

IPWorks 3GPP AAA Server-HSS SWx Interface

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2011-2016. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document IPWorks Trademark Information.



Contents

1	Introduction	1
1.1	Prerequisites	1
1.2	Related Information	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	4
3	Procedures	5
3.1	Authentication	5
3.2	Location Management	6
3.3	Network Initiated De-registration by HSS	6
3.4	HSS Initiated Update of User Profile	7
3.5	HSS Initiated P-CSCF Restoration	8
4	Information Model	11
4.1	General	11
4.2	Authentication	11
4.3	Location Management	12
4.4	Network Initiated De-Registration by HSS	18
4.5	HSS Initiated Update of User Profile	19
5	Diameter AVPs	21
5.1	IETF Protocol AVPs	21
5.2	3GPP AVPs	23
6	Formal Syntax	39
7	Related Standards	41
	Reference List	43





1 Introduction

This document describes the SWx interface between the 3GPP AAA server and the HSS.

Scope

The scope of this document includes the SWx interface protocol described in TS 29.273. Now the SWx interface only support 3GPP AAA server initiated diameter request message.

This document covers the following topics:

- Interface Overview
- Interface Role
- Services
- Encapsulation and Addressing
- Procedures
- Information Model
- Diameter AVPs
- Formal Syntax
- Related Standards

Target Groups

This document is intended for personnel needing to understand the logical entity, including interfaces and protocols, of the IPWorks.

1.1 Prerequisites

Not Applicable.

1.2 Related Information

Trademark information, typographic conventions, definition and explanation of acronyms and terminology can be found in the following documents:

- Glossary of Terms and Acronyms, Reference [1]
- Trademark Information, Reference [2]



— Typographic Conventions, Reference [3]

The standard, related to the S6b interface, can be found in the section Reference.



2 Interface Overview

The SWx interface is defined between the 3GPP AAA server and HSS. The interface is used by the 3GPP AAA server to fetch authentication vectors and user profiles from the HSS. The 3GPP AAA server uses the interface to register and deregister users in the HSS when the Trusted Non-3GPP IP Access Network executes the authentication and authorization process. It is also used to update the PDN GW information in HSS when PDN GW executes the authorization process.

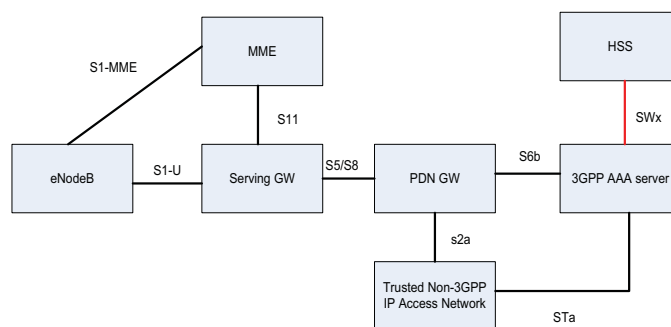


Figure 1 SWx Interface Entities

2.1 Interface Role

In the SWx interface, the IPWorks AAA server will take the role of 3GPP AAA server in EPC network.

2.2 Services

This section describes the services that the SWx Interface offers.

The services offered by the SWx interface are shown in Table 1.

Table 1 Offered Services

Offered Service	Description
Authorization , Authentication	<p>The 3GPP AAA Server is used to authenticate/authorize the UE from Non-3GPP IP Access Network:</p> <ul style="list-style-type: none"> • Authenticate/Authorize the UE from Trusted/Untrusted Non-3GPP IP Access Network. • Convey the PDN GW message. • Register PDN GW/3GPP AAA to HSS and download user profile.



2.3 Encapsulation and Addressing

The following lower level protocols are used on this interface:

- SCTP
- TCP
- DIAMETER



3 Procedures

This section describes the procedures used in connection with the offered and used interfaces of IPWorks:

- Authentication
- Location management
- Network initiated de-registration by HSS
- HSS initiated update of user profile

3.1 Authentication

This procedure is triggered when the 3GPP AAA server authenticates and fetches the authentication vector from the HSS.

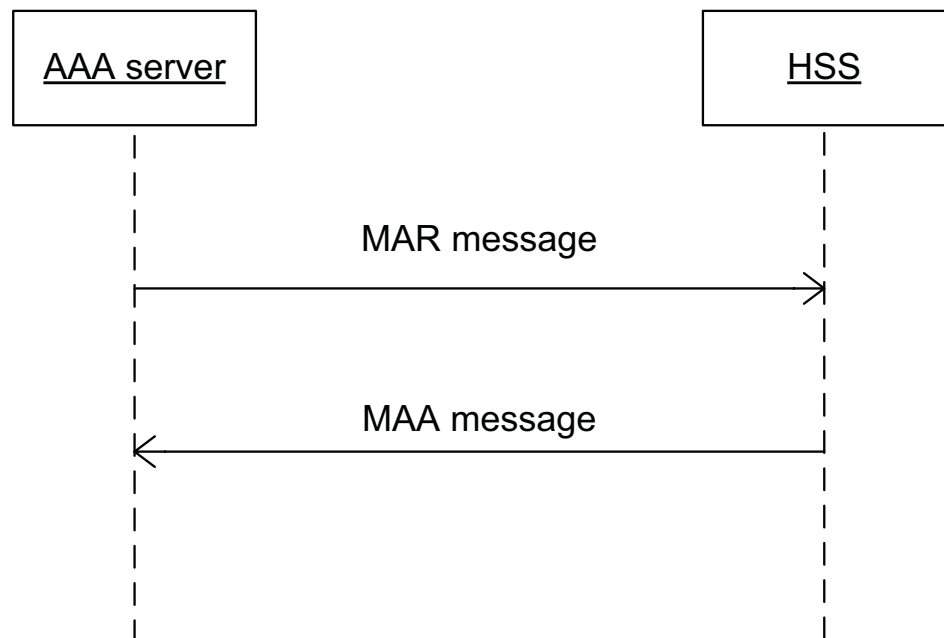


Figure 2 Authentication procedure

3.2 Location Management

The location management includes the following procedure:

- Fetch user profile procedure
- Register and deregister user procedure
- Update PDN GW information procedure
- Error notification to HSS

