

CSCF Cx and Dx Interface

Call Session Control Function

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2013–2018. 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 Trademark Information.



Contents

1	Introduction	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	5
3	Procedures	7
3.1	Lower-Level Procedures	7
3.2	User Registration Status Query	10
3.3	User Location Query	13
3.4	Server-Assignment-Request	18
3.5	Authentication Request	35
3.6	Network Initiated Deregistration	46
3.7	HSS Initiated User Profile Update	52
4	Information Model	57
4.1	Supported Diameter Cx/Dx Commands	58
5	Formal Syntax	99
5.1	Diameter Base AVPs	99
5.2	3GPP Cx/Dx Diameter Applications AVPs	109
5.3	ETSI Diameter Applications AVPs	133
5.4	Ericsson Diameter Applications AVPs	134
5.5	User Profile	136
6	Security Considerations	153
7	Related Standards	155





1 Introduction

This document describes the interface between the Call Session Control Function (CSCF) and the Home Subscriber Server/Subscriber Location Function (HSS/SLF) using the reference point Cx/Dx interface as described in the [3GPP TS 29.229 Cx and Dx interfaces based on the Diameter Protocol](#) specification.





2 Interface Overview

The interface between the CSCF and the HSS/SLF is shown in Figure 1.

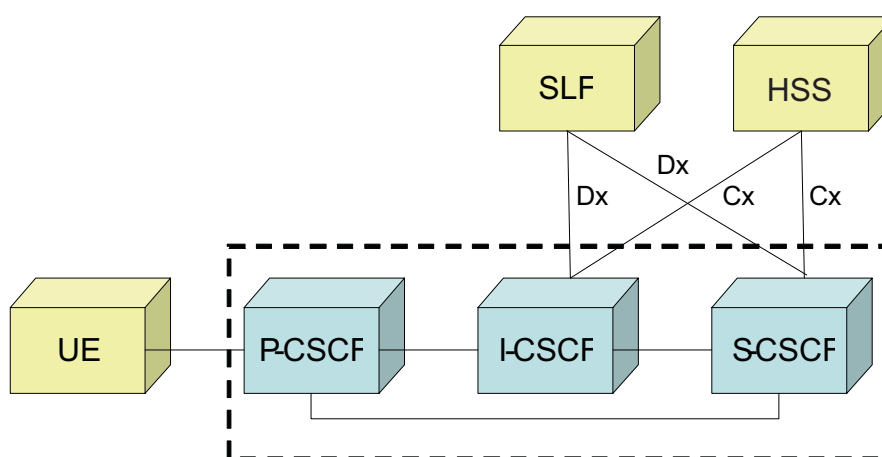


Figure 1 Interface Entities

Note: The dotted line illustrates the system boundaries.

The Cx/Dx interface is the reference point between the CSCF, meaning the Interrogating CSCF (I-CSCF) and the Serving CSCF (S-CSCF), and the HSS/SLF in the IMS multimedia network.

2.1 Interface Role

All services between the CSCF and the HSS/SLF are described from a CSCF point of view.

2.2 Services

The services offered by the CSCF are shown in Table 1.

Table 1 Offered 3GPP Cx Services

Offered Service	Description
Network Initiated Deregistration	Deregistration of the User initiated from the HSS.
User Profile Update	Update of the User Profile initiated from the HSS.

The user services offered by the 3GPP® Cx/Dx are shown in Table 2.



Table 2 Used 3GPP Cx/DxServices

Used Service	Description
User Registration Status Query	Used to authorize the registration of the Public Id and to obtain either S-CSCF name or server capabilities that the S-CSCF has to support.
User Location Query	Used to obtain the S-CSCF assigned to a Public Id, or the name of the Application Server (AS) hosting a Public Service Identity (PSI) for direct routing.
S-CSCF Registration/De registration Notification and User Profile download Restoration Information upload/download P-CSCF Restoration Procedure	Used to assign the S-CSCF to a Public Identity or clear the S-CSCF assigned to one or more Public Identities or to download the User Profile. Used to upload/download the Restoration Information of a user in HSS. Used to request the triggering of the P-CSCF Restoration Procedure at the HSS for a user whose registering P-CSCF is not functioning.
Authentication Request	Used to exchange information to support the authentication between the user and the home IMS network.

The user services offered by the Ericsson proprietary services Cx/Dx are shown in Table 3.

Table 3 Used Ericsson Proprietary Services

Used Service	Description
Subscription Id Info	Used for relaying subscription identity data in Charging output to Charging systems.
Roaming Awareness	Used for relaying roaming status in Charging output to Charging systems. The information is also included at message sending to Application Servers. Both fixed broadband and wireless network types of accesses are supported.
Max Number of Session Restrictions	Used to restrict the subscriber to a limited number of simultaneous sessions.
Activity Information	Used to measure the use of an IMS service by how many users have started a specific service in a time interval. The measurement is per service and globally for all services.



Used Service	Description
Authentication Request	Used to exchange information to support the authentication between the user and the home IMS network.
Max Number of Contacts	Used to restrict the subscriber to a limited number of registered contacts per Implicit Registration Set (IRS).

2.3 Encapsulation and Addressing

The CSCF Cx/Dx application protocol is used on top of the Diameter Base Protocol, as described in the [RFC 3588 Diameter Base Protocol](#) specification.

The CSCF supports Diameter over SCTP and TCP.

The Attribute-Value Pair (AVP) Length indicates the number of octets in this AVP including the AVP Code, AVP Length, AVP Flags, Vendor-ID field, if present, and the AVP data.

The DiameterIdentity format is derived from the OctetString AVP Base Format, as follows:

— DiameterIdentity = FQDN

The DiameterURI must follow the Uniform Resource Identifiers (URI) syntax, as follows:

— "aaa://" FQDN [port] [transport] [protocol]





3 Procedures

The 3GPP Diameter procedures are shown in Table 4.

Table 4 3GPP Diameter Procedures

3GPP Procedure	Command-Name	Abbreviation
User Registration Status Query	User-Authorization-Request	UAR
	User-Authorization-Answer	UAA
User Location Query	Location-Info-Request	LIR
	Location-Info-Answer	LIA
S-CSCF registration/deregistration notification and User Profile Download	Server-Assignment-Request	SAR
	Server-Assignment-Answer	SAA
Authentication Request	Multimedia-Auth-Request	MAR
	Multimedia-Auth-Answer	MAA
Network Initiated Deregistration	Registration-Termination-Request	RTR
	Registration-Termination-Answer	RTA
User Profile Update	Push-Profile-Request	PPR
	Push-Profile-Answer	PPA

3.1 Lower-Level Procedures

3.1.1 HSS Selection

There can be one or several HSS nodes in the network where the following apply:

- Where there is only one HSS in the network, the CSCF uses a “static” HSS configuration parameter `CscfCXDestinationHost`.
- In a network with several HSS nodes, the parameter is set to **NotConfigured** and the Subscriber Location Function (SLF) node is used to find out which HSS that keeps data for a specific subscriber.

In the SLF case, the CSCF sends the Diameter message on the Dx interface where the `Destination-Host` AVP is not present. The response from the SLF contains a redirection host in the `Redirect-Host` AVP and the `Result-Code` is set to **DIAMETER_REDIRECT_INDICATION**. The CSCF forwards the same request on the Cx interface, now including the `Destination-Host` AVP received in the `Redirect-Host` AVP from the SLF.

3.1.1.1 Successful HSS Selection

A successful HSS selection procedure is shown in Figure 2.

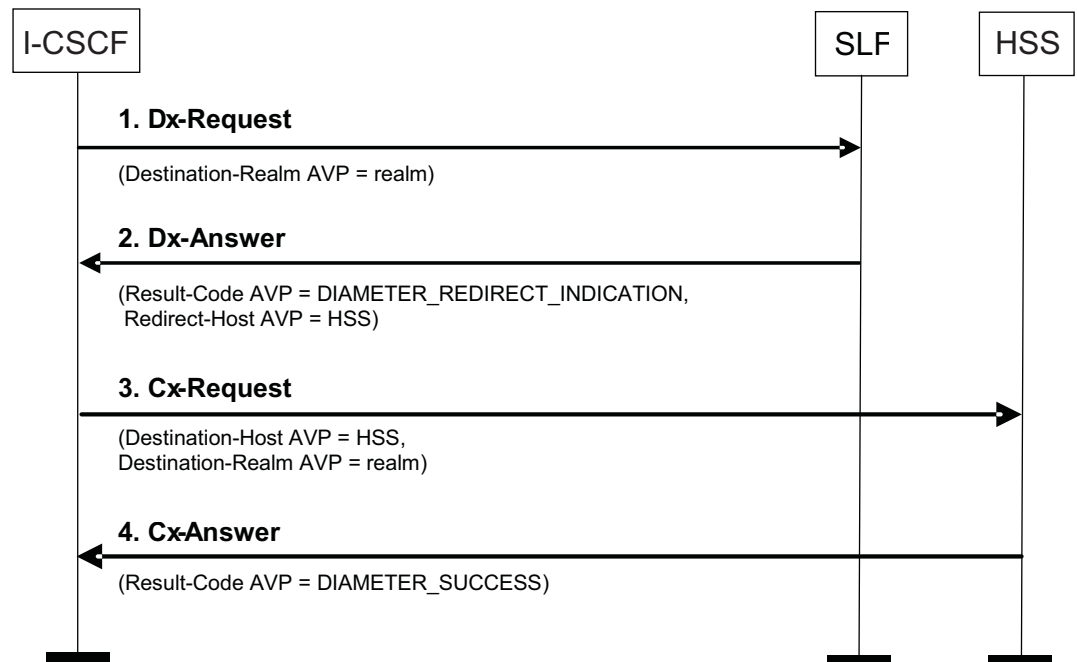


Figure 2 Successful HSS Selection

The procedure is as follows:

- 1 The `CscfCxDestinationHost` is set to **NotConfigured**, so the CSCF sends the Request over the Dx interface to the SLF.
- 2 The SLF finds the HSS and inserts the `Redirect-Host` AVP and `Result-Code` `DIAMETER_REDIRECT_INDICATION` in the response to the CSCF.
- 3 The CSCF inserts the received redirect host into the `Destination-Host` AVP and forwards the message over the Cx interface to the HSS.
- 4 The HSS responds with `Result-Code` `DIAMETER_SUCCESS`.

3.1.1.2

Unsuccessful HSS Selection – User Not Found

An unsuccessful HSS selection procedure, where the user is not found, is shown in Figure 3.

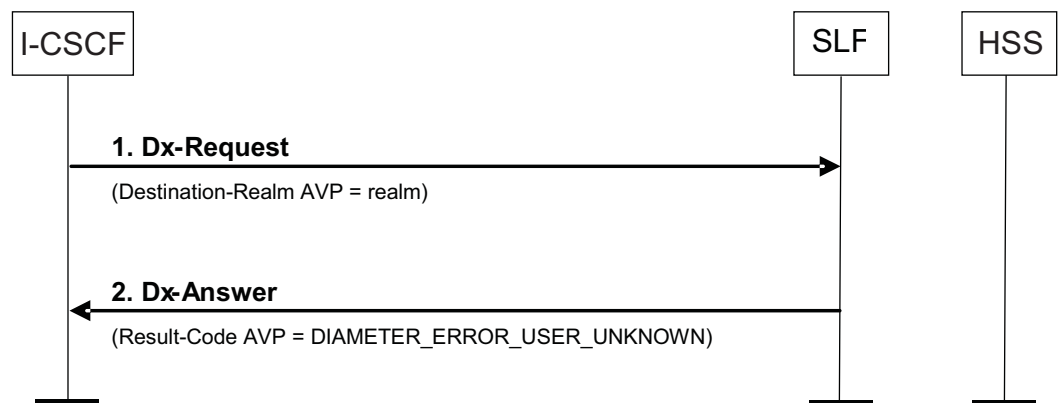


Figure 3 Unsuccessful HSS Selection – User Not Found

The procedure is as follows:

- 1 The CscfCxDestinationHost is set to **NotConfigured**, so the CSCF sends the Request over the Dx interface to the SLF.
- 2 The SLF does not find the user and responds with Result-Code DIAMETER_ERROR_USER_UNKNOWN.

3.1.1.3

Unsuccessful HSS Selection – Time-Out to SLF

An unsuccessful HSS selection process, where there is a time-out to the SLF, is shown in Figure 4.

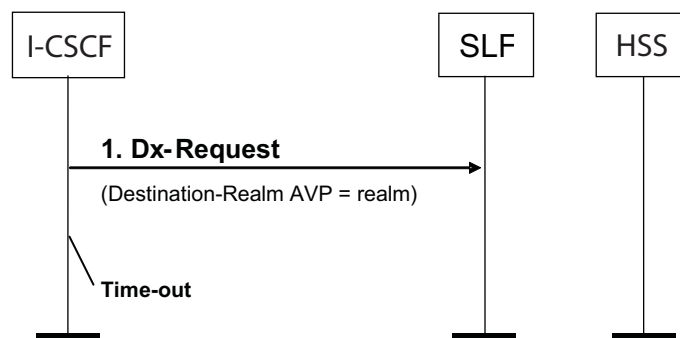


Figure 4 Unsuccessful HSS Selection – Time-Out to SLF

The procedure is as follows:

- 1 The CscfCxDestinationHost is set to **NotConfigured**, so the CSCF sends the Request over the Dx interface to the SLF.
- 2 At time-out to the SLF, the CSCF rejects the SIP request.

3.2 User Registration Status Query

The following procedure is used by the I-CSCF to the HSS during SIP registration:

- Authorize the registration of the Public User Identity, checking access permissions and roaming agreements.
- Perform a first security check, determining whether the Public User Identity in the message is associated with the Private User Identity sent in the message.
- Obtain either the S-CSCF where the Public User Identity is registered or unregistered, or if not registered the list of capabilities that the S-CSCF has to support.

The list of capabilities can be empty allowing the I-CSCF to select any available S-CSCF.

The I-CSCF requests the authorization of the registration of the user by the User-Authorization-Request (UAR) command.

The CSCF provides the Public and Private User Identities and the visited network identity to the HSS.

The HSS uses registration information provided by the I-CSCF to authorize the user, based on internal information and on roaming agreements with the visited network.

If the user is registered or unregistered, the HSS returns a stored S-CSCF name.

If the user is not registered, the HSS can return S-CSCF capabilities (mandatory and optional S-CSCF capabilities, or both) that are used for the selection of an S-CSCF by the I-CSCF. The S-CSCF capabilities can also include a list of preconfigured S-CSCF names to be used for the initial registration. If no S-CSCF capabilities are returned, it is up to the I-CSCF to select a suitable S-CSCF.

3.2.1 Use Cases – User Registration

3.2.1.1 Successful UAR – Initial Registration

A successful UAR with initial registration is shown in Figure 5.

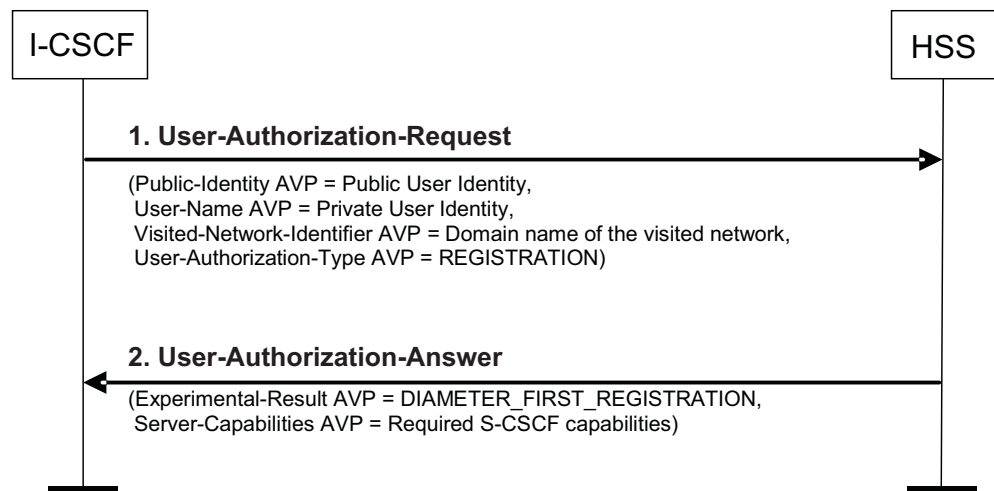


Figure 5 Successful UAR – Initial Registration

The procedure is as follows:

- 1 The I-CSCF sends a UAR to the HSS. The I-CSCF extracts the Public User Identity, the Private User Identity, and the visited network domain name from the received SIP message and includes them in the command.
- 2 The HSS responds with an indication that this is a first registration and can include server capabilities in the response. The server capabilities can include mandatory S-CSCF capabilities, optional S-CSCF capabilities, or a list of preconfigured S-CSCF names.

