm }
                            { Destination-Realm }
                            { Destination-Host }
                            { Auth-Application-Id }
                            { Re-Auth-Request-Type }
                            [ User-Name ]
                            ...
                            *[ 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 >
                            < Session-Id >
                            { Result-Code }
                            { Origin-Host }
                            { Origin-Realm }
                            [ User-Name ]
                            ...
                            *[ AVP ]
```

9.2.3 Information Elements

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**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
MIP6-Agent-Info	486	9.2.3.2.2	Grouped	M			V	No
MIP6-Feature-Vector	124	9.2.3.2.3	Unsigned64	M			V	No
Visited-Network-Identifier	600	9.2.3.1.2	UTF8String	M, V				No
QoS-Capability	tbd	9.2.3.2.4	Grouped	M			V	
QoS-Resources	tbd	9.2.3.2.5	Grouped	M			V	
Trace-Info	1505	8.2.3.13	Grouped	V	M			No

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

9.2.3.1.3 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 Draft draft-ietf-dime-mip6-integrated [6] and extended by IETF Draft draft-ietf-dime-mip6-split-12 [11].

Following capabilities are supported on S6b reference point in DSMIPv6 mode:

- MIP6_SPLIT (0x0000000100000000)
  This flag shall be set by the PDN GW and by the 3GPP AAA Server. When this flag is set, it shows that DSMIPv6 mobility protocol is used on the S2c interface.

9.2.3.2 S6b PMIPv6 procedures

9.2.3.2.1 General

The following table describes the Diameter AVPs defined for the S6b interface protocol in PMIPv6 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

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
MIP6-Agent-Info	486	9.2.3.2.2	Grouped	M			V	No
MIP6-Feature-Vector	124	9.2.3.2.3	Unsigned64	M			V	No
QoS-Capability	Tbd	9.2.3.2.4	Grouped	M			V	No
QoS-Resources	Tbd	9.2.3.2.5	Grouped	M			V	No
Trace-Info	1505	8.2.3.13	Grouped	V	M			No

9.2.3.2.2 MIP6-Agent-Info

The MIP6-Agent-Info AVP contains the PDN GW address information or (for the chained S2 - PMIP based S8 case) the Serving GW address information. This AVP is defined in IETF RFC 5447 [6]. 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 ]
```

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 mode:

- PMIP6_SUPPORTED
- IP4_HOA_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 Draft draft-ietf-dime-qos-attributes [9].

Editor"s Note: The description of this AVP will change slightly when the new version of the draft becomes available.

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 Draft draft-ietf-dime-qos-attributes [9].

Editor"s Note: The description of this AVP will change slightly when the new version of the draft becomes available.

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. 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 3588 [7]).

Annex A (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2008-12	CT#42	CP-080717			V2.0.0 approved in CT#42	2.0.0	8.0.0
2009-03	CT#43	CP-090051	0002	2	Clarification on QoS Resource on S6b	8.0.0	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 section 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		
		CP-090289	0084	1	Use of Access-Restriction-Data AVP	8.1.0	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		

History

Document history		
V8.0.0	January 2009	Publication
V8.1.0	April 2009	Publication
V8.2.0	June 2009	Publication