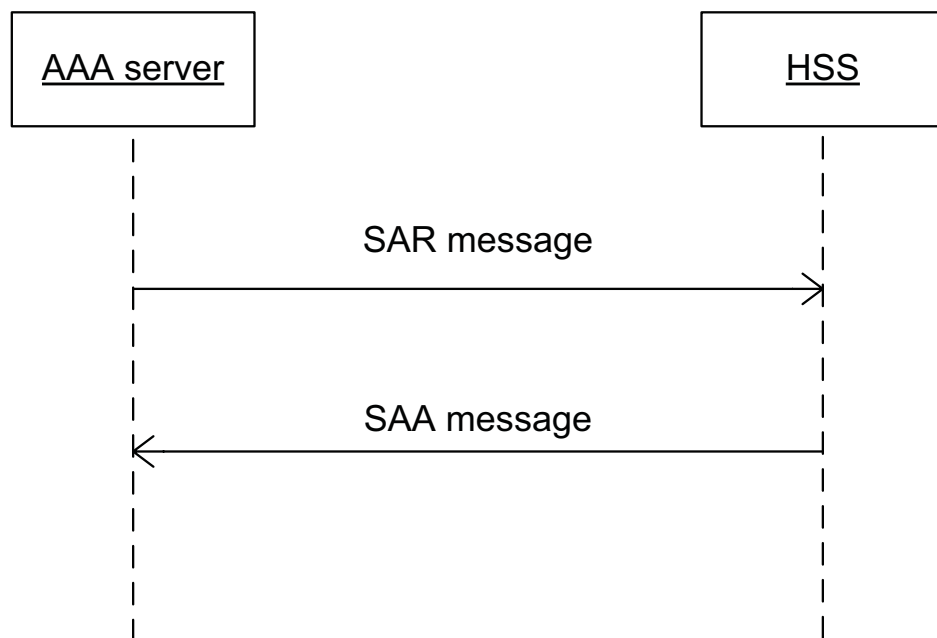


Figure 3 Location management procedure

3.3 Network Initiated De-registration by HSS

The procedure is triggered by the HSS when a subscription is to be removed, including removing a previous registration and all associated states:

The HSS sends in the Deregistration-Reason AVP the reasons for the de-registration and a reason code that determines the action that AAA server must perform. The possible reason codes are listed as follows:

- PERMANENT_TERMINATION: The Non-3GPP subscription or service profile(s) has been permanently terminated.

- **NEW_SERVER_ASSIGNED**: The HSS indicates to the 3GPP AAA Server that a new 3GPP AAA Server has been allocated to the user.

The diameter messages are RTR and RTA (see Section 4.4 on page 18).

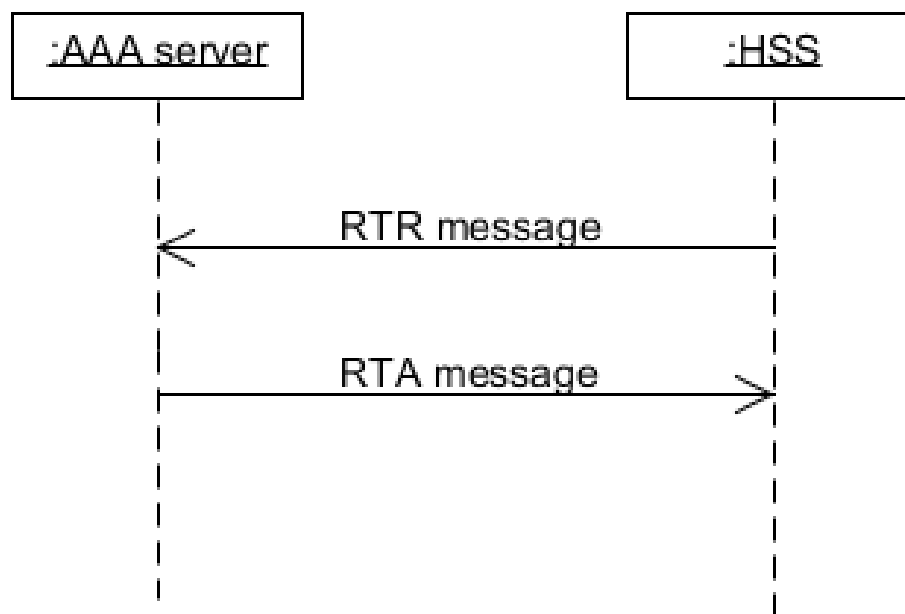


Figure 4 Network Initiated De-Registration by HSS

3.4 HSS Initiated Update of User Profile

The procedure is triggered by the HSS when the subscriber profile has been modified and needs to be sent to the 3GPP AAA Server.

Table 2 shows the functions supported by HSS and AAA:

Table 2 Functions Supported by HSS and AAA

Function	HSS	AAA
Updating the relevant user profile in the 3GPP AAA server	√	√
Activating or deactivating the subscriber and equipment trace	√	
Requesting identity	√	
Requesting location information	√	√
Requesting UE local time zone of the access network where the UE is currently attached	√	

The diameter messages are PPR and PPA (see Section 4.5 on page 19).

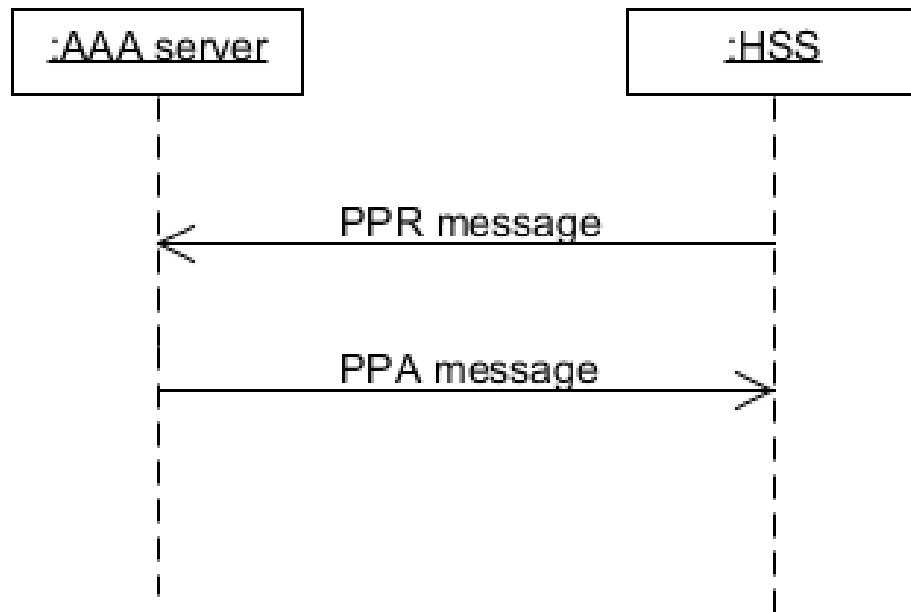


Figure 5 HSS Initiated Update of User Profile

3.5 HSS Initiated P-CSCF Restoration

The procedure is triggered by the HSS when the P-CSCF restoration is interrupted. A PPR message indicating P-CSCF restoration must be sent to the AAA server.