3.2.1.2

Successful UAR – Subsequent Registration

A successful UAR with subsequent registration is shown in Figure 6.

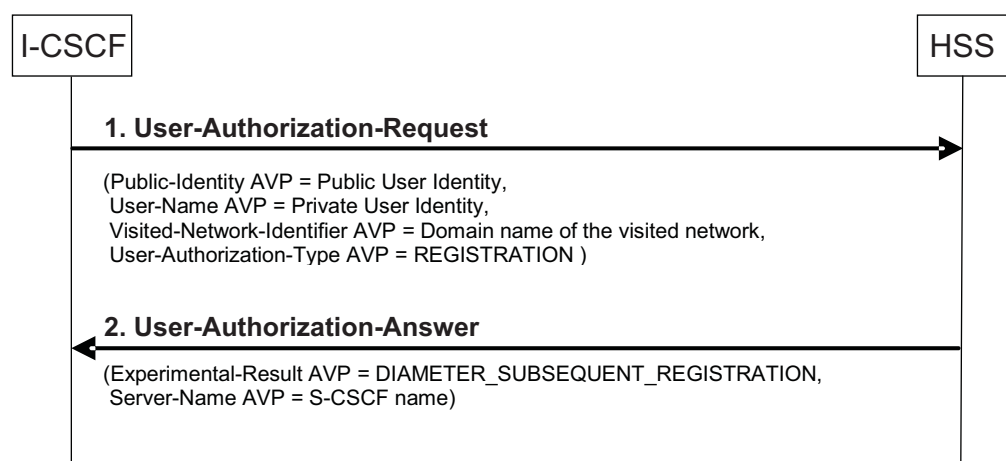


Figure 6 Successful UAR – Subsequent Registration

The procedure is as follows:

- 1 The I-CSCF sends a UAR to the HSS. The I-CSCF extracts the Public User Identity, the Private User Identity, and the visited network domain name from the received SIP message and includes them in the command.
- 2 The HSS responds with an indication that this is a subsequent registration and includes the assigned S-CSCF name in the response.

3.2.1.3 Successful UAR – Deregistration

A successful UAR with deregistration is shown in Figure 7.

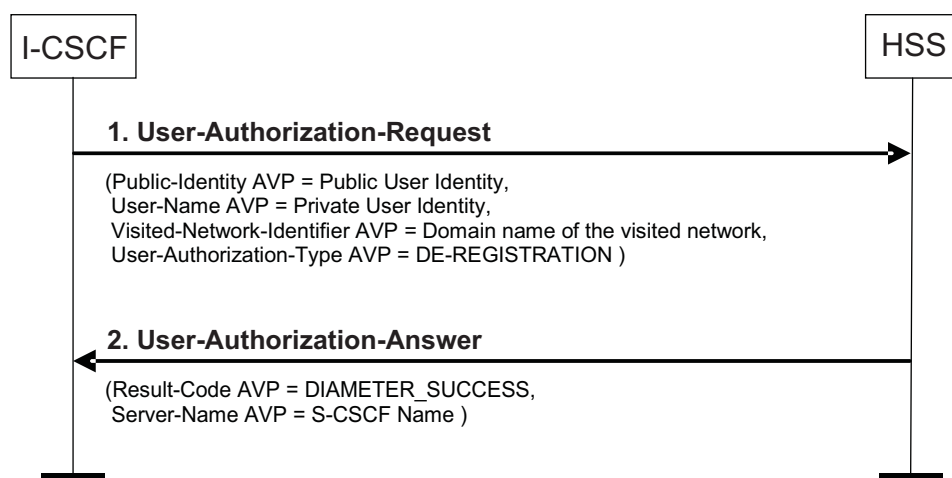


Figure 7 Successful UAR – Deregistration

The procedure is as follows:

- 1 The I-CSCF sends a UAR to the HSS indicating that the user is deregistering. The I-CSCF extracts the Public User Identity, the Private User Identity, and the visited network domain name from the received SIP message and includes them in the command.
- 2 The HSS responds with an indication that the request was successful and includes the assigned S-CSCF name in the response.

3.2.1.4 Request for Capabilities in Case of Reselection of S-CSCF

A request for capabilities, in case of reselection of an S-CSCF, is shown in Figure 8.

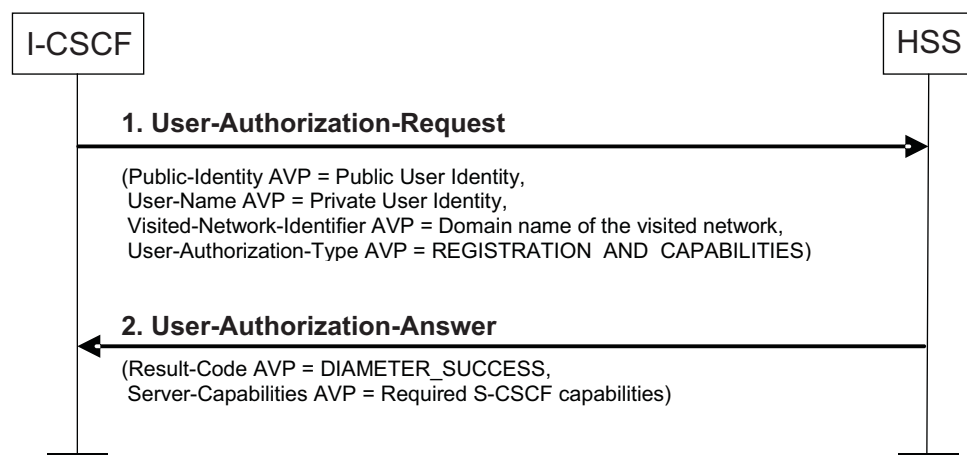


Figure 8 Request for Capabilities in Case of Reselection of S-CSCF

The procedure is as follows:

- 1 The I-CSCF needs to reselect in case an assigned S-CSCF for a subsequent registration or deregistration is not responding. The I-CSCF requests the HSS for server capabilities used for selection of a new S-CSCF.

The I-CSCF sends a UAR to the HSS indicating that the I-CSCF requires the server capabilities assigned to the user.

The I-CSCF extracts the Public User Identity, the Private User Identity, and the visited network domain name from the received SIP message and includes them in the command.

- 2 The HSS can include server capabilities in the response. The server capabilities can include mandatory S-CSCF capabilities, optional S-CSCF capabilities, and a list of preconfigured S-CSCF names, or a combination of this.

If no server capabilities are returned, it is up to the I-CSCF to select a suitable S-CSCF.

3.3 User Location Query

This procedure is used by the I-CSCF to the HSS to obtain the following:

- The name of the S-CSCF assigned to a Public Identity
- The server capabilities to help the I-CSCF in the selection of the S-CSCF
- The name of the AS hosting a PSI for direct routing

The I-CSCF requests S-CSCF location information by the Location Information Request (LIR) command.

The I-CSCF provides the Public User Identity to the HSS. The Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN is returned if the

user is unknown, otherwise depending on the state of the user, the following answers can be provided:

- 1 If the user is registered, then the stored S-CSCF name is returned, the Server-Name AVP contains the SIP URI of the server, or the Server-Capabilities AVP is returned, if User-Authorization-Type (UAT) is set to **REGISTRATION_AND_CAPABILITIES** in the LIR message. The Server-Capabilities AVP enables the I-CSCF to select an S-CSCF. The Result-Code AVP set to **DIAMETER_SUCCESS** is returned.
- 2 If the user is unregistered, then the stored S-CSCF name is returned, the Server-Name AVP contains the SIP URI of the server, or the Server-Capabilities AVP is returned, if UAT is set to **REGISTRATION_AND_CAPABILITIES** in the LIR message. The Server-Capabilities AVP enables the I-CSCF to select an S-CSCF. The Result-Code AVP set to **DIAMETER_SUCCESS** is returned.
- 3 If the user is not registered and it has services related to unregistered services, or the request contains an Originating-Request AVP, then the HSS can return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF.

If Server-Capabilities AVP is not present, it is up to the I-CSCF to select any S-CSCF suitable for the IMS Subscription. The Experimental-Result-Code **DIAMETER_UNREGISTERED_SERVICE** is returned.

- 4 If the user is not registered and the Public Identity has no services related to the unregistered state and the request does not contain the Originating-Request AVP, then the Experimental-Result-Code set to **DIAMETER_ERROR_IDENTITY_NOT_REGISTERED** is returned.
- 5 If the user is a wildcarded Public User, then the wildcarded public identity is returned in the Wildcarded-Public-Identity AVP.

The I-CSCF supports the 3GPP Standardized Restoration Procedure; it always indicates the support of the feature by setting the IMSRestorationInd bit in the Supported-Features AVP of the LIR command. If the I-CSCF sends an LIR with UAT equals to **REGISTRATION_AND_CAPABILITIES** and sets the IMSRestorationInd bit of the Supported-Features AVP, the HSS allows the S-CSCF name of the user to be updated in the next Server-Assignment-Request (SAR) message.

3.3.1 Use Cases – User Location

3.3.1.1 Successful User Location Query – Public Identity Registered or Unregistered

A successful user location query with public identity that is registered or unregistered is shown in Figure 9.

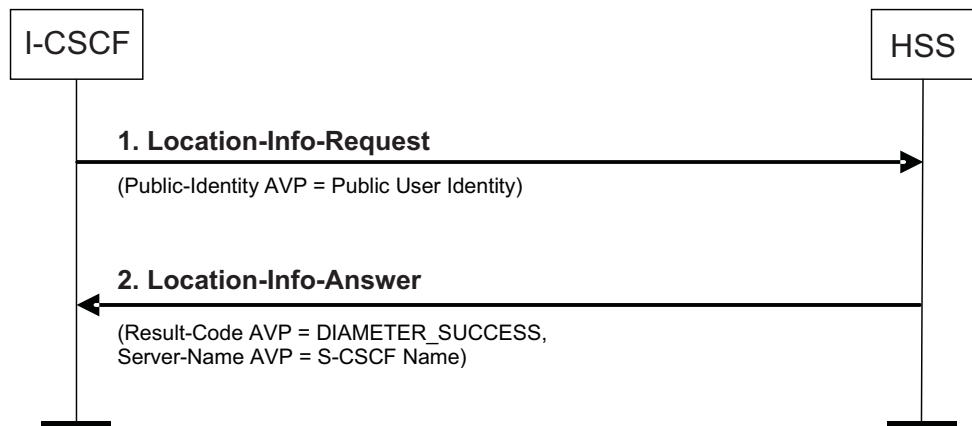


Figure 9 Successful User Location Query – Public Identity Registered or Unregistered

The procedure is as follows:

- 1 The I-CSCF sends an LIR to the HSS. The I-CSCF extracts the Public User Identity from the received SIP message and includes it in the command.
- 2 The Public Identity is registered or unregistered and has an S-CSCF assigned, so the HSS responds with Result-Code DIAMETER_SUCCESS and includes the stored S-CSCF Name in the response.

Note: If the HSS matches the IP Multimedia Public Identity (IMPU) to a wildcarded public identity, the Location Information Answer (LIA) message includes a Wildcarded-Public-Identity AVP.

3.3.1.2

Successful User Location Query – Public Identity Registered or Unregistered, Server Capabilities Are Requested

A successful user location query with public identity that is registered or unregistered, and where server capabilities are requested, is shown in Figure 10.

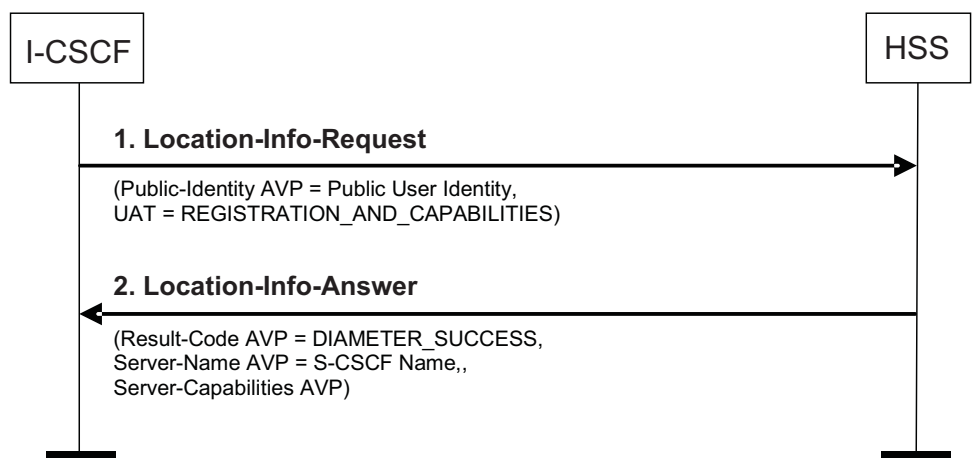


Figure 10 Successful User Location Query – Public Identity Registered or Unregistered, Server Capabilities Are Requested

The procedure is as follows:

- 1 The I-CSCF sends an LIR to the HSS. The I-CSCF extracts the Public User Identity from the received SIP message and includes it in the command. The I-CSCF is requesting the HSS for the server capabilities only by including the UAT AVP with value set to REGISTRATION_AND_CAPABILITIES.
- 2 The Public Identity is registered or unregistered; the HSS responds with Result-Code DIAMETER_SUCCESS and includes the Server-Capabilities AVP in the response.

Note: If the HSS matches the IMPU to a wildcarded public identity, the LIA message includes a Wildcarded-Public-Identity AVP.

3.3.1.3

Successful User Location Query – Public Identity Not Registered but Has Unregistered Services

A successful user location query with public identity that is not registered but has unregistered services is shown in Figure 11.

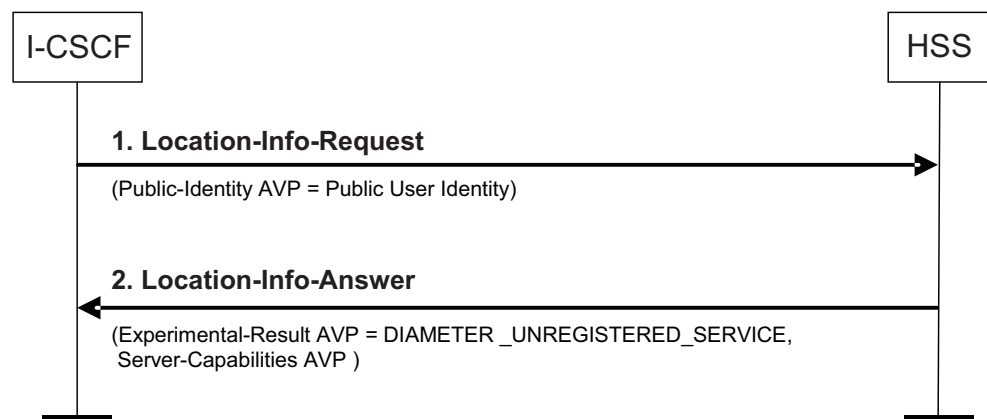


Figure 11 Successful User Location Query – Public Identity Not Registered but Has Unregistered Services

The procedure is as follows:

- 1 The I-CSCF sends an LIR to the HSS. The I-CSCF extracts the Public User Identity from the received SIP message and includes it in the command.
- 2 The HSS responds with the Experimental-Result-Code DIAMETER_UNREGISTERED_SERVICE and can include the S-CSCF server capabilities in the response.

Note: If the HSS matches the IMPU to a wildcarded public identity, the LIA message includes a Wildcarded-Public-Identity AVP.



3.3.1.4

Unsuccessful User Location Query – Public Identity Not Registered and Has No Unregistered Services

An unsuccessful user location query with public identity that is not registered and has no unregistered services is shown in Figure 12 .