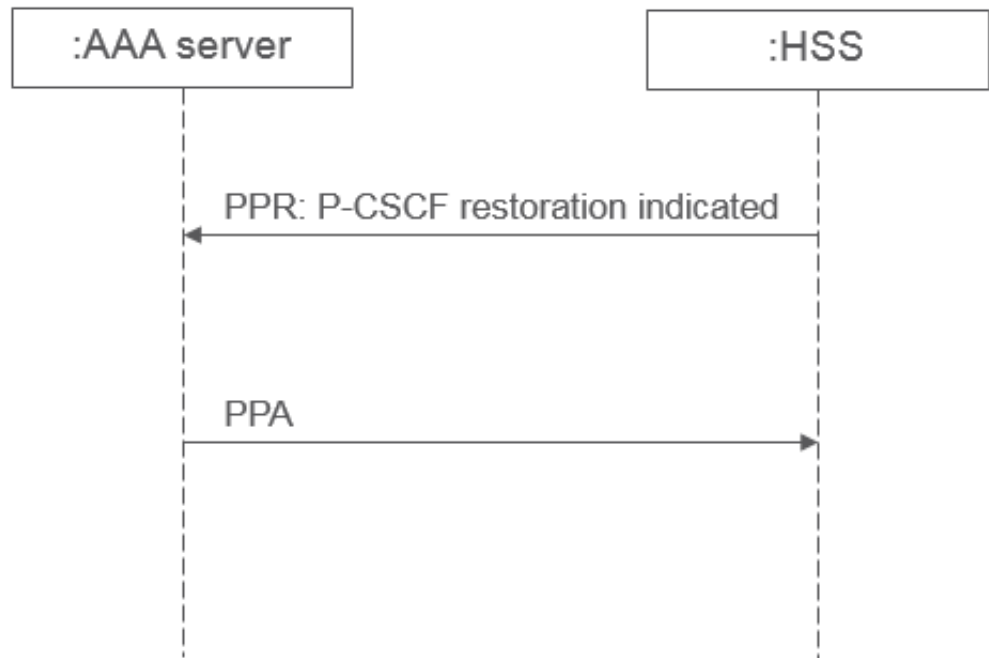


Figure 6 HSS Initiated P-CSCF Restoration





4 Information Model

This section describes the information model, including mandatory and optional parameters of each service operation.

4.1 General

This section describes the commands and the AVPs involved in the application. The description and format of the Base Protocol is described in Reference [4]. In this document, only the messages and the AVPs are described.

Table 3 indicates the Naur Form (ABNF) format in Augmented Backus.

Table 3 Naur Form (ABNF) format

{ }	Mandatory
< >	Mandatory with fixed place
[]	Optional
*	Zero or more Occurrences
*n	At most
n	Occurrences

4.2 Authentication

4.2.1 Multimedia-Authentication-Request (MAR) Command

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.

Message Format:

```

<Multimedia-Auth-Request> ::= <Diameter Header: 303, REQ, PXY,
                               16777265>
                               <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]
[AAA-Failure-Indication]
[Terminal-Information]
[SIP-Auth-Data-Item]
[SIP-Number-Auth-Items]
*[Supported-Features]
*[AVP]
```

4.2.2 Multimedia-Authentication-Answer (MAA) Command

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.

Message Format:

```
<Multimedia-Auth-Answer>::=<Diameter Header: 303, PXY, 16777265>
                                <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]
                                *[Supported-Features]
                                *[AVP]
```

4.3 Location Management

4.3.1 Fetching User Profile

4.3.1.1 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR), indicated by the Command-Code field set to 301 and the “R” bit set in the message flags field, is sent by the 3GPP AAA Server to HSS to request the registration, de-registration, user profile download or update the HSS with the PGW identity.

Message Format:



```

<Server-Assignment-Request>::=<Diameter Header: 301, REQ,
    PXY,16777265
    <Session-Id>
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    [Destination-Host]
    {Destination-Realm}
    [Service-Selection]
    [Context-Identifier]
    [MIP6-Agent-Info]
    [Visited-Network-Identifier]
    {User-Name}
    {Server-Assignment-Type}
    *[Supported-Features]
    *[AVP]

```

Server-Assignment-Type is AAA_USER_DATA_REQUEST.

4.3.1.2

Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA), indicated by the Command-Code field set to 301 and the “R” set to zero in the Command Flags field of the header, is sent by HSS in response to Server-Assignment-Request (SAR) command.

Message Format:

```

<Server-Assignment-Answer>::=<Diameter Header:301, PXY,16777265>
    <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]
    [Supported-Features]
    *[AVP]

```



4.3.2 Registering and De-registering User

4.3.2.1 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR), indicated by the Command-Code field set to 301 and the “R” bit set in the message flags field, is sent by the 3GPP AAA Server to HSS to request the registration, de-registration, user profile download or update the HSS with the PGW identity.

Message Format (for Registration):

```
<Server-Assignment-Request>::=<Diameter Header: 301, REQ,
    PXY,16777265>
    <Session-Id>
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    [Destination-Host]
    {Destination-Realm}
    {User-Name}
    {Server-Assignment-Type}
    [Terminal-Information]
    *[Supported-Features]
    *[AVP]
```

Server-Assignment-Type is REGISTRATION.

Message Format (for Deregistration):

```
<Server-Assignment-Request>::=<Diameter Header: 301, REQ,
    PXY,16777265>
    <Session-Id>
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    [Destination-Host]
    {Destination-Realm}
    {User-Name}
    {Server-Assignment-Type}
    *[AVP]
```

Server-Assignment-Type is USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION.



4.3.2.2 Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA), indicated by the Command-Code field set to 301 and the “R” set to zero in the Command Flags field of the header, is sent by HSS in response to Server-Assignment-Request (SAR) command.

Message Format (for Registration):

```
<Server-Assignment-Answer>::=<Diameter Header:301, PXY,16777265>
    <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]
    [Supported-Features]
    *[AVP]
```

Message Format (for Deregistration):

```
<Server-Assignment-Answer>::= <Diameter Header:301, PXY,16777265>
    <Session-Id>
    {Vendor-Specific-Application-Id}
    [Result-Code]
    [Experimental Result]
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    {User-Name}
    *[AVP]
```

4.3.3 Updating PDN GW Information

4.3.3.1 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR), indicated by the Command-Code field set to 301 and the “R” bit set in the message flags field, is sent by the 3GPP AAA Server to HSS to request the registration, de-registration, user profile download or update the HSS with the PGW identity.

Message Format (for update PDN GW Information):

```
<Server-Assignment-Request>::=<Diameter Header: 301, REQ,
    PXY,16777265>
```



```
<Session-Id>
{Vendor-Specific-Application-Id}
{Auth-Session-State}
{Origin-Host}
{Origin-Realm}
[Destination-Host]
{Destination-Realm}
[Service-Selection]
[Context-Identifier]
[MIP6-Agent-Info]
[Visited-Network-Identifier]
{User-Name}
{Server-Assignment-Type}
*[Supported-Features]
*[AVP]
```

Server-Assignment-Type is PGW_UPDATE.

Message Format (for remove PDN GW Information):

```
<Server-Assignment-Request>::=<Diameter Header: 301, REQ,
    PXY,16777265>
    <Session-Id>
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    [Destination-Host]
    {Destination-Realm}
    [Service-Selection]
    [Context-Identifier]
    [Visited-Network-Identifier]
    {User-Name}
    {Server-Assignment-Type}
    *[Supported-Features]
    *[AVP]
```

Server-Assignment-Type is PGW_UPDATE.

4.3.3.2 Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA), indicated by the Command-Code field set to 301 and the “R” set to zero in the Command Flags field of the header, is sent by HSS in response to Server-Assignment-Request (SAR) command.

Message Format (for update and remove PDN GW Information):

```
<Server-Assignment-Answer>::=<Diameter Header:301, PXY,16777265>
    <Session-Id>
```



```

{Vendor-Specific-Application-Id}
[Result-Code]
[Experimental Result]
{Auth-Session-State}
{Origin-Host}
{Origin-Realm}
{User-Name}
[3GPP-AAA-Server-Name]
[Supported-Features]
*[AVP]

```

4.3.4 Error notification to HSS

4.3.4.1 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR), indicated by the Command-Code field set to 301 and the “R” bit set in the message flags field, is sent by the 3GPP AAA Server to HSS to request the registration, de-registration, user profile download or update the HSS with the PGW identity.

Message Format:

```

<Server-Assignment-Request>::=<Diameter Header: 301, REQ,
    PXY,16777265>
    <Session-Id>
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    [Destination-Host]
    {Destination-Realm}
    {User-Name}
    {Server-Assignment-Type}
    *[AVP]

```

Server-Assignment-Type is AUTHENTICATION_FAILURE.

4.3.4.2 Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA), indicated by the Command-Code field set to 301 and the “R” set to zero in the Command Flags field of the header, is sent by HSS in response to Server-Assignment-Request (SAR) command.

Message Format:

```

<Server-Assignment-Answer>::=<Diameter Header:301, PXY,16777265>
    <Session-Id>
    {Vendor-Specific-Application-Id}

```



```
[Result-Code]
[Experimental Result]
{Auth-Session-State}
{Origin-Host}
{Origin-Realm}
{User-Name}
*[AVP]
```

4.4 Network Initiated De-Registration by HSS

4.4.1 Registration-Termination -Request (RTR) Command

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 HSS to a 3GPP AAA Server in order to request the de-registration of a user.

Message Format:

```
<Registration-Termination-Request> ::=
< Diameter Header:304, REQ, PXY, 16777265>
< Session-Id >
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    {Destination-Host}
    {Destination-Realm}
    {User-Name}
    {Deregistration-Reason}
    *[Supported-Features]
    *[Proxy-Info]
    *[Route-Record]
    *[AVP]
```

4.4.2 Registration-Termination -Answer (RTA) Command

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 the 3GPP AAA Server in response to the Registration-Termination-Request (RTR) command.

Message Format:

```
<Registration-Termination-Answer> ::=
<Diameter Header:304, PXY, 16777265>
< Session-Id >
    {Vendor-Specific-Application-Id}
    [Result-Code]
```



```
[Experimental-Result]
{Auth-Session-State}
{Origin-Host}
{Origin-Realm}
*[Supported-Features]
*[Proxy-Info]
*[AVP]
```

4.5 HSS Initiated Update of User Profile

4.5.1 Push-Profile-Request (PPR) Command

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.

Message Format:

```
<Push-Profile-Request> ::=
<Diameter Header:305, REQ,16777265 >
  <Session-Id>
    {Vendor-Specific-Application-Id}
    {Auth-Session-State}
    {Origin-Host}
    {Origin-Realm}
    {Destination-Host}
    {Destination-Realm}
    {User-Name}
    [Non-3GPP-User-Data]
    [PPR-Flags]
    *[Supported-Features]
    *[Proxy-Info]
    *[Route-Record]
    *[AVP]
```

4.5.2 Push-Profile-Answer (PPA) Command

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 3GPP AAA Server in response to the Push-Profile-Request command.

Message Format:

```
<Push-Profile-Answer> ::=
< Diameter Header:305, PXY, 16777265>
  <Session-Id>
    {Vendor-Specific-Application-Id}
```



```
[Result-Code]
[Experimental-Result]
{Auth-Session-State}
{Origin-Host}
{Origin-Realm}
[Access-Network-Info]
[Local-Time-Zone]
*[Supported-Features]
*[Proxy-Info]
*[AVP]
```




5 Diameter AVPs

5.1 IETF Protocol AVPs

Diameter Base Protocol (RFC3588) AVPs that are included in the SWx messages, are described in Reference [4].

Table 4 IETF Protocol AVPs

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not
MIP6-Home-Link-Prefix	125	OctetString	M	P		V
MIP-Home-Agent-Host	348	Grouped	M	P		V
Subscription-Id	443	Grouped	M	P		V
Subscription-Id-Data	444	UTF8String	M	P		V
Subscription-Id-Type	450	Enumerated	M	P		V
Service-Selection	493	UTF8String	M	P		V
Proxy-Info	284	Grouped	M			P,V
Route-Record	282	DiamIdent	M			V

5.1.1 MIP6-Home-Link-Prefix

The MIP6-Home-Link-Prefix AVP defined in RFC 5447 is of type OctetString and contains the Mobile IPv6 home network prefix information in a network byte order.

5.1.2 MIP-Home-Agent-Host

The MIP-Home-Agent-Host AVP is of type Grouped and is defined in RFC 4004. This AVP shall contain a FQDN of the PDN-GW which shall be used to resolve the PDN-GW IP address using the Domain Name Service function as defined in Reference [9], 3GPP TS 29.273.



The Data field of this AVP has the following ABNF grammar:

```
MIP-Home-Agent-Host ::= <AVP Header: 348>
                        {Destination-Realm}
                        {Destination-Host}
                        *[AVP]
```

5.1.3 Subscription-Id

The Subscription-Id AVP is of type Grouped and defined in RFC 4006. It contains the user identity to be used for charging purposes. This grouped AVP shall set the sub-AVP Subscription-Id-Type to value "END_USER_E164" and shall set the sub-AVP Subscription-Id-Data to the MSISDN value as indicated in 3GPP TS 29.273, Reference [9].