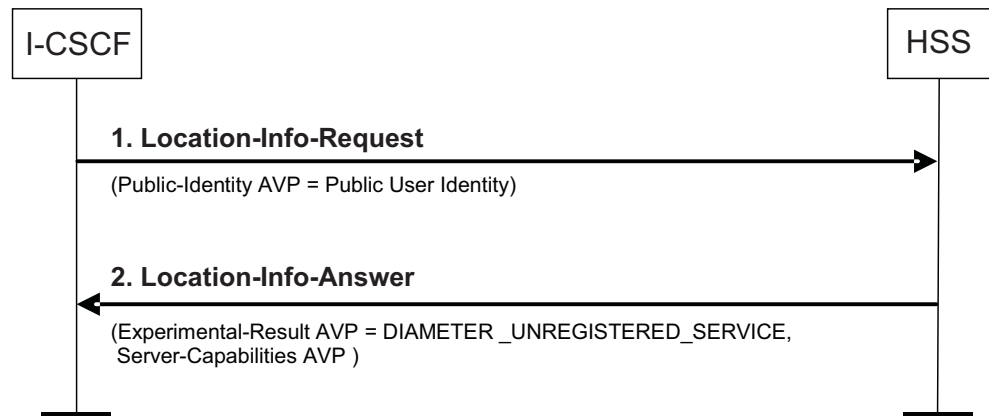


Figure 12 Unsuccessful User Location Query – Public Identity Not Registered and Has No Unregistered Services

The procedure is as follows:

- 1 The I-CSCF sends an LIR to the HSS. The I-CSCF extracts the Public User Identity from the received SIP message and includes it in the command.
- 2 The HSS responds with Experimental-Result-Code DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

3.3.1.5

Successful User Location Query – Originating Request

A successful user location query with originating request is shown in Figure 13.

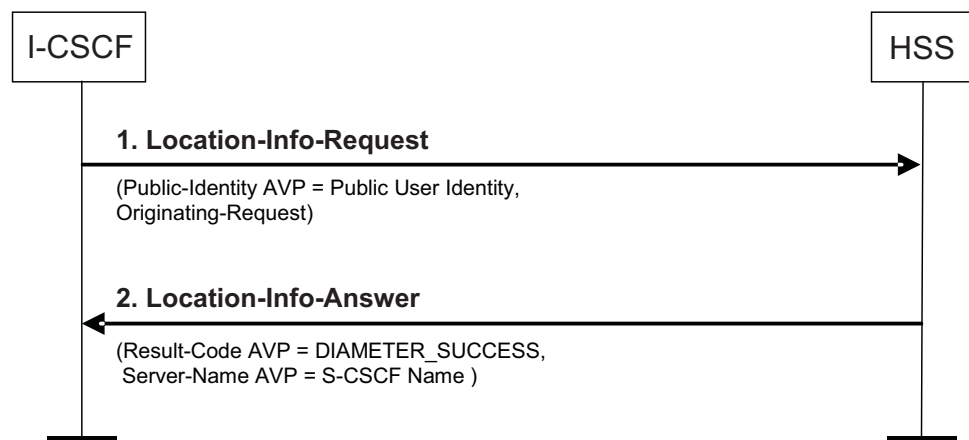


Figure 13 Successful User Location Query – Originating Request

The procedure is as follows:

- 1 The I-CSCF sends an LIR to the HSS. The I-CSCF extracts the Public User Identity from the received SIP message and includes it and the Originating-Request AVP in the command.
- 2 The Public Identity is registered and has an S-CSCF assigned, so the HSS responds with Result-Code DIAMETER_SUCCESS and includes the stored S-CSCF Name in the response.

Note: If the HSS matches the IMPU to a wildcarded public identity, the LIA message includes a Wildcarded-Public-Identity AVP.

3.3.1.6

Unsuccessful User Location Query – Originating Request

An unsuccessful user location query with originating request is shown in Figure 14.

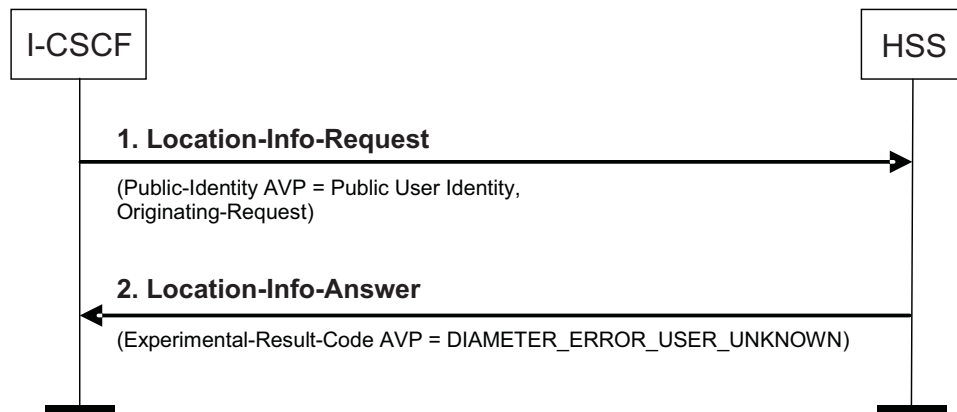


Figure 14 Unsuccessful User Location Query – Originating Request

The procedure is as follows:

- 1 The I-CSCF sends an LIR to the HSS. The I-CSCF extracts the Public User Identity from the received SIP message and includes it and the Originating-Request AVP in the command.
- 2 The Public Identity is unknown in the HSS, which responds with Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN.

3.4

Server-Assignment-Request

This procedure is used by the S-CSCF to the HSS to perform the following:

- Assign an S-CSCF to a Public Identity or clear the name of the S-CSCF assigned to one or several Public Identities.
- Download the user profile and the Charging information from the HSS.
- Store and retrieve restoration information with or without subscription information of a user if the restoration procedure is supported and enabled in the S-CSCF and the HSS.



- Trigger the P-CSCF restoration procedure for a user whose registered P-CSCF is not functioning.

The S-CSCF requests the Registration/Deregistration Notification, User profile download, restoration information upload and download, and triggering of P-CSCF restoration procedure by the SAR command.

In an Initial Registration, the S-CSCF updates the specified user in the HSS with the S-CSCF name and the restoration information, and requests the user data and Charging information from the HSS by sending the SAR. The main data is the S-CSCF server name, the username, the Public User Identity, and an indication that the update concerns setting the S-CSCF name, `Server-Assignment-Type = REGISTRATION`. In addition, if the restoration procedure is enabled in the S-CSCF, the S-CSCF includes the restoration information, `Multiple-Registration-Indication AVP`, and `Supported-Feature AVP` with `IMSRestorationInd` bit set in the SAR message.

When a `Server-Assignment-Answer (SAA)` is received, the S-CSCF checks that the operation is successful, as follows:

- If it is successful, the S-CSCF stores the Private User Identity and the Public User Identity. In case the requested Public User Identity belongs to an Implicit Registration Set, several Public User Identities are received. The CSCF stores user data and Charging information for each IMPU. If restoration procedure is enabled in both S-CSCF and HSS, HSS can for `Server-Assignment-Types REGISTRATION` and `RE_REGISTRATION` indicate that there are other Private Identities different from the Private Identity received in the SAR command being registered with the Public Identity received in the SAR command. For the `REGISTRATION` case, the S-CSCF sends another SAR with `SAT NO_ASSIGNMENT` to fetch restoration data for all IMPIs associated with this IRS. S-CSCF does not need to send a second SAR in the `RE_REGISTRATION` case. If the restoration procedure is enabled in the S-CSCF and the `Server-Assignment-Answer` indicates that the HSS does not support the restoration procedure, the S-CSCF stops updating the restoration information of the user in the same registration session. If the `Loose-Route-Indication AVP` is received for a registered Public Identity, it is stored by the S-CSCF.
- If it is unsuccessful and the restoration procedure is disabled, the S-CSCF maps the answer to a SIP response code and rejects the registration.
- If it is unsuccessful and the response code is `ERROR_IN_ASSIGNMENT_TYPE` and the restoration procedure is enabled, the S-CSCF restores all user information according to the restoration information received and sends another `Server-Assignment-Request` message with updated restoration information and the `USER_DATA_ALREADY_AVAILABLE AVP` to the HSS with `Server-Assignment-Type` set to `RE_REGISTRATION`.
- If no response is received from the HSS within Diameter time-out period, the registration is rejected.

If Deregistration (user, time-out or administrative deregistration), the S-CSCF sends the SAR requesting the HSS to clear the S-CSCF for a specified user.

User profile or Charging information is not downloaded. If the Deregistration is triggered by the user or the S-CSCF and if restoration procedure is enabled, the S-CSCF includes the updated restoration information in the Server-Assignment-Request.

The CSCF supports the 3GPP Standardized Restoration Procedure; if the Restoration Procedure is enabled, the S-CSCF always indicates the support of the feature by setting the IMSRestorationInd bit in the Supported-Features AVP of the SAR command. The CSCF also supports the 3GPP Shared Initial Filter Criteria (SiFC) feature; if the SiFC is enabled, the S-CSCF always indicates the support of the feature by setting the SiFC bit in the Supported-Features AVP of the SAR command. The Restoration Procedure and SiFC handling proceeds according to the returned Server-Assignment-Answer (SAA).

If terminating an INVITE, NOTIFY, UPDATE, or MESSAGE request to a registered user whose P-CSCF is not functioning, and if the P-CSCF restoration procedure is enabled, the S-CSCF sends a SAR to the HSS to trigger P-CSCF restoration. The SAR includes the SAR-Flags AVP with bit 0 set and the Supported-Features AVP with the third bit set to indicate the support of the P-CSCF restoration procedure.

If terminating call to an unregistered user, the S-CSCF sends a SAR to the HSS to store the S-CSCF name and request the user profile. If the restoration procedure is enabled in the S-CSCF, restoration information is requested as well.

If terminating call to a not registered Wildcarded Public Service Identity, the S-CSCF sends an SAR with Server-Assignment-Type = UNREGISTERED_USER to the HSS and includes the Wildcarded Public Service Identity, extracted from the received P-Profile-Key header, in the Wildcarded-Public-Identity AVP.

If originating call to an unregistered Wildcarded Public User Identity, the S-CSCF sends an SAR with Server-Assignment-Type = UNREGISTERED_USER to the HSS and includes the Wildcarded Public User Identity, extracted from the received P-Profile-Key header, in the Wildcarded-Public-Identity AVP.

If S-CSCF Network Initiated Deregistration, with Server-Assignment-Type = TIMEOUT_DEREGISTRATION, for a Wildcarded Public Service Identity, the S-CSCF includes the Wildcarded Public Service Identity in the Server-Assignment-Request, in the Wildcarded-Public-Identity AVP.

If S-CSCF Network Initiated Deregistration, with Server-Assignment-Type = TIMEOUT_DEREGISTRATION, for a Wildcarded Public User Identity, the S-CSCF includes the default Public User Identity from the Implicit Registration Set (IRS) in the Server-Assignment-Request, in the Public-Identity AVP, if it is a Public Identity. If the default Public User Identity is a Wildcarded Public User Identity, the S-CSCF includes it in the Wildcarded-Public-Identity AVP.

If initial registration of the emergency contact, and there are no other contacts registered, the S-CSCF sends an SAR with Server-Assignment-Type = NO_ASSIGNMENT.



If there is a registration of a regular, non-emergency, contact and there is already an emergency contact, the S-CSCF sends an SAR with Server-Assignment-Type = REGISTRATION.

If there is a deregistration of a regular contact and only the emergency contact remains registered, the S-CSCF sends an SAR Server-Assignment-Type = USER_DEREGISTRATION_STORE_SERVER_NAME.

When the regular contact has expired its registration period and only the emergency contact remains, the S-CSCF is to send an SAR with Server-Assignment-Type = TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME.

When the last contact which is an emergency contact expires, SAR with Server-Assignment-Type = TIMEOUT_DEREGISTRATION.

When an originating RegEvent subscription request is received from a contact of a registered user and if the restoration with subscription information procedure is enabled, the S-CSCF sends SAR to HSS with Server-Assignment-Type = RE_REGISTRATION and User-Data-Already-Available = USER_DATA_ALREADY_AVAILABLE to update the subscription information of the contact restoration information.

3.4.1 Use Cases – Registration, Deregistration, Downloading User Profile, and Restoration Procedures

3.4.1.1 Successful Initial Registration

A successful initial registration is shown in Figure 15.

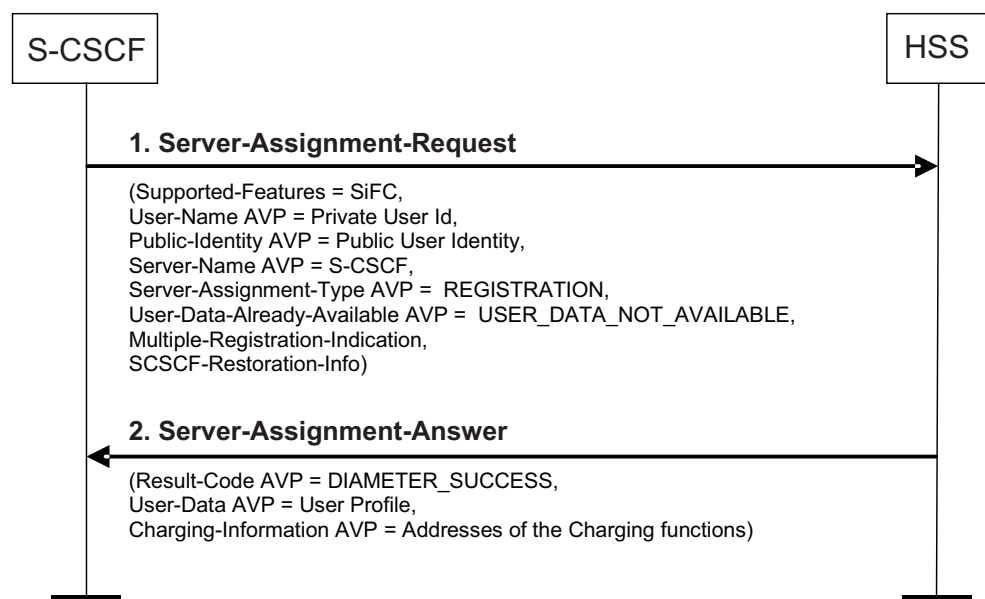


Figure 15 Successful Initial Registration

The procedure is as follows:

- 1 When the CSCF receives an initial registration from the user, the S-CSCF sends an SAR to update the HSS with the S-CSCF name and requests the User Data and Charging information for the specified user. The S-CSCF includes its own server name, the username, Public User Identity, and Server-Assignment-Type = REGISTRATION. If restoration procedure is enabled, the S-CSCF includes Multiple-Registration-Indication AVP and SCSCF-Restoration-Info AVP in the SAR.
- 2 The HSS stores the S-CSCF name and includes the user profile and Charging information in the SAA. If restoration procedure is supported by the HSS, the HSS stores the restoration information of the user. Result-Code is set to DIAMETER_SUCCESS. The HSS can include the supported features indication when it also supports the SiFC feature and the restoration procedure (by setting the IMSRestorationInd bit), or both. The Loose-Route-Indication AVP can be added by the HSS.

3.4.1.2

Successful Deregistration Notification Request – No User Profile Download

A successful deregistration notification request with no user profile download is shown in Figure 16.

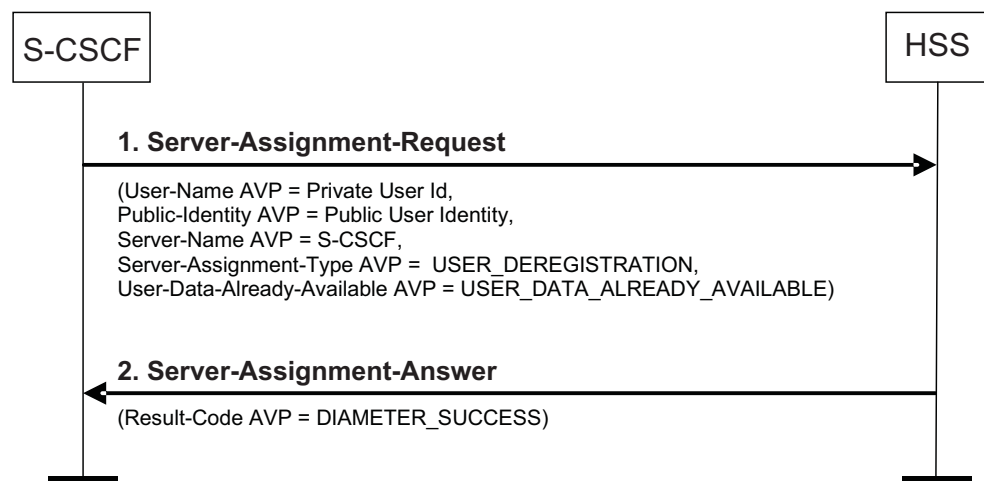


Figure 16 Successful Deregistration Notification Request – No User Profile Download

The procedure is as follows:

- 1 When the CSCF receives a deregistration from the user, the S-CSCF sends an SAR to the HSS to clear the stored S-CSCF name. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = USER_DEREGISTRATION.
- 2 The HSS clears the S-CSCF name and includes the Result-Code DIAMETER_SUCCESS in the SAA.