The Data field of this AVP has the following ABNF grammar:

```
Subscription-Id ::= <AVP Header: 443>
                  {Subscription-Id-Type}
                  {Subscription-Id-Data}
                  *[AVP]
```

5.1.4 Subscription-Id-Data

The Subscription-Id-Data AVP defined in RFC 4006 is of type UTF8String and contains the MSISDN of the user.

5.1.5 Subscription-Id-Type

The Subscription-Id-Type AVP defined in Reference [9] is of type Enumerated and contains information about the type of identifier carried by the Subscription-Id AVP. The following subscription identifier shall be used for SWx:

Table 5 Subscription-Id-Type AVP values

AVP value	Description
0	END_USER_E164

5.1.6 Service-Selection

The Service-Selection AVP is of type UTF8String defined in RFC 5778. This AVP shall contain either the APN Network Identifier, such as an APN without the Operator Network Identifier, or the wild card value as defined in 3GPP TS 29.272.



The contents of the Service-Selection AVP shall be formatted as a character string composed of one or more labels separated by dots (“.”) or as the wild card APN, i.e., consisting of only one ASCII label.

5.1.7 Proxy-Info

The Proxy-Info AVP is of type Grouped defined in RFC 6733. This AVP shall contain the identity and local state information of the Diameter node that creates and adds it to a message.

5.1.8 Route-Record

The Route-Record AVP is of type DiameterIdentity defined in RFC 6733. The identity added in this AVP must be the same as the one received in the Origin-Host of the Capabilities Exchange message.

5.2 3GPP AVPs

The following table describes the 3GPP AVPs defined in the STa application, their AVP Code values, types and possible AVP flag values. The 3GPP AVPs have Vendor-ID= 10415.

Table 6 3GPP AVPs

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not	Description
3GPP-Charging-Characteristics	13	UTF8String	V			M	See Section 5.2.1 on page 25
3GPP-AA-Server-Name	318	DiameterIdentity	M,V			M	See Section 5.2.2 on page 26
Max-Requested-Bandwidth-DL	515	Unsigned32	M,V				See Section 5.2.3 on page 26
Max-Requested-Bandwidth-UL	516	Unsigned32	M,V				See Section 5.2.4 on page 26
Visited-Network-Identifier	600	OctetString	V			M	See Section 5.2.5 on page 26
AAA-Failure-Indication	1518	Unsigned32	V			M, P	See Section 5.2.6 on page 27
SIP-Number-Auth-Items	607	Unsigned32	M, V				See Section 5.2.7 on page 27



Table 6 3GPP AVPs

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not	Description
SIP-Authentification-Scheme	608	UTF8String	M, V				See Section 5.2.8 on page 27
SIP-Authenticate	609	OctetString	M, V				See Section 5.2.9 on page 27
SIP-Authorization	610	OctetString	M, V				See Section 5.2.10 on page 27
SIP-Auth-Data-Item	612	Grouped	M, V				See Section 5.2.11 on page 28
SIP-Item-Number	613	Unsigned32	M, V				See Section 5.2.12 on page 28
Server-Assignment-Type	614	Enumerated	M, V				See Section 5.2.13 on page 29
Deregistration-Reason	615	Grouped	M, V				See Section 5.2.41 on page 36
Reason-Code	616	Enumerated	M, V				See Section 5.2.42 on page 36
Reason-Info	617	UTF8String	M, V				See Section 5.2.43 on page 36
Confidentiality-Key	625	OctetString	M, V				See Section 5.2.14 on page 29
Integrity-Key	626	OctetString	M, V				See Section 5.2.15 on page 29
Supported-Features	628	Grouped	V			M	See Section 5.2.37 on page 35
Feature-List-ID	629	Unsigned32	V			M	See Section 5.2.38 on page 35
Feature-List	630	Unsigned32	V			M	See Section 5.2.39 on page 35
Served-Party-IP-Address	848	Address	M, V				See Section 5.2.40 on page 36
QoS-Class-Identifier	1028	Enumerated	M, V				See Section 5.2.16 on page 29
RAT-Type	1032	Enumerated	M, V	P			See Section 5.2.17 on page 29
Allocation-Retention-Priority	1034	Grouped	V			M	See Section 5.2.18 on page 30
Priority-Level	1046	Unsigned32	V			M	See Section 5.2.19 on page 30
Terminal-Information	1401	Grouped	M, V				See Section 5.2.20 on page 30



Table 6 3GPP AVPs

Attribute Name	AVP Code	Value Type	Must	May	Should not	Must not	Description
IMEI	1402	UTF8String	M,V				See Section 5.2.21 on page 30
Software-Version	1403	UTF8String	M,V				See Section 5.2.22 on page 30
Context-Identifier	1423	Unsigned32	M,V				See Section 5.2.23 on page 31
APN-OI-Replacement	1427	UTF8String	M,V				See Section 5.2.24 on page 31
APN-Configuration	1430	Grouped	M,V				See Section 5.2.25 on page 31
EPS-Subscribed-QoS-Profile	1431	Grouped	M,V				See Section 5.2.26 on page 31
VPLMN-Dynamic-Address-Allowed	1432	Enumerated	M,V				See Section 5.2.27 on page 32
AMBR	1435	Grouped	M,V				See Section 5.2.28 on page 32
PDN-GW-Allocation-Type	1438	Enumerated	M,V				See Section 5.2.29 on page 32
PDN-Type	1456	Enumerated	M,V				See Section 5.2.29 on page 32
3GPP2-MEID	1471	OctetString	M,V				See Section 5.2.31 on page 33
Specific-APN-Info	1472	Grouped	M,V				See Section 5.2.32 on page 33
Non-3GPP-User-Data	1500	Grouped	V				See Section 5.2.33 on page 33
Non-3GPP-IP-Access	1501	Enumerated	V				See Section 5.2.34 on page 34
Non-3GPP-IP-Access-APN	1502	Enumerated	V				See Section 5.2.35 on page 34
ANID	1504	UTF8String	M,V				See Section 5.2.36 on page 35
PPR-Flags	1508	Unsigned32	V			M,P	See Section 5.2.44 on page 36
RAR-Flags	1522	Unsigned32	V			M,P	See Section 5.2.45 on page 37

5.2.1 3GPP-Charging-Characteristics

The 3GPP-Charging-Characteristics AVP is of type UTF8String. It contains the Charging Characteristics is defined in 3GPP TS 29.061.

The structure of the Charging Characteristics value according to 3GPP TS 32.299 is as follows:

Table 7 3GPP-Charging-Characteristics

8	7	6	5	4	3	2	1	
B4	B3	B2	B1	P3	P2	P1	P0	octet 1
B12	B11	B10	B9	B8	B7	B6	B5	octet 2

Bits P0-P3 refer to the Charging Characteristics Profile Index and B1-B12 may be used by the operator for non-standardised behavior.