3.4.1.3 Registration Time-out

A registration time-out is shown in Figure 17.

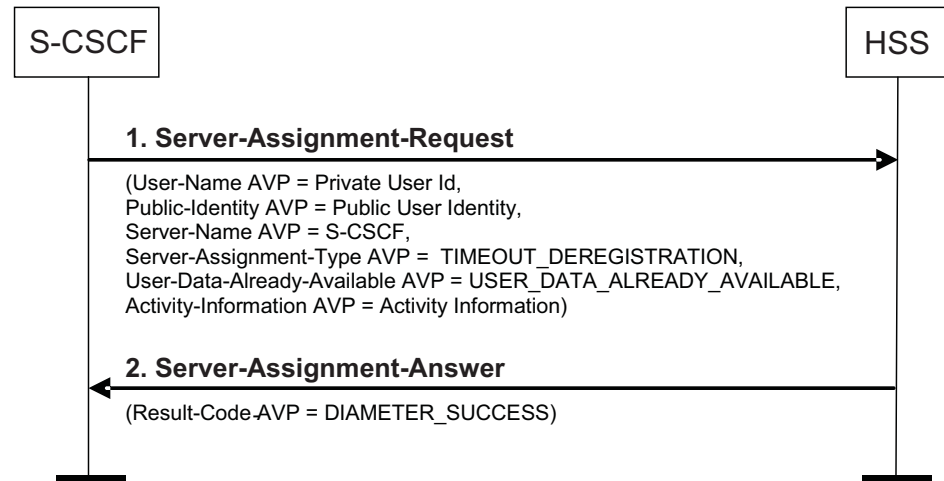


Figure 17 Registration Time-Out

The procedure is as follows:

- 1 When a registration times out, the S-CSCF sends a Server-Assignment-Request to the HSS to clear the stored S-CSCF name. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = TIMEOUT_DEREGISTRATION.
- 2 The HSS clears the S-CSCF name and includes the Result-Code DIAMETER_SUCCESS in the SAA.

Note: When the CSCF administrative state is changed to locked and there exist registered users in the CSCF, then the CSCF initiates deregistration for these users and sets the Server-Assignment-Type to TIMEOUT_DEREGISTRATION.

3.4.1.4 Administrative Deregistration

An administrative deregistration is shown in Figure 18.

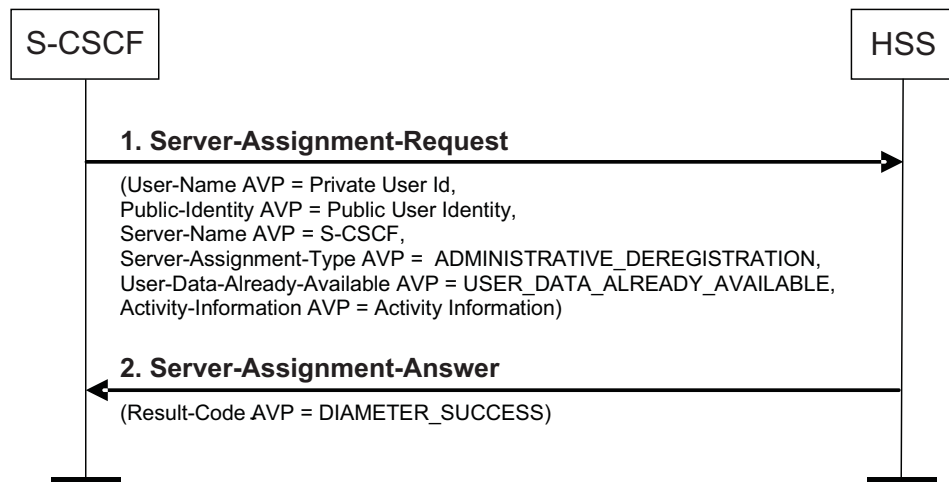


Figure 18 Administrative Deregistration

The procedure is as follows:

- 1 If administrative deregistration, the S-CSCF removes the registration state for the user by sending an SAR to the HSS to clear the stored S-CSCF name. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = ADMINISTRATIVE_DEREGISTRATION.
- 2 The HSS clears the S-CSCF name and includes the Result-Code DIAMETER_SUCCESS in the SAA.

Note: At internal S-CSCF failure, following a successful Server-Assignment-Request (SAA) response, the CSCF performs administrative deregistration by initiating deregistration for that user and setting the Server-Assignment-Type to ADMINISTRATIVE_DEREGISTRATION.

When the CSCF administrative state is changed to locked and there exist registered users in the CSCF, then the CSCF initiates deregistration for these users and sets the Server-Assignment-Type to TIMEOUT_DEREGISTRATION.

When a user is deregistered by an administrator in the S-CSCF through shortening the remaining registration time to 0, that is, to set the time element of ScscfShortenUserRegistrationTime to 0, the S-CSCF initiates deregistration for this user and sets the Server-Assignment-Type to ADMINISTRATIVE_DEREGISTRATION.

3.4.1.5

Successful Call – User Not Registered in S-CSCF and HSS, User Profile Download

A successful call where the user is not registered in the S-CSCF and the HSS, and the user profile is downloaded is shown in Figure 19.

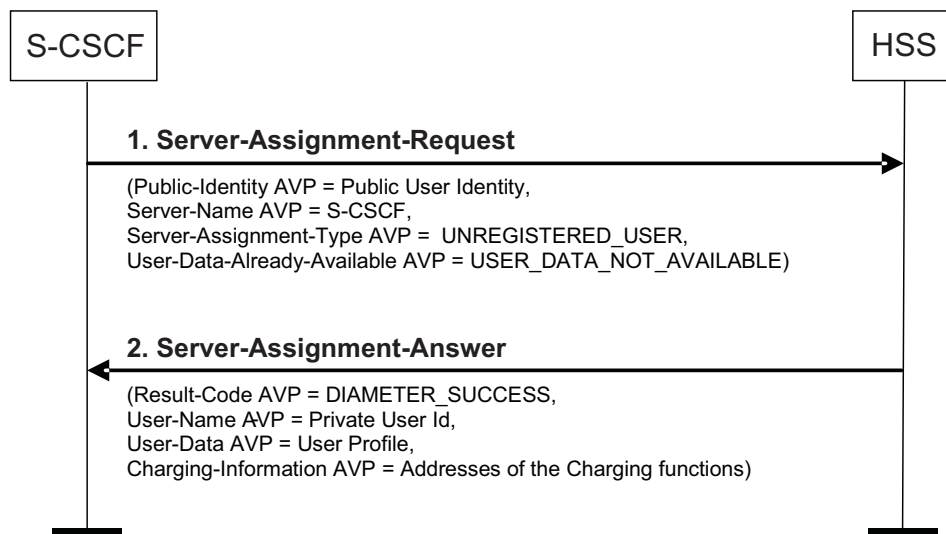


Figure 19 Successful Call – User Not Registered in S-CSCF and HSS, User Profile Download

The procedure is as follows:

- 1 In a call from or to an unregistered user, the S-CSCF sends a Server-Assignment-Request to the HSS to store the S-CSCF name and request the user profile. The S-CSCF includes the Public User Identity and Server-Assignment-Type = UNREGISTERED_USER.
- 2 The HSS stores the S-CSCF name and includes the user profile and Charging information in the SAA. Result-code is set to **DIAMETER_SUCCESS**. The HSS can include the supported features indication when it also supports the SiFC feature. The Loose-Route-Indication AVP can be added by the HSS.

3.4.1.6

Successful Call – User Not Registered in S-CSCF but Registered in HSS, Restoration Information, and User Profile Download

A successful call where the user is not registered in the S-CSCF but registered in the HSS and the restoration information and user profile are downloaded, is shown in Figure 20.

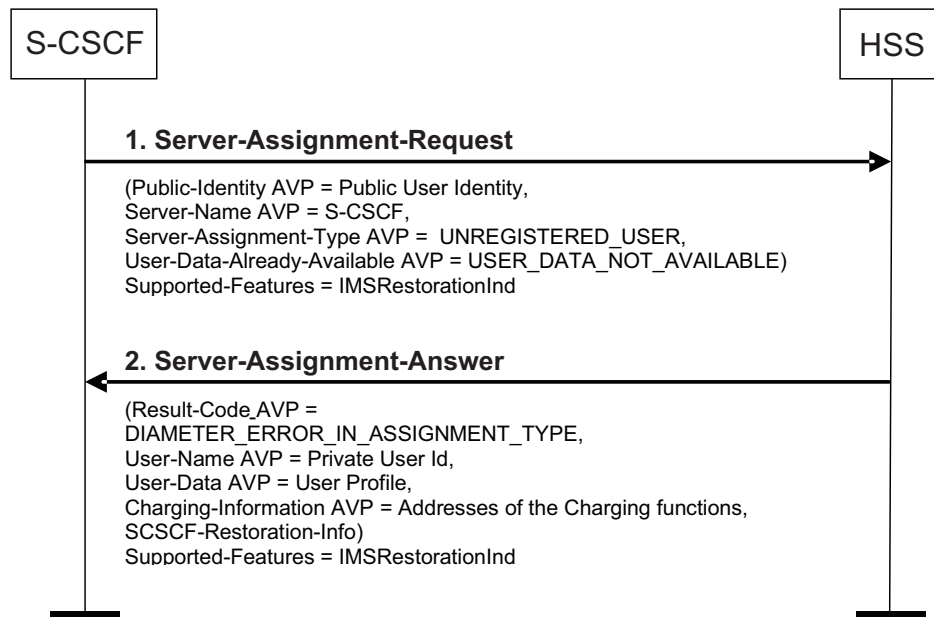


Figure 20 Successful Call – User Not Registered in S-CSCF but Registered in HSS, Restoration Information, and User Profile Download

The procedure is as follows:

- 1 In a call from or to an unregistered user, the S-CSCF sends an SAR to the HSS to store the S-CSCF name and request the user profile and restoration information, if the restoration procedure is enabled in the S-CSCF. The S-CSCF includes the Public User Identity and Server-Assignment-Type = UNREGISTERED_USER.
- 2 The HSS stores the S-CSCF name and includes the user profile, restoration information, if supported, and Charging information in the SAA. Result-code set to **DIAMETER_Error_in_Assignment_Type**. The Loose-Route-Indication AVP can be added by the HSS.

3.4.1.7

Successful Registration Notification Request – User in Unregistered State

A successful registration notification request where the user is in unregistered state is shown in Figure 21.

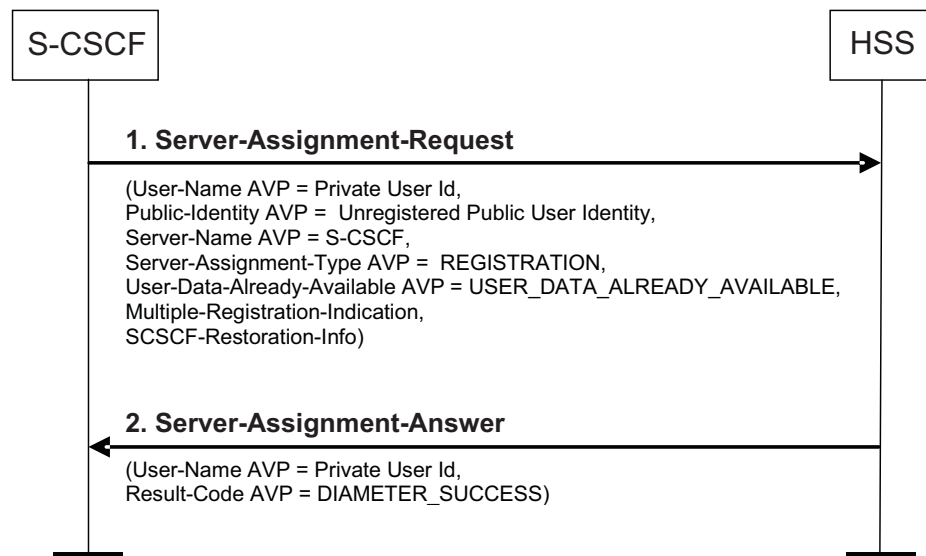


Figure 21 Successful Registration Notification Request – User in Unregistered State

The procedure is as follows:

- 1 The S-CSCF sends an SAR to the HSS to store the S-CSCF name. The S-CSCF includes the username, Public User Identity, Multiple-Registration-Indication, SCSCF-Restoration-Info, and Server-Assignment-Type = REGISTRATION. The user is unregistered, so the S-CSCF sends USER_DATA_ALREADY_AVAILABLE.
- 2 The HSS returns the SAA with Result-Code DIAMETER_SUCCESS.

3.4.1.8 Unsuccessful Registration Notification Request

An unsuccessful registration notification request is shown in Figure 22.

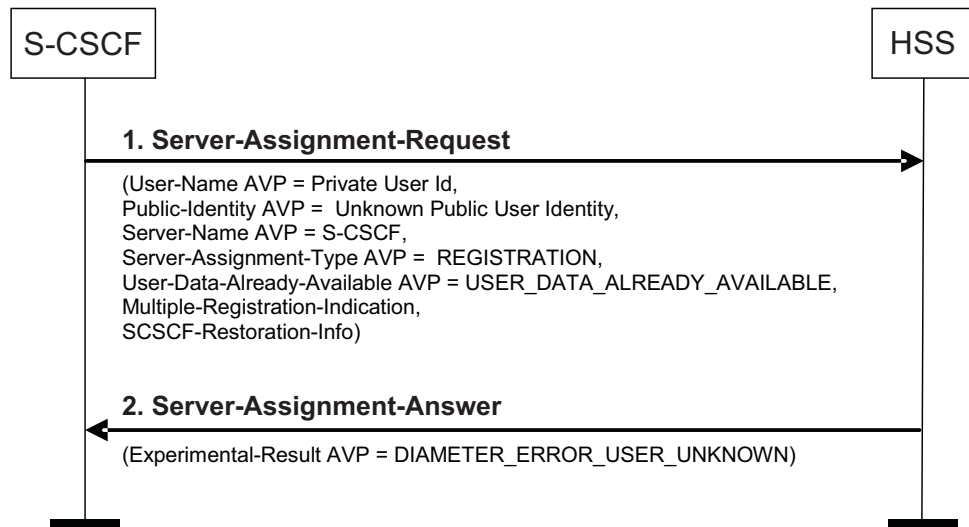


Figure 22 Unsuccessful Registration Notification Request

The procedure is as follows:

- 1 The S-CSCF sends an SAR to the HSS to store the S-CSCF name and the restoration information, if restoration procedure is enabled in the S-CSCF. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = REGISTRATION. If restoration procedure is enabled, SCSCF-Restoration-Info AVP and Multiple-Registration-Indication AVP are included in the Server-Assignment-Request.
- 2 If the user is unknown in the HSS, the HSS returns the SAA with Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN.

3.4.1.9

Successful Registration Notification – Answer Rejected

A successful registration notification with an answer rejected is shown in Figure 23.