Each octet of the Charging Characteristics value is represented via 2 UTF-8 encoded characters in the 3GPP-Charging-Characteristics AVP, defining its hexadecimal representation. For example, if P3 and P1 are set to 1, and all the B bits are set to 0, the value of octet 1 is 10, which hexadecimal representation is 0x0A, and in text form is "0A". Octet 2 is set to 0, represented as 0x00 in hexadecimal and "00" in text, so the 3GPP-Charging-Characteristics value in UTF-8 would be "0A00".

5.2.2 3GPP-AAA-Server-Name

The 3GPP-AAA-Server-Name AVP is of type DiameterIdentity defined in 3GPP TS 29.234, and defines the Diameter address of the 3GPP AAA Server node.

5.2.3 Max-Requested-Bandwidth-DL

The Max-Requested-Bandwidth-DL AVP is of type Unsigned32 defined in 3GPP TS 29.124 and it indicates the maximum requested bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, for instance: IP, UDP, RTP and RTP payload.

5.2.4 Max-Requested-Bandwidth-UL

The Max-Requested-Bandwidth-UL AVP is of type Unsigned32 defined in 3GPP TS 29.124, and it indicates the maximum requested bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, for instance: IP, UDP, RTP and RTP payload.

5.2.5 Visited-Network-Identifier

The Visited-Network-Identifier AVP defined in 3GPP TS 29.229 is of type OctetString. It contains an identifier of the visited network when it is received in MAR message. Otherwise it contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as defined in 3GPP TS 29.272:



mnc<MNC>.mmc<MCC>.3gppnetwork.org

5.2.6 AAA-Failure-Indication

The AAA-Failure-Indication AVP is of type Unsigned32 and it contains a bitmask.

Table 8 shows the meaning of the bits:

Table 8 AAA-Failure-Indication

Bit	Name	Description
0	AAA Failure	This bit, when set, indicates that a previously assigned 3GPP AAA Server is unavailable.

For bits not defined in Table 8, they must be cleared by the sender and discarded by the receiver.

5.2.7 SIP-Number-Auth-Items

The SIP-Number-Auth-Items AVP is of type Unsigned32. When used in a request, the SIP-Number-Auth-Items AVP indicates the number of authentication vectors the 3GPP AAA Server is requesting.

In the answer message, the SIP-Number-Auth-Items AVP indicates the actual number of SIP-Auth-Data-Item AVPs provided by the Diameter server.

5.2.8 SIP-Authentication-Scheme

The SIP-Authentication-Scheme AVP is of type UTF8String defined in 3GPP TS 29.229 and indicates the used authentication scheme. The following values are defined for this interface:

Table 9 SIP-Authentication-Scheme

AVP value	Description
EAP-AKA	EAP-AKA is to be used
EAP-AKA'	EAP-AKA' is to be used

5.2.9 SIP-Authenticate

The SIP-Authenticate AVP is of type OctetString defined in 3GPP TS 29.229 and contains, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN.



5.2.10 SIP-Authorization

The SIP-Authorization AVP is of type OctetString defined in 3GPP TS 29.229 and contains, binary encoded, the expected response XRES.

5.2.11 SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP is of type Grouped defined in 3GPP TS 29.229 and contains the authentication and/or authorization information for the Diameter Client. The optional AVPs that are needed in this interface are included in the ABNF representation below.

```
SIP-Auth-Data-Item ::= <AVP Header : 612, Vendor Id: 10415>
    [SIP-Item-Number]
    [SIP-Authentication-Scheme]
    [SIP-Authenticate]
    [SIP-Authorization]
    [Confidentiality-Key]
    [Integrity-Key]
    *[AVP]
```

For a normal authentication request, the SIP-Auth-Data-Item AVP is grouped with the next AVPs:

```
SIP-Auth-Data-Item ::= <AVP Header: 612, Vendor Id: 10415>
    {SIP-Authentication-Scheme}
    *[AVP]
```

For an authentication request after synchronization failure, the SIP-Auth-Data-Item AVP is grouped with the next AVPs:

```
SIP-Auth-Data-Item ::= <AVP Header: 612, Vendor Id: 10415>
    {SIP-Authentication-Scheme}
    {SIP-Authorization}
    *[AVP]
```

For authentication response, SIP-Auth-Data-Item AVP is grouped with the next AVPs:

```
SIP-Auth-Data-Item ::= <AVP Header : 612, Vendor Id: 10415>
    [SIP-Item-Number]
    {SIP-Authentication-Scheme}
    {SIP-Authenticate}
    {SIP-Authorization}
    {Confidentiality-Key}
    {Integrity-Key}
    *[AVP]
```




5.2.12 SIP-Item-Number

The SIP-Item-Number AVP is of type Unsigned32 defined in 3GPP TS 29.229, and is included in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVP. The order in which they are coded is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value are coded before SIP-Auth-Data-Item AVPs with a high SIP-Item-Number value.

5.2.13 Server-Assignment-Type

The Server-Assignment-Type AVP is of type Enumerated defined in 3GPP TS 29.229 and indicates the type of server update being performed in a Server-Assignment-Request operation. The following values are used in this interface:

Table 10 Server-Assignment-Type

AVP	Description
1	REGISTRATION
5	USER_DEREGISTRATION
8	ADMINISTRATIVE_DEREGISTRATION
9	AUTHENTICATION_FAILURE
12	AAA_USER_DATA_REQUEST
13	PGW_UPDATE

5.2.14 Confidentiality-Key

The Confidentiality-Key AVP is of type OctetString defined in 3GPP TS 29.229, and contains the Confidentiality Key (CK) or, after key derivation using the Access Network Identifier, the derived Confidentiality Key (CK').

5.2.15 Integrity-Key

The Integrity-Key AVP is of type OctetString defined in 3GPP TS 29.229, and contains the Integrity Key (IK) or, after key derivation using the Access Network Identifier, the derived Integrity Key (IK').

5.2.16 QoS-Class-Identifier

The QoS-Class-Identifier AVP is of type Enumerated defined in 3GPP TS 29.212, and it identifies a set of IP-CAN specific QoS parameters that define the authorized QoS, excluding the applicable bitrates for the IP-CAN bearer or service flow.

5.2.17 RAT-Type

The RAT-Type AVP is of type Enumerated defined in 3GPP TS 29.212 and is used to identify the radio access technology that is serving the UE.

5.2.18 Allocation-Retention-Priority

The Allocation-Retention-Priority AVP is of type Grouped defined in 3GPP TS 29.212. It indicates Priority of Allocation and Retention for the corresponding Access Point Name (APN) configuration within the Priority-Level AVP. The Data field of this AVP has the following ABNF grammar:

```
Allocation-Retention-Priority ::= <AVP Header: 1034, Vendor-Id: 10415>
                                {Priority-Level}
                                *[AVP]
```

5.2.19 Priority-Level

The Priority-Level AVP is of type Unsigned 32 defined in 3GPP TS 29.212. The priority level defines the relative importance of a resource request. The AVP is used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations.

The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request. Values 1 to 15 are defined, with value 1 as the highest level of priority.

5.2.20 Terminal-Information

The Terminal-Information AVP is of type Grouped defined in 3GPP TS 29.272. This AVP contains the information about the user's terminal.

The Data field of this AVP has the following ABNF grammar:

```
Terminal-Information ::= <AVP Header: 1401, Vendor-Id: 10415>
                        [IMEI]
                        [3GPP2-MEID]
                        [Software-Version]
                        *[AVP]
```

5.2.21 IMEI

The IMEI AVP is of type UTF8String defined in 3GPP TS 29.272. This AVP contains the International Mobile Equipment Identity.



5.2.22 Software-Version

The Software-Version AVP is of type UTF8String. This AVP defined in 3GPP TS 29.272, contains the Software Version of the International Mobile Equipment Identity.

5.2.23 Context-Identifier

The Context-Identifier AVP is of type Unsigned32 defined in 3GPP TS 29.272 and uniquely identifies an EPS APN configuration within a user subscription.

5.2.24 APN-OI-Replacement

The APN-OI-Replacement AVP is of type UTF8String defined in 3GPP TS 29.272. This AVP Indicates the domain name to replace the APN Operator Identifier (OI) when constructing the Packet Data Network (PDN) Gateway (GW) Fully Qualified Domain Name (FQDN) upon which to perform a Domain Name System (DNS) resolution. The contents of the APN-OI-Replacement AVP are formatted as a character string composed of one or more labels separated by dots (“.”).

5.2.25 APN-Configuration

The APN-Configuration AVP is of type Grouped defined in 3GPP TS 29.272. It contains the information related to APN configuration for a single APN.

The Data field of this AVP has the following ABNF grammar:

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

5.2.26 EPS-Subscribed-QoS-Profile

The EPS-Subscribed-QoS-Profile AVP is of type Grouped defined in 3GPP TS 29.272 and contains the bearer-level QoS parameters (QoS Class Identifier and



Allocation Retention Priority) associated to the default bearer for an APN. See Reference [9].

The Data field of this AVP has the following ABNF grammar:

```
EPS-Subscribed-QoS-Profile ::= <AVP Header: 1431, Vendor-Id: 10415>
                               {QoS-Class-Identifier}
                               {Allocation-Retention-Priority}
                               *[AVP]
```

5.2.27 VPLMN-Dynamic-Address-Allowed

The VPLMN-Dynamic-Address-Allowed AVP is of type Enumerated defined in 3GPP TS 29.272. It indicates whether the UE is allowed to use a dynamic address allocated in the Visited PLMN (VPLMN). The following values are defined:

Table 11 VPLMN-Dynamic-Address-Allowed AVP

AVP value	Description
0	NOT ALLOWED
1	ALLOWED

5.2.28 AMBR

The AMBR AVP is of type Grouped defined in 3GPP TS 29.212, and contains AVPs that indicate the aggregate maximum bitrates requested for the uplink and downlink bandwidth.

The Data field of this AVP has the following ABNF grammar:

```
AMBR ::= <AVP Header: 1435 , Vendor-Id:10415>
         {Max-Requested-Bandwidth-UL}
         {Max-Requested-Bandwidth-DL}
         *[AVP]
```

5.2.29 PDN-GW-Allocation-Type

The PDN-GW-Allocation-Type AVP is of type Enumerated defined in 3GPP TS 29.272 and indicates whether the PDN GW address is statically allocated or dynamically selected by other nodes.

The following values are defined:



Table 12 PDN-GW-Allocation-Type AVP

AVP value	Description
0	STATIC
1	DYNAMIC

5.2.30

PDN-Type

The PDN-Type AVP is of type Enumerated defined in 3GPP TS 29.272 and indicates the address type of PDN. The following values are defined:

Table 13 PDN-Type

AVP value	Description
0	IPv4: This value shall be used to indicate that the PDN can be accessed only in IPv4 mode.
1	IPv6: This value shall be used to indicate that the PDN can be accessed only in IPv6 mode.
2	IPv4v6: This value shall be used to indicate that the PDN can be accessed both in IPv4 mode, in IPv6 mode, and also from UEs supporting dualstack IPv4v6.
3	3 IPv4_OR_IPv6: This value shall be used to indicate that the PDN can be accessed either in IPv4 mode, or in IPv6 mode, but not from UEs supporting dualstack IPv4v6.

5.2.31

3GPP2-MEID

The 3GPP2-MEID AVP is of type OctetString defined in 3GPP TS 29.272. This AVP contains the Mobile Equipment Identifier of the user's terminal.

5.2.32

Specific-APN-Info

The Specific-APN-Info AVP is of type Grouped defined in 3GPP TS 29.272. It shall only be present in the APN configuration when the APN is a wild card APN. It shall contain 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 and optionally the PLMN Id of the PDN GW.

```
Specific-APN-Info ::= <AVP Header : 1472, Vendor Id: 10415>
    {Service-Selection}
    [MIP6-Agent-Info]
    [Visited-Network-Identifier]
    *[AVP]
```



5.2.33 Non-3GPP-User-Data

The Non-3GPP-User-Data AVP is of type Grouped defined in 3GPP TS 29.273, and contains the user profile information relevant for EPS. The Data field of the Non-3GPP-User-Data AVP has the following ABNF grammar:

```
Non-3GPP-User-Data ::= <AVP Header: 1500, Vendor-Id: 10415>
                        [Subscription-ID]
                        {Non-3GPP-IP-Access}
                        {Non-3GPP-IP-Access-APN}
                        [AMBR]
                        [3GPP-Charging-Characteristics]
                        {Context-Identifier}
                        [APN-OI-Replacement]
                        1*[APN-Configuration]
                        *[AVP]
```

At least one item of the APN-Configuration AVP shall always be included.

5.2.34 Non-3GPP-IP-Access

The Non-3GPP-IP-Access AVP is of type Enumerated, and allows the operator to determine barring of 3GPP <=> non-3GPP interworking as defined in 3GPP TS 29.273. The following values are defined:

Table 14 Non-3GPP-IP-Access AVP

AVP value	Description
0	NON_3GPP_SUBSCRIPTION_ALLOWED: The subscriber has non-3GPP subscription to access EPC network.
1	NON_3GPP_SUBSCRIPTION_BARRIED: The subscriber has no non-3GPP subscription to access EPC network.