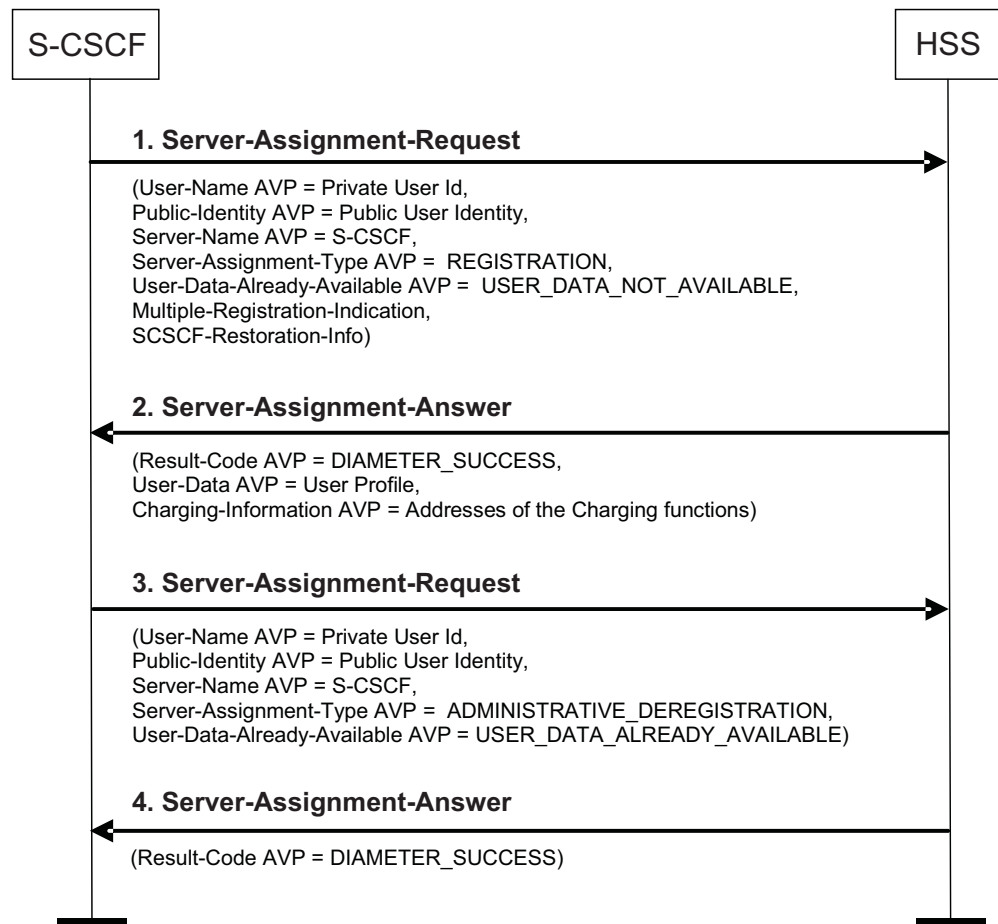


Figure 23 Successful Registration Notification – Answer Rejected

The procedure is as follows:

- 1 When the S-CSCF receives an initial registration from the user, the S-CSCF sends an SAR to update the HSS with the S-CSCF name, SCSCF-Restoration-Info, and requests the User Data and Charging information for the specified user. The S-CSCF includes its own server name, the username, Public User Identity, and Server-Assignment-Type = REGISTRATION. If the Restoration Procedure is enabled, Multiple-Registration-Indication and SCSCF-Restoration-Info are also included in the SAR command.
- 2 The HSS stores the S-CSCF name and the restoration information. The HSS includes the user profile and charging information in the SAA. Result-Code set to DIAMETER_SUCCESS.

- 3 If a SiFC identity included in the user data is not defined in the S-CSCF or an Alias Identity Group Id is present in the user data, the S-CSCF removes the registration state for the user by sending an SAR to the HSS to clear the stored S-CSCF name. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = ADMINISTRATIVE_DEREGISTRATION.
- 4 The HSS clears the S-CSCF name and includes the Result-Code DIAMETER_SUCCESS in the SAA.

3.4.1.10

Successful Request of User Data

A successful request of the user data from the HSS is shown in Figure 24.

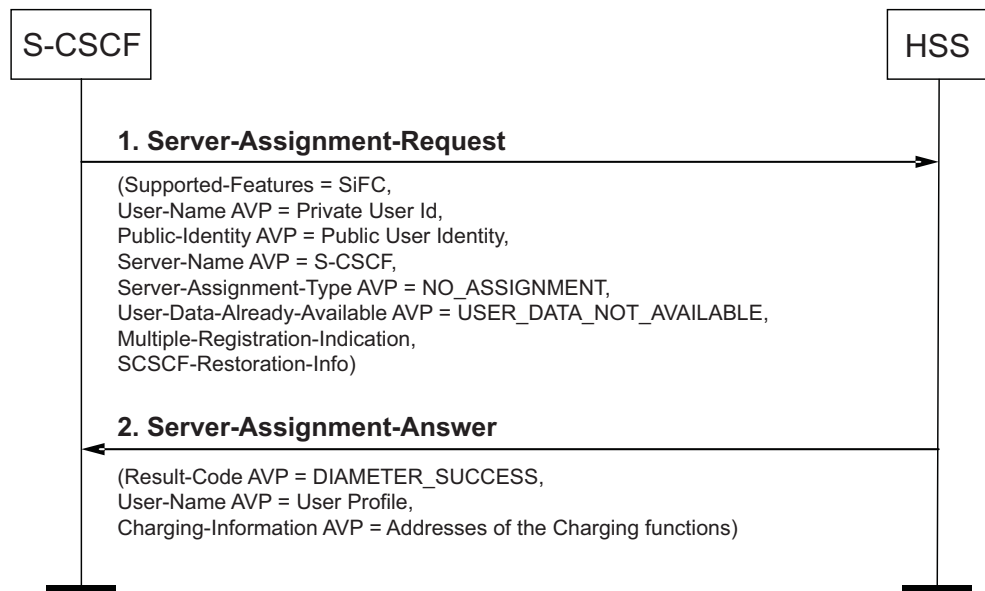


Figure 24 Successful Request of User Data

The procedure is as follows:

- 1 When the S-CSCF requires user data, it sends an SAR to request the User Data and charging information for the specified user. The S-CSCF includes its own server name, the username, Public User Identity, and Server-Assignment-Type = NO_ASSIGNMENT.
- 2 The HSS includes the user profile and charging information in the SAA. Result-Code is set to DIAMETER_SUCCESS.

3.4.1.11

Successful Registration Time-out Notification with Request to Store Server Name

A registration time-out and the S-CSCF request to the HSS to deregister the user but to keep the server name is shown in Figure 25.

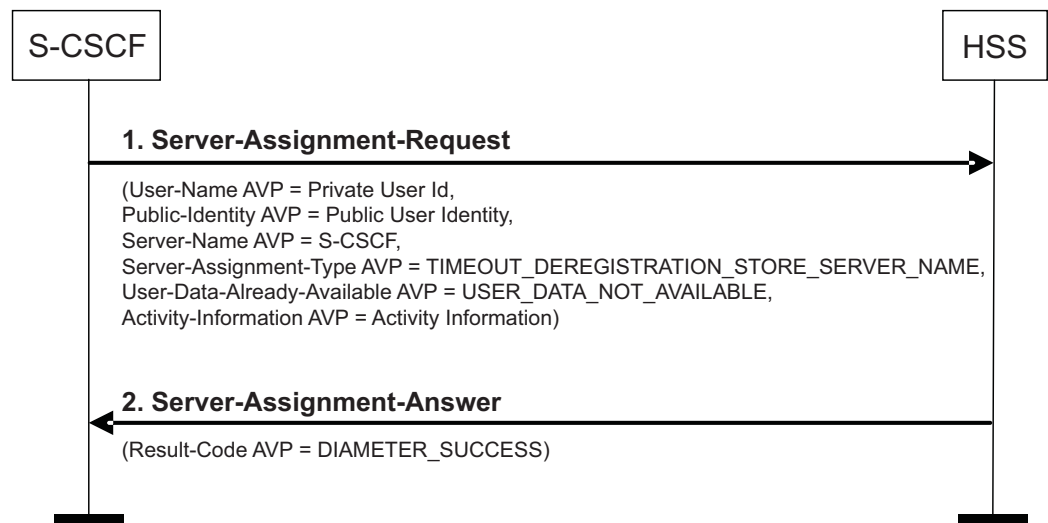


Figure 25 Successful Registration Time-Out Notification with Request to Store Server Name

The procedure is as follows:

- 1 When the last regular contact times out, the S-CSCF sends an SAR to the HSS to store the S-CSCF name. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME.
- 2 The HSS sets the registration state of the Public User Identity to **unregistered**, keeps the server name, and includes the Result-Code DIAMETER_SUCCESS in the SAA.

3.4.1.12 Successful Deregistration Notification with Request to Store Server Name

A successful deregistration notification request to deregister the user but keep the server name is shown in Figure 26.

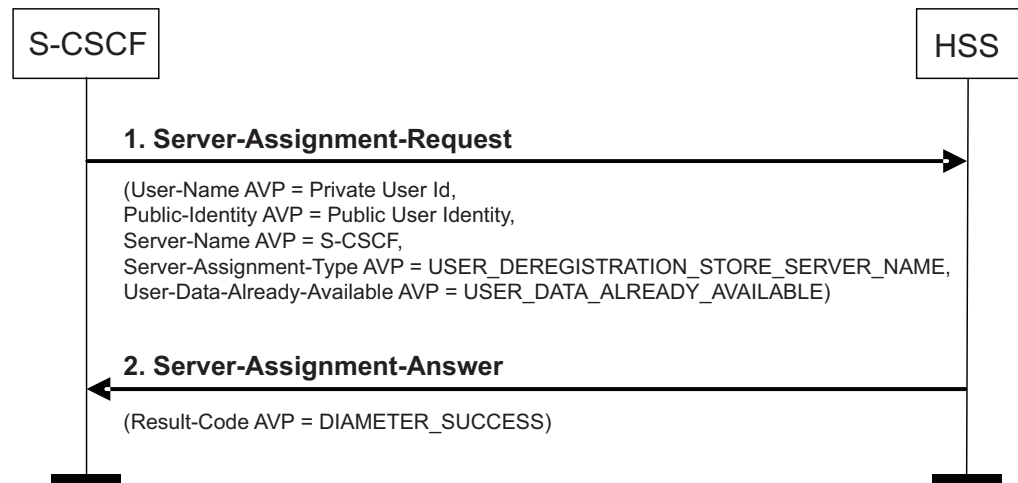


Figure 26 Successful Deregistration Notification with Request to Store Server Name

The procedure is as follows:

- 1 When the last regular contact is deregistered from the user, the S-CSCF sends an SAR to the HSS to keep the S-CSCF name. The S-CSCF includes the username, Public User Identity, and Server-Assignment-Type = USER_DEREGISTRATION_STORE_SERVER_NAME.
- 2 The HSS sets the registration state of the Public User Identity to unregistered, keeps the server name, and includes the Result-Code DIAMETER_SUCCESS in the SAA.

3.4.1.13 Successful Triggering of P-CSCF Restoration Procedure for an IMPU Registered with One IMPI

Successful triggering of the P-CSCF Restoration Procedure for an IMPU that is registered with one IMS Private Identity (IMPI) is shown in Figure 27.

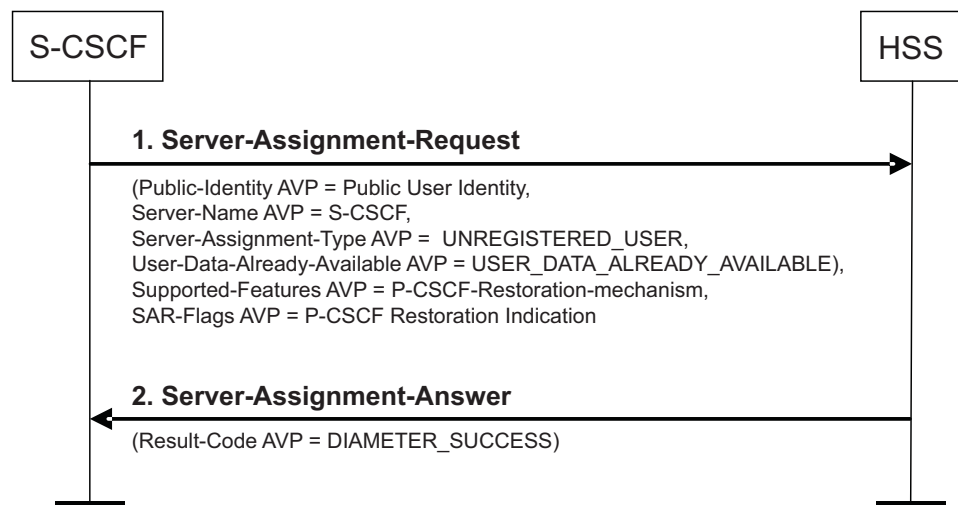


Figure 27 Successful Triggering of P-CSCF Restoration Procedure for an IMPU Registered with One IMPI

The procedure is as follows:

- 1 When the terminating P-CSCF is not available, the S-CSCF triggers the HSS-based P-CSCF Restoration Procedure for the terminating user by sending a Server-Assignment-Request to the HSS.

If the terminating user is registered with one Private User Identity, the Server-Assignment-Type is set to **UNREGISTERED_USER**. The SAR-Flags AVP is set to **P-CSCF Restoration Indication**. The Supported-Features AVP is set to **P-CSCF-Restoration-mechanism**. If the terminating user is registered with multiple Private User Identities, see Section 3.4.1.14 Successful Triggering of P-CSCF Restoration Procedure for an IMPU Registered with Multiple IMPIs on page 33 for more information.

- 2 If the HSS successfully executes the P-CSCF Restoration Procedure, then the HSS sets the registration state of the Public User Identity to **unregistered**, keeps the server name, and includes the Result-code **DIAMETER_SUCCESS** in the SAA.

3.4.1.14

Successful Triggering of P-CSCF Restoration Procedure for an IMPU Registered with Multiple IMPIs

Successful triggering of the P-CSCF Restoration Procedure for an IMPU that is registered with multiple IMPIs is shown in Figure 28.

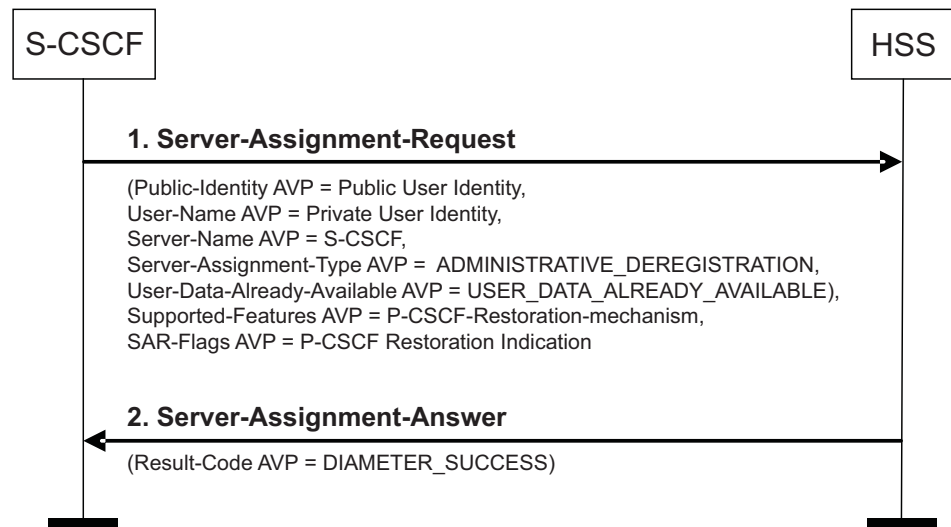


Figure 28 Successful Triggering of P-CSCF Restoration Procedure for an IMPU Registered with Multiple IMPIs

The procedure is as follows:

- 1 When the terminating P-CSCF is not available, the S-CSCF triggers the HSS-based P-CSCF Restoration Procedure for the terminating user by sending a SAR to the HSS.

If the terminating user is registered with multiple Private User Identities, the SAT is set to **ADMINISTRATIVE_DEREGISTRATION**. The Private User Identity which triggers the P-CSCF Restoration Procedure is included in the User-Name AVP. The SAR-Flags AVP is set to **P-CSCF Restoration Indication**. The Supported-Features AVP is set to **P-CSCF-Restoration-mechanism**.
- 2 If the HSS successfully executes the P-CSCF Restoration Procedure, then the HSS sets the registration state of the Private User Identity to **deregistered**, and includes the Result-code **DIAMETER_SUCCESS** in the SAA.

3.4.1.15

Successful RegEvent Subscription Request – No User Profile Download

A successful RegEvent subscription is shown in Figure 29.