5.2.35 Non-3GPP-IP-Access-APN

The Non-3GPP-IP-Access-APN AVP is of type Enumerated, and allows the operator to disable all APNs for a subscriber at one time as defined in 3GPP TS 29.273. The following values are defined:



Table 15 Non-3GPP-IP-Access-APN AVP

AVP value	Description
0	NON_3GPP_APNS_ENABLE: Enable all APNs for a subscriber.
1	NON_3GPP_APNS_DISABLE: Disable all APNs for a Subscriber.

5.2.36 ANID

The ANID AVP is of type UTF8String defined in 3GPP TS 29.212 and contains the Access Network Identity. It is used for key derivation function when the authentication method is EAP-AKA'. See Reference [10] for possible values.

5.2.37 Supported-Features

The Supported-Features AVP is of type Grouped and it is defined in 3GPP TS 29.229. If this AVP is present it may inform the destination host about the features that the origin host supports.

The Feature-List AVP contains a list of supported features of the origin host. The Vendor-Id AVP and the Feature-List AVP together identify which feature list is carried in the Supported-Features AVP. Where a Supported-Features AVP is used to identify features that have been defined by 3GPP, the Vendor-Id AVP contains the vendor ID of 3GPP.

Vendors may define proprietary features, but it is strongly recommended that the possibility is used only as the last resort. Where the Supported-Features AVP is used to identify features that have been defined by a vendor other than 3GPP, it contains the vendor ID of the specific vendor in question. If there are multiple feature lists defined by the same vendor, the Feature-List-ID AVP differentiates those lists from one another.

The destination host uses the value of the Feature-List-ID AVP to identify the feature list. Its Data field has the following ABNF grammar:

```
Supported-Features ::= <AVP Header: 628, Vendor-Id: 10415>
                        {Vendor-Id}
                        {Feature-List-ID}
                        {Feature-List}
                        *[AVP]
```

5.2.38 Feature-List-ID

The Feature-List-ID AVP is of type Unsigned32 defined in 3GPP TS 29.229 and it contains the identity of a feature list.



5.2.39 Feature-List

The Feature-List AVP is of type Unsigned32 defined in 3GPP TS 29.229 and it contains a bit mask indicating the supported features of an application. When the bit set, indicates the corresponding feature is supported by the application.

5.2.40 Served-Party-IP-Address

The Served-Party-IP-Address AVP is of type Address defined in 3GPP TS 32.299. It contains the IPv4 address, the IPv6 address or the IPv6 prefix of the user, if static IP address allocation is used. For the IPv6 prefix, the lower 64 bits of the address shall be set to zero.

5.2.41 Deregistration-Reason

The Deregistration-Reason AVP is of type Grouped, and indicates the reason for a de-registration operation.

AVP format:

```
Deregistration-Reason :: = < AVP Header : 615 10415 >
{ Reason-Code }
[ Reason-Info ]
* [AVP]
```

5.2.42 Reason-Code

The Reason-Code AVP is of type Enumerated, and defines the reason for the network initiated de-registration. The following values are defined:

```
PERMANENT_TERMINATION (0)
NEW_SERVER_ASSIGNED (1)
SERVER_CHANGE (2)
REMOVE_S-CSCF (3)
```

5.2.43 Reason-Info

The Reason-Info AVP is of type UTF8String, and contains textual information to inform the user of the reason for a de-registration.

5.2.44 PPR-Flags

The PPR-Flags AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined as follow:

Note: Bits not defined in this table must be cleared by the sender and discarded by the command receiver.



Bit	Name	Description
0	Reset-Indication	This bit, when set, indicates that the HSS has undergone a restart event and registration data and dynamic data needs to be restored, if available at the Server.
1	Access-Network-Info-Request	This bit, when set, indicates that the HSS requests the 3GPP AAA Server the location information of the access network where the UE is currently attached.
2	UE-Local-Time-Zone-Request	This bit, when set, indicates that the HSS requests the 3GPP AAA Server the location in the access network where the UE is attached.
3	P-CSCF Restoration Request	This bit, when set, indicates to the 3GPP AAA Server that the HSS requests the execution of the HSS-based P-CSCF restoration procedures for WLAN, as described in 3GPP TS 23.380 [52] subclause 5.6.

5.2.45

RAR-Flags

The RAR-Flags AVP is of type Unsigned32 and it contains a bit mask. The meaning of the bits is defined as follows:

Note: Bits not defined in this table must be cleared by the sender and discarded by the command receiver.

Bit	Name	Description
0	Trust-Relationship-Update-indication	This bit, when set, indicates to the PDN GW that the 3GPP AAA server only re-authentication procedure send the trust relationship to the PDN GW, and the PDN GW shall not perform any authorization procedure towards the UE.
1	P-CSCF Restoration Request	This bit, when set, shall indicate to the PDN GW that the 3GPP AAA Server requests the execution of the HSS-based P-CSCF restoration procedures for WLAN, as described in 3GPP TS 23.380 [52] subclause 5.6.





6 Formal Syntax

This interface uses following syntax:

- Diameter Base Protocol RFC 3588, Reference [4], is used to describe messages and AVPs.





7 Related Standards

- 3GPP EPS AAA interfaces 3GPP TS 29.273 version 12.5.0
- Diameter Base Protocol RFC 3588
- Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA) RFC 4187
- Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA') RFC 5448
- Extensible Authentication Protocol (EAP) RFC 3748
- Diameter Extensible Authentication Protocol (EAP) Application RFC 4072
- Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for non-3GPP accesses (3GPP TS 23.402 version 9.6.0 Release 9)





Reference List

IPWorks Library Documents

- [1] Glossary of Terms and Acronyms
- [2] Trademark Information
- [3] Typographic Conventions

Standards

- [4] [Diameter Base Protocol RFC 3588](#)
- [5] [Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA\) RFC 4187](#)
- [6] [Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement \(EAP-AKA'\) RFC 5448](#)
- [7] [Extensible Authentication Protocol \(EAP\) RFC 3748](#)
- [8] [Diameter Extensible Authentication Protocol \(EAP\) Application RFC 4072](#)
- [9] [Universal Mobile Telecommunications System \(UMTS\); LTE3GPP EPS AAA interfaces; Evolved Packet System \(EPS\); \(3GPP TS 29.273 version 12.5.0 Release 12\)](#)
- [10] [Universal Mobile Telecommunications System \(UMTS\); LTE; Architecture enhancements for non-3GPP accesses\(3GPP TS 23.402 version 9.6.0 Release 9\)](#)