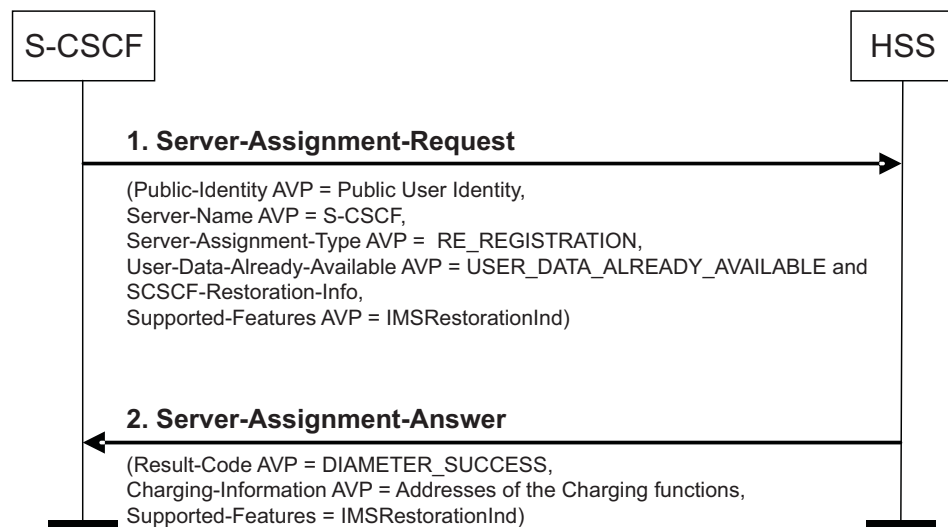


Figure 29 Successful RegEvent Subscription Request – No User Profile Download

The procedure is as follows:

- 1 When a RegEvent subscription is received from a contact of a registered user and if the restoration with subscription information procedure is enabled, the S-CSCF sends an SAR to the HSS to store the S-CSCF name and to update the subscription information. The S-CSCF includes the Public User Identity, Server-Assignment-Type = RE_REGISTRATION, User-Data-Already-Available = USER_DATA_ALREADY_AVAILABLE, and SCSCF-Restoration-Info AVP that contains Subscription-Info AVP.
- 2 The HSS stores the S-CSCF name and the restoration information with subscription information and includes Charging information in the SAA. The Result-code AVP is set to **DIAMETER_SUCCESS**. The Loose-Route-Indication AVP can be added by the HSS.

3.5 Authentication Request

This procedure is used by the S-CSCF to the HSS, for the following:

- AKA authentication; retrieve Authentication Vectors (AVs) from the HSS.
- AKA authentication; resolve synchronization failures between the sequence numbers in UE and the HSS.
- NASS Bundled Authentication retrieves the Line Identifiers or an indication that the Line Profile verification has successfully been performed in the HSS.
- Digest Authentication; retrieve AVs from the HSS.
- GPRS IMS Bundled Authentication (GIBA) authentication, retrieve UE IP address from the HSS.

The S-CSCF requests the Authentication Request by the Multimedia-Authentication-Request (MAR) command.

When the S-CSCF has determined that the IMS AKA authentication applies, it sends an MAR to the HSS requesting the AV. The request identifies the user by both private and Public User Identities and specifies that the AVs are desired and the SIP-Authentication-Scheme AVP set to Digest-AKA_{v1}-MD5.

When MAA with Result-Code DIAMETER_SUCCESS is received, the S-CSCF extracts the RAND, AUTN, XRES, IK, and CK from the AV and includes it in a challenge to the UE.

When the S-CSCF has determined that the NASS Bundled Authentication applies, it sends an MAR to the HSS requesting the Line Identifiers for NASS-Bundled. The request includes the private and Public User Identities and the SIP-Authentication-Scheme AVP is set to NASS-Bundled. The private user identity is sent by the UE or if not, the S-CSCF derives it from the To header of the SIP REGISTER request.

The S-CSCF receives the Multimedia-Authentication-Answer (MAA) with Result-Code DIAMETER_SUCCESS and one or several Line-Identifier AVPs. The SIP-Authentication-Scheme AVP is set to NASS-Bundled. The S-CSCF compares the string in the Line-Identifier AVPs with the string in the dsl-location parameter in the PAccess-Network-Id header. If there is a match, the authentication is successful and the S-CSCF continues to process the request.

When the S-CSCF has determined that Digest Authentication applies, it sends an MAR to the HSS with the SIP-Authentication-Scheme AVP set to SIP Digest. The request identifies the user by both private and Public User Identities and specifies that the AVs are desired. The private user identity is either sent by the UE or if not, the S-CSCF derives it from the To header of the SIP REGISTER request.

When the MAA with Result-Code DIAMETER_SUCCESS is received, the S-CSCF extracts the SIP Digest Authentication data (Digest-Realm, Digest-Algorithm, Digest-QoP, Digest-HA1, and optionally Secondary-Digest-HA1) from the response and uses the information to challenge the UE.

When the S-CSCF has determined that GIBA authentication applies, it sends an MAR to the HSS with the SIP-Authentication-Scheme AVP set to **Early-IMS-Security**. The request identifies the user by both private and Public User Identities and specifies that one authentication item, the UE IP address, is desired. The private user identity is not sent by the UE but the S-CSCF derives it from the SIP REGISTER request To header.

When the MAA with Result-Code DIAMETER_SUCCESS and SIP-Authentication-Scheme Early-IMS-Security is received, the S-CSCF extracts the UE IP address from the response and uses the information to compare to the UE IP address received in the REGISTER request.

When the S-CSCF has determined that NASS Bundled Authentication and Digest both can apply, it sends an MAR to the HSS with the SIP-Authentication-Scheme AVP set to **Unknown**. The request identifies the user by both the private and Public



User Identities. The private user identity is either sent by the UE or if not, the S-CSCF derives it from the To header of the SIP REGISTER request.

The S-CSCF receives the MAA with Result-Code DIAMETER_SUCCESS and the SIP-Authentication-Scheme AVP is set to **NASSBundled** or SIP Digest. If set to **SIP Digest**, the regular SIP digest procedures are executed. If set to **NASS-Bundled**, the S-CSCF compares the string in the Line-Identifier AVPs with the string in the ds1-location parameter in the P-Access-Network-Id header. If there is a match, the authentication is successful and the S-CSCF continues to process the request. If the Line-Identifier AVP contains the string Line_Profile, no further authentication is performed by the S-CSCF.

When the MAA with an error indication is received or the S-CSCF fails to get any response from the HSS, that is time-out, the SIP request is rejected. In either case, no security information is included in the response.

3.5.1 Use Cases – Authentication Request

3.5.1.1 Successful Authentication Request, AKA

A successful authentication request with AKA, is shown in Figure 30.

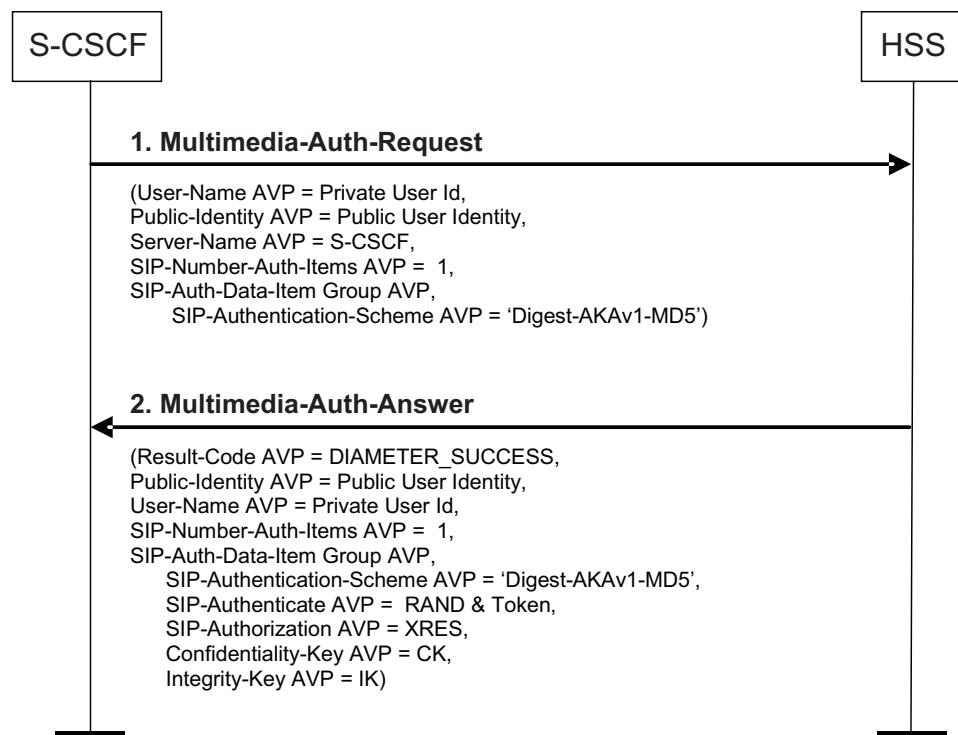


Figure 30 Successful Authentication Request – AKA

The procedure is as follows:

- 1 If AKA authentication, the S-CSCF sends an MAR to the HSS requesting an AV. The request includes the Private and Public User Identities, specifies that an AV is desired and the SIP-Authentication-Scheme AVP set to **Digest-AKAv1-MD5**.
- 2 The HSS responds with an MAA containing the Authentication data items including the Authentication Vector and the Result-Code set to **DIAMETER_SUCCESS**.

3.5.1.2

Successful Authentication Request, AKA – Synchronization Failure

A successful authentication request with AKA and synchronization failure is shown in Figure 31.

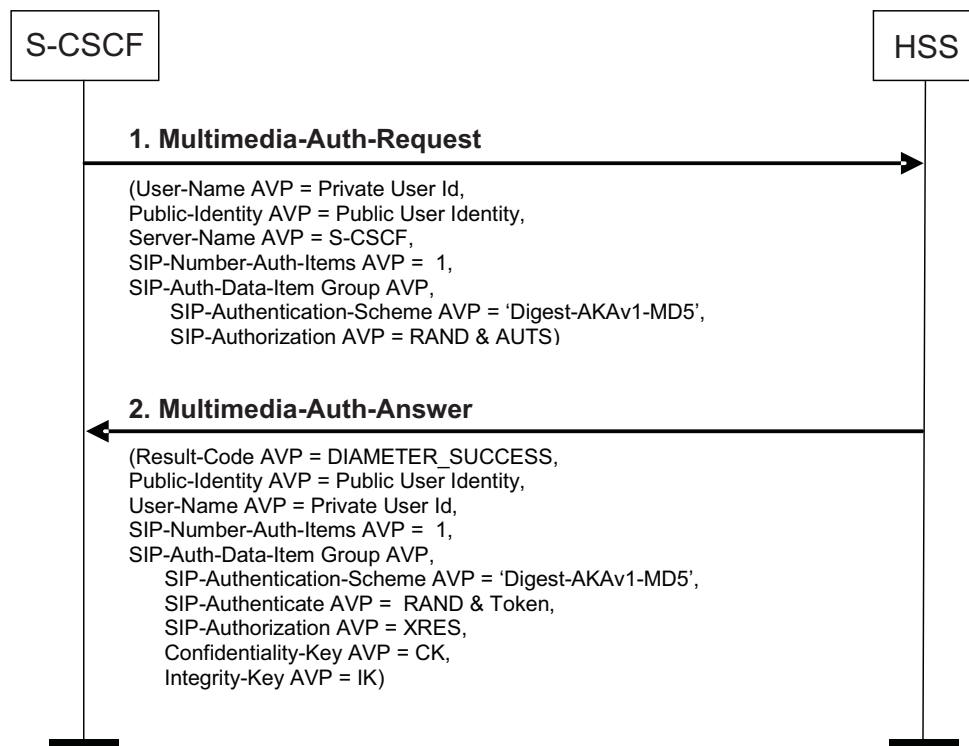


Figure 31 Successful Authentication Request, AKA – Synchronization Failure

The procedure is as follows:



- 1 If AKA authentication, S-CSCF sends an MAR to the HSS requesting an AV. The request includes the private and Public User Identities, specifies that a single AV is desired and the SIP-Authentication-Scheme AVP set to **Digest-AKAv1-MD5**.
- 2 The request indicates that there is a synchronization failure, the HSS compares the server names. If identical, the HSS processes the AUTS and responds with an MAA containing the requested Authentication information and the Result-Code set to **DIAMETER_SUCCESS**. If not, the HSS stores the S-CSCF name, downloads the authentication data received in the request, and sets the authentication pending flag for the user. Result-Code **DIAMETER_SUCCESS** is returned in the MAA.

3.5.1.3

Successful Authentication Request-NASS-Bundled

A successful authentication request with NASS-Bundled is shown in Figure 32.

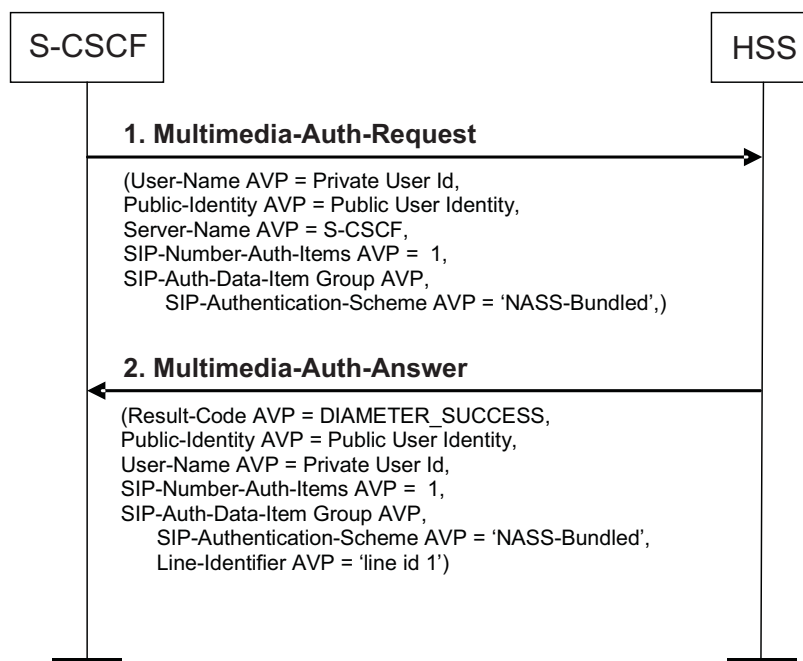


Figure 32 Successful Authentication Request – NASS-Bundled

The procedure is as follows:

- 1 If NASS Bundled Authentication, the S-CSCF sends a Multimedia-Auth-Request to the HSS requesting the line identifiers. The request includes the private and Public User Identities and the SIP-Authentication-Scheme AVP set to **NASS-Bundled**.
- 2 The HSS responds with an MAA containing the Authentication data items including the line identifiers and the Result-Code set to **DIAMETER_SUCCESS**.

3.5.1.4 Unsuccessful Authentication Request – NASS-Bundled Not Supported for User

An unsuccessful authentication request with NASS-Bundled not supported for the user is shown in Figure 33.

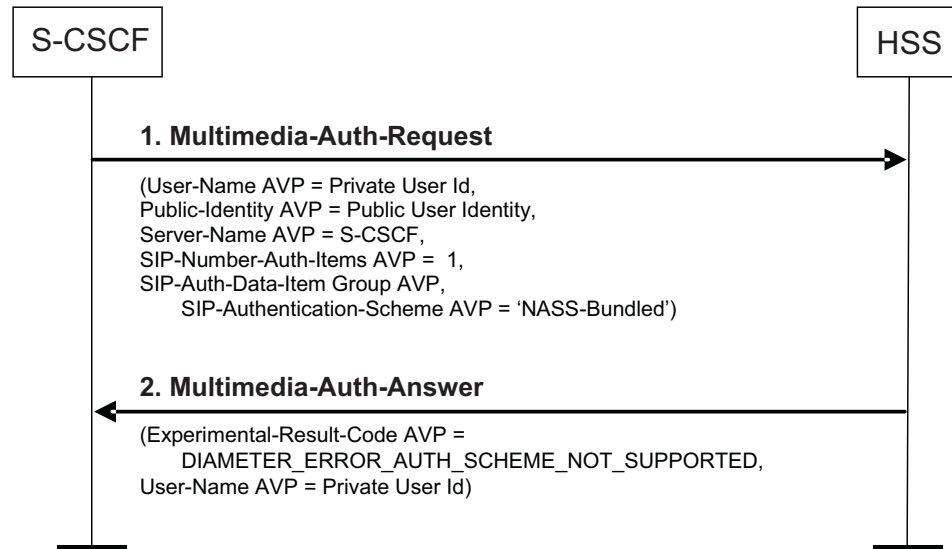


Figure 33 Unsuccessful Authentication Request – NASS-Bundled Not Supported for User

The procedure is as follows:

- 1 The S-CSCF sends an MAR to the HSS requesting the Line Identifies for NASS-Bundled. The request includes the private and Public User Identities and the SIP-Authentication-Scheme AVP set to NASS-Bundled.
- 2 The NASS Bundled Authentication is not supported for the user, so the HSS responds with an MAA containing the Experimental-Result-Code set to **DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED**.

3.5.1.5 Successful Authentication Request – Digest

A successful authentication request with digest is shown in Figure 34.

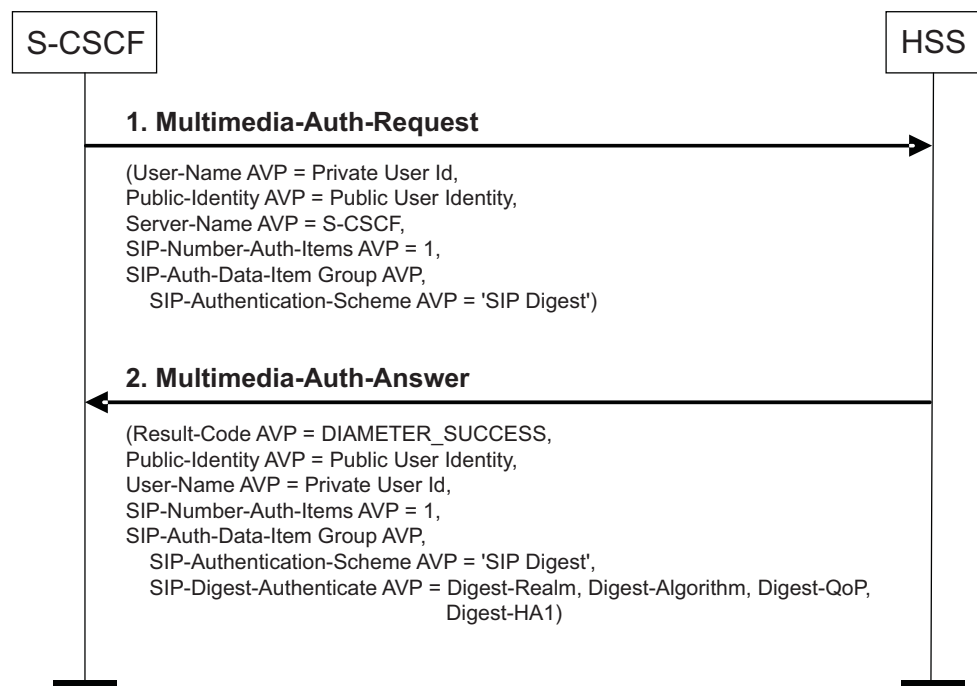


Figure 34 Successful Authentication Request – Digest

The procedure is as follows:

- 1 If SIP Digest Authentication, the S-CSCF sends a **Multimedia-Auth-Request** to the HSS requesting an AV for SIP Digest. The request includes the Private and Public User Identities, and the SIP-Authentication-Scheme AVP is set to **SIP Digest**.
- 2 The HSS responds with an MAA containing the Authentication data items including the Authentication Vector and the Result-Code set to **DIAMETER_SUCCESS**.

3.5.1.6 Unsuccessful Authentication Request – Digest Not Supported for User

An unsuccessful authentication request with digest not supported for the user is shown in Figure 35.

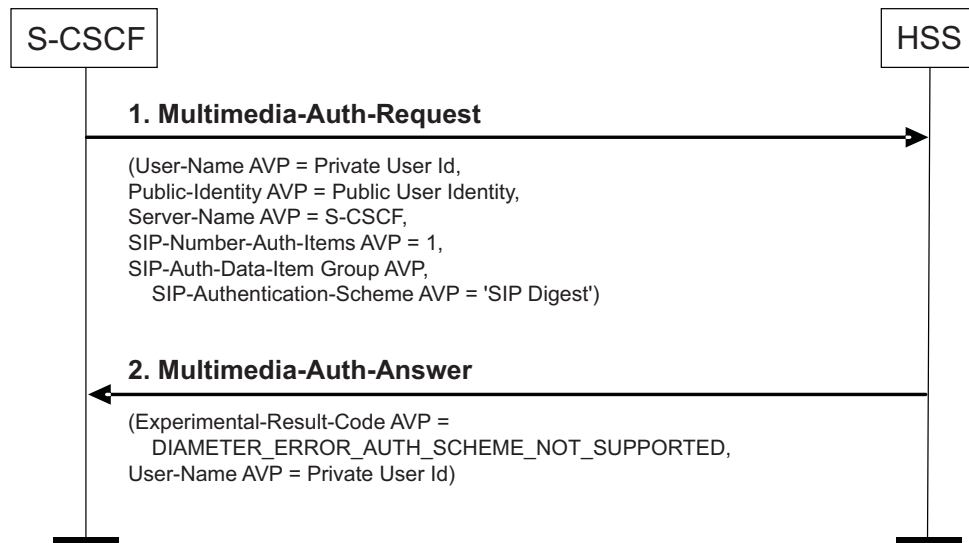


Figure 35 Unsuccessful Authentication Request – Digest Not Supported for User

The procedure is as follows:

- 1 If Digest Authentication, the S-CSCF sends an MAR to the HSS requesting an AV for SIP Digest. The request includes the private and Public User Identities, and the SIP-Authentication-Scheme AVP set to **SIP Digest**.
- 2 SIP Digest Authentication is not supported for the user so, the HSS responds with an MAA containing the Experimental-Result-Code set to **DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED**.

3.5.1.7 Successful Authentication Request – GIBA

A successful authentication request with GIBA is shown in Figure 36.

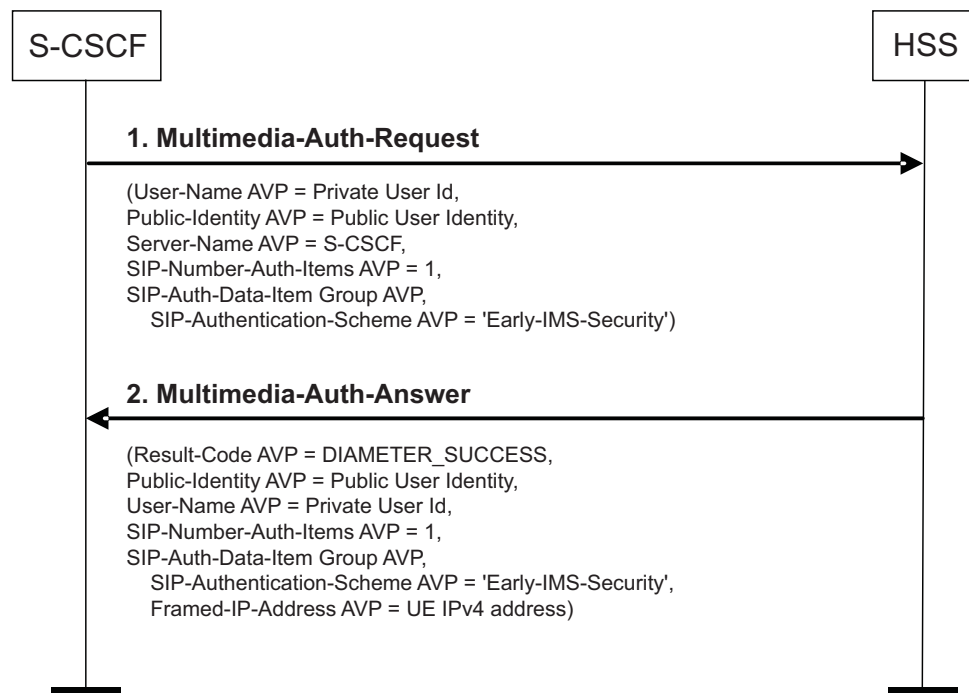


Figure 36 Successful Authentication Request – GIBA

The procedure is as follows:

- 1 If GPRS IMS Bundled Authentication, the S-CSCF sends an MAR to the HSS requesting the UE IP address. The request includes the private and Public User Identities, and the SIP-Authentication-Scheme AVP is set to **Early-IMS-Security**. The private user identity is derived from the Public User Identity, since no SIPAuthorization header is received in the initial REGISTER.
- 2 The HSS responds with an MAA containing the Authentication data items including the UE IP address and the SIP-Authentication-Scheme set to **Early-IMS-Security**, and the Result-Code set to **DIAMETER_SUCCESS**.

3.5.1.8

Unsuccessful Authentication Request – GIBA Not Supported for User

An unsuccessful authentication request with GIBA not supported for the user is shown in Figure 37.

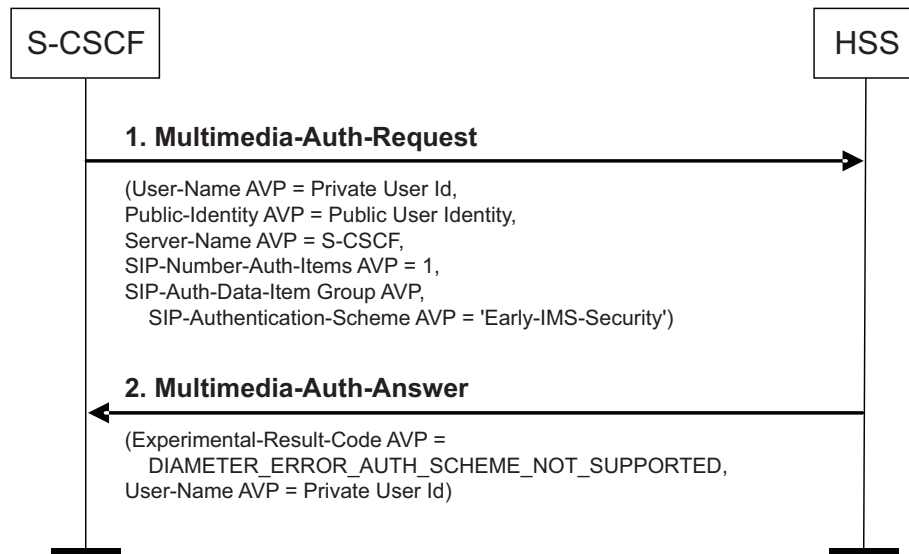


Figure 37 Unsuccessful Authentication Request – GIBA Not Supported for User

The procedure is as follows:

- 1 Request to the HSS requesting the UE IP address. The request includes the private and Public User Identities, and the SIP-Authentication-Scheme AVP is set to **Early-IMS-Security**.
- 2 GIBA is not supported for the user, so the HSS responds with an MAA containing the Experimental-Result-Code set to **DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED**.

3.5.1.9

Successful Authentication Request – Unknown Authentication

A successful authentication request with unknown authentication is shown in Figure 38.

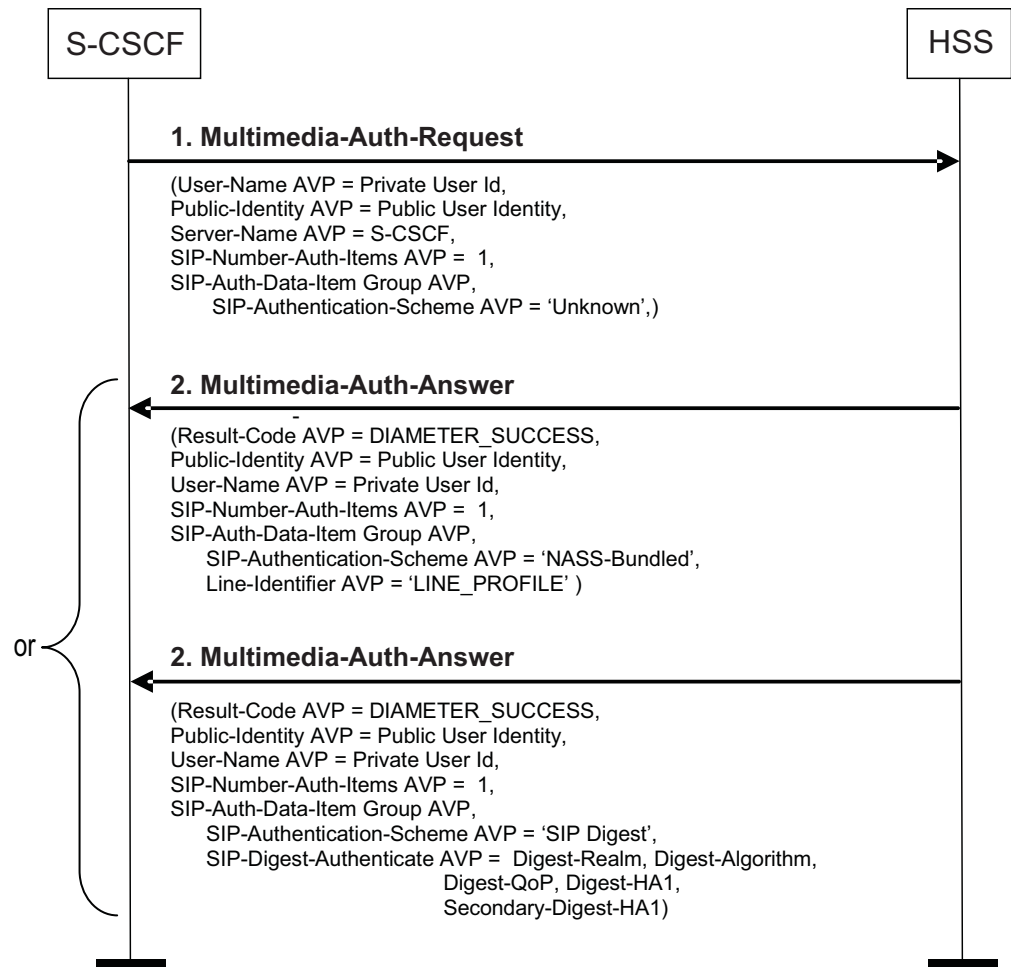


Figure 38 Successful Authentication Request – Unknown Authentication

The procedure is as follows:

- 1 If NBA and Digest Authentication both apply, the S-CSCF sends an MAR to the HSS with the SIP-Authentication-Scheme AVP is set to **Unknown**. The request includes the private and Public User Identities.
- 2 The HSS responds with an MAA and the Result-Code set to DIAMETER_SUCCESS. The SIP-Authentication-Scheme AVP is set to either **SIP Digest** or **NASS-Bundled**. If set to **SIP Digest**, the MAA also contains the Digest Authentication data items including the optional Secondary-Digest-HA1. If set to **NASSBundled**, the MAA includes either one Line-Identifier AVP which contains the string Line_Profile or one or several Line-Identifier AVP where each AVP contains a fixed broadband access line identifier.

3.5.1.10

Unsuccessful Authentication Request – Unknown Authentication, No Matching Line Profile for User

An unsuccessful authentication request with unknown authentication and no matching line profile for user is shown in Figure 39.

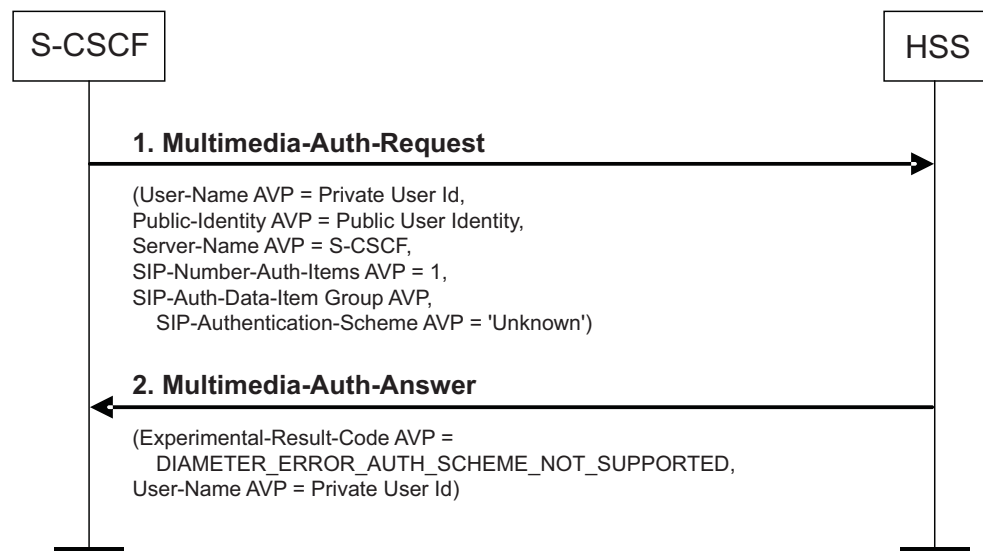


Figure 39 Unsuccessful Authentication Request – Unknown Authentication, No Matching Line Profile for User

The procedure is as follows:

- 1 If NBA and Digest Authentication both apply, the S-CSCF sends an MAR to the HSS with the SIP-Authentication-Scheme AVP is set to **Unknown**. The request includes the private and Public User Identities.
- 2 There is no matching line profile for the user, so the HSS responds with an MAA containing the Experimental-Result-Code set to **DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED**.

3.6

Network Initiated Deregistration

The following procedure is used by the HSS to the S-CSCF to request deregistration of a user, Public Identity, or a list of Public Identities:

- The HSS requests the Network Initiated Deregistration through the Registration Termination Request (RTR) command.

The RTR contains a Private User Identity and optionally one or several Public User Identities.

- The S-CSCF checks the processor load. If the processor capacity cannot be granted, the S-CSCF returns the Result-Code **DIAMETER_TOO_BUSY**. Also other initial checks of the Diameter request are performed.



- The S-CSCF checks that the Private User Identity and Public User Identity has the state registered or unregistered in the CSCF. If not, then the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN is returned.

Where the RTR contains only a Private User Identity, and none of the Public Identities are emergency registered, the Private User Identity is removed from the CSCF database. All Public User Identities or Implicit Registration Sets tied to the Private User Identity are removed unless they are also tied to other Private User Identities.

Where the RTR contains a Private User Identity and one or more Public User Identities which are not emergency registered, all implicit registrations sets that the Public User Identities belongs to are removed. In case they are associated with other Private User Identities, the Public Identity is only removed for the private identity specified in the request. If a list of Public User Identities is received, each registered Public User Identity is deregistered. An unregistered Public User Identity in the list is ignored.

The Private User Identity is removed if no more Public User Identities or Implicit Registration Sets are tied to it.

Where the HSS initiates a deregistration of a Wildcarded Public Identity, the RTR contains the Private identity, User-Name, associated with the Wildcarded Public Identity.

Where deregistration of a Wildcarded Public User Identity, the RTR can also contain one or more Distinct IMPUs from the IRS.

If the HSS initiates a permanent deregistration of a Private User Identity with the Reason Code PERMANENT_TERMINATION, where one or a subset of the Public Identities or Implicit Registration Set is emergency registered, the S-CSCF only deregisters the public identities that are not emergency registered.

Where the RTR results in that Public User Identities or Implicit Registration Sets are removed the following two steps are performed for each removed Public User Identity or Implicit Registration Set, as follows:

- The S-CSCF releases each multimedia session that was initiated with this Public User Identity or any of the implicitly registered Public User Identities.
 - The S-CSCF removes the Public User Identities, their registration states and their associated service profiles.
- After successful deregistration, the S-CSCF sends a Registration Termination Answer (RTA) with Result-Code = "DIAMETER_SUCCESS" to the HSS.
 - If a proper subset of the identities to be deregistered are emergency registered, the S-CSCF sends an RTA with Result-Code = "DIAMETER_LIMITED_SUCCESS". The RTA includes a list of IMPI/IMPU pairs

that are emergency registered, and have been requested to be deregistered by the HSS through the RTR. One IMPI/IMPU pair is included in one Identity-with-Emergency-Registration AVP.

- If all identities to be deregistered are emergency registered, the S-CSCF sends an RTA with Result-Code = “DIAMETER_UNABLE_TO_COMPLY.” The RTA includes a list of IMPI/IMPU pairs that are emergency registered and have been requested to be deregistered by the HSS through the RTR. One IMPI/IMPU pair is included in one Identity-with-Emergency-Registration AVP.

3.6.1 Use Cases – Network Initiated Deregistration

3.6.1.1 Successful Network Initiated Deregistration of User

A successful network initiated deregistration of a user is shown in Figure 40.

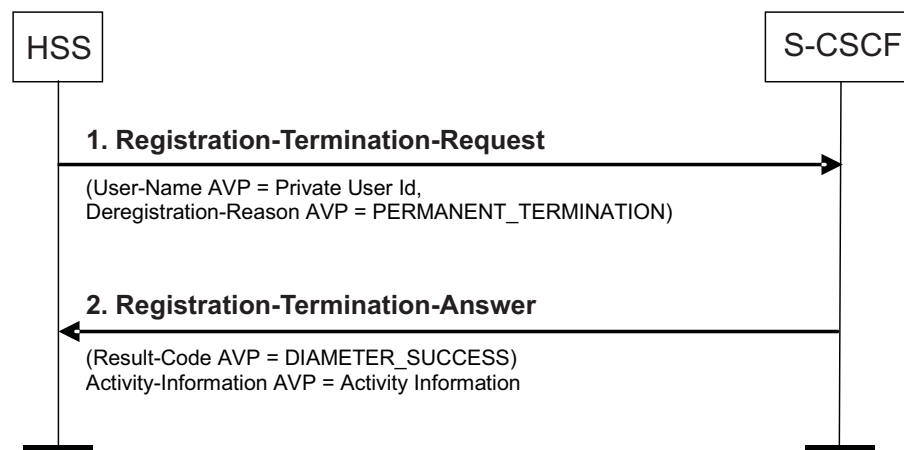


Figure 40 Successful Network Initiated Deregistration of User

The procedure is as follows:

- 1 The HSS sends an RTR to the S-CSCF to deregister a user. The HSS includes the username and the Deregistration-Reason AVP with Reason-Code PERMANENT_TERMINATION.
- 2 The S-CSCF removes all Public User Identities and Implicit Registration Sets tied to the Private User Identity and includes the Result-code DIAMETER_SUCCESS in the RTA.

3.6.1.2 Successful Network Initiated Deregistration of Public Identity or List of Public Identities

A successful network initiated deregistration of a public identity or a list of public identities is shown in Figure 41.

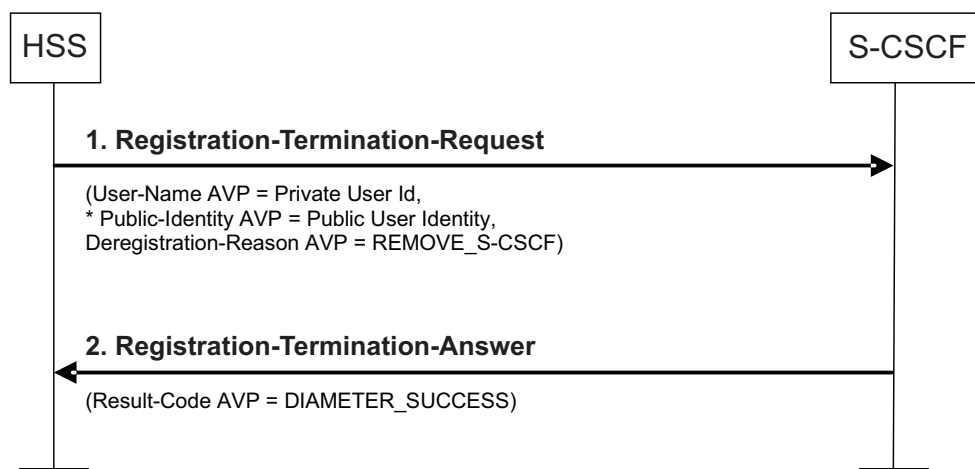


Figure 41 Successful Network Initiated Deregistration of Public Identity or List of Public Identities

The procedure is as follows:

- 1 The HSS sends an RTR to the S-CSCF to deregister a user. The HSS includes the username, one or several Public User Identities, and the Deregistration-Reason = REMOVE_S-CSCF.
- 2 The S-CSCF removes all implicit registrations sets that the Public User Identities belongs to in case they are not associated with other Private User Identities. The Private User Identity is removed in case no more Public User Identities or Implicit Registration Sets are tied to it. The S-CSCF includes the Result-Code DIAMETER_SUCCESS in the RTA.

3.6.1.3

Successful Network Initiated Deregistration – Public Identity Not Registered

A successful network initiated deregistration with public identity not registered is shown in Figure 42.

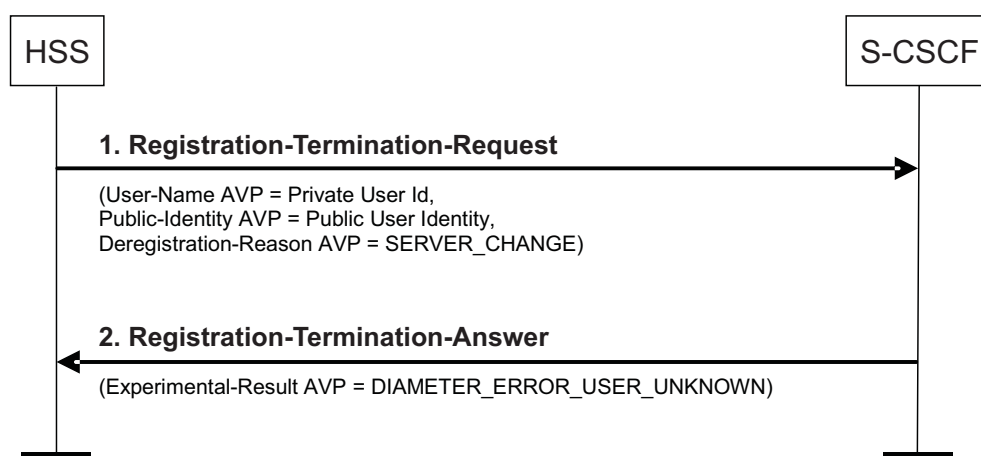


Figure 42 Successful Network Initiated Deregistration – Public Identity Not Registered

The procedure is as follows:

- 1 The HSS sends an RTR to the S-CSCF to deregister a user. The HSS includes the username, one Public User Identity, and the Deregistration-Reason = SERVER_CHANGE.
- 2 If the Public Identity is not registered, the S-CSCF responds with the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN in the RTA.

3.6.1.4

Unsuccessful Network Initiated Deregistration, Public Identity Only Emergency Registered

An unsuccessful network initiated deregistration with public identity emergency registered in the CSCF is shown in Figure 43.

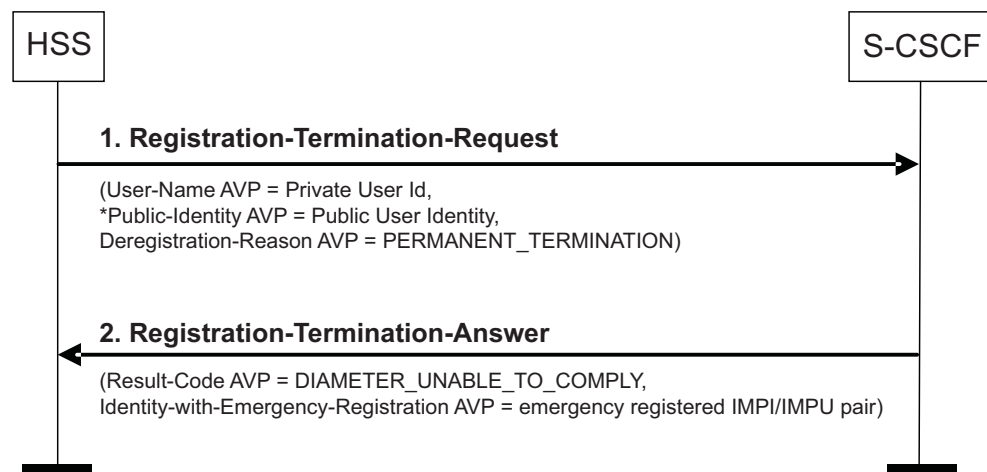


Figure 43 Unsuccessful Network Initiated Deregistration, Public Identity Only Emergency Registered

The procedure is as follows:



- 1 The HSS sends an RTR to the S-CSCF to deregister a user. The HSS includes the username, and optionally the Public User Identity and the Deregistration-Reason AVP with Reason-Code PERMANENT_TERMINATION.
- 2 If the Public Identity included in the RTR is emergency registered, the S-CSCF responds an RTA with Result-Code of DIAMETER_UNABLE_TO_COMPLY and a list of Private Identity/Public Identity pairs that are emergency registered, and have been requested to be deregistered by HSS through the RTR. One IMPI/IMPU pair is included in one Identity-with-Emergency-Registration AVP.

Alternatively, if the public identity is not included in the request, and all public identities tied to the private identity are emergency registered, the S-CSCF responds an RTA with a Result-Code of DIAMETER_UNABLE_TO_COMPLY and a list of Private Identity/Public Identity pairs that are emergency registered. One IMPI/IMPU pair is included in one Identity-with-Emergency-Registration AVP.

3.6.1.5

Limited Success of Network Initiated Deregistration, Public Identity Registered, and Emergency Registered

A network initiated deregistration with a subset of public identity emergency registered in the CSCF is shown in Figure 44.

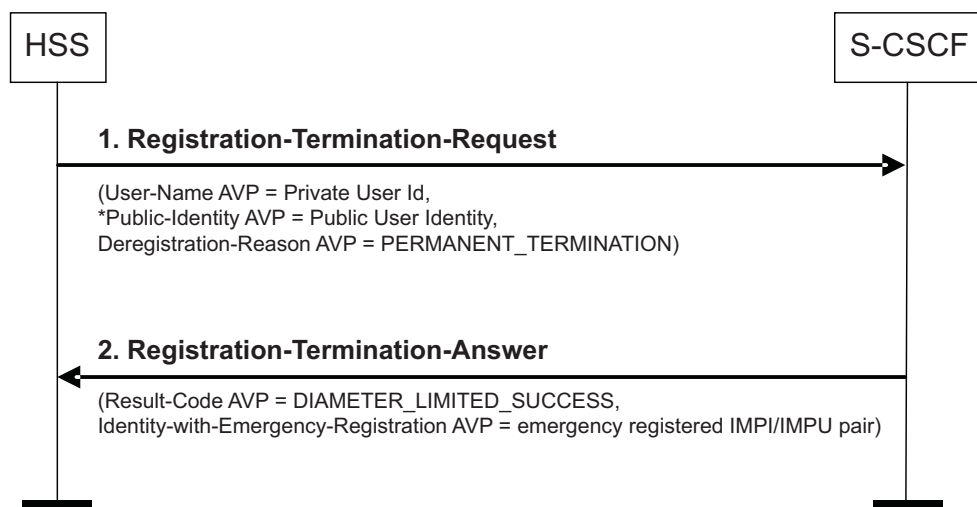


Figure 44 Limited Success of Network Initiated Deregistration, Public Identity Registered, and Emergency Registered

The procedure is as follows:

- 1 The HSS sends an RTR to the S-CSCF to deregister a user. The HSS includes the username, optionally the Public User Identity, and the Deregistration-Reason AVP with Reason-Code PERMANENT_TERMINATION.
- 2 If a proper subset of the registered Public Identities, which have been requested to be deregistered by the RTR, is emergency registered, the S-CSCF responds an RTA with a Result-Code of DIAMETER_LIMITED_SUCCESS, and a list of Private Identity/Public Identity pairs, that are emergency registered, and have been requested to be deregistered by HSS through RTR. One IMPI/IMPU pair is included in one Identity-with-Emergency-Registration AVP.

3.7 HSS Initiated User Profile Update

The following procedure is used by the HSS to the S-CSCF to update user profile information, Charging information, and digest authentication information, or all three:

- The HSS requests the S-CSCF to update the relevant user information through the Push-Profile-Request (PPR) command.

The PPR contains the user profile information, including updating server profiles for IMPUs, adding IMPUs, removing IMPUs, and changing barring states of IMPUs in an IRS, and Charging information.

- The S-CSCF checks the processor load. If the processor capacity cannot be granted, the S-CSCF returns the Result-Code DIAMETER_TOO_BUSY. Also other initial checks of the Diameter request are performed.

If the request requires support of the SiFC feature and this feature is disabled in the S-CSCF, the Experimental-Result-Code DIAMETER_ERROR_FEATURE_UNSUPPORTED is returned.

If an Alias Identity Group is received, the S-CSCF responds with Experimental-Result-Code DIAMETER_ERROR_FEATURE_UNSUPPORTED in the Push-Profile-Answer (PPA) to the HSS.

- The S-CSCF checks if the request contains an Implicit Registration Set, that there is no change of the default IMPU. That means that the first unbarred IMPU is not replaced, or removed, or has changed its barring state. If so, the Experimental-Result-Code DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA is returned.
- If the request contains a new Wildcarded Public User Identity (wIMPU) for an Implicit Registration Set that was not registered for any wIMPU, then the Experimental-Result-Code DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA is returned.
- The S-CSCF checks that the user has the state registered or unregistered in the CSCF. If not, then the Experimental-Result-Code DIAMETER_ERROR_USER_UNKNOWN is returned.



If the User-Data AVP includes an SiFC identity not defined in the S-CSCF, then the Experimental-Result-Code DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA is returned.

If the user is registered or unregistered and the User-Data AVP is present in the request, the S-CSCF replaces the current information with the information received from the HSS, for all the Public Identities that are indicated in the User profile that is included in the request.

If the Charging-Information AVP is present in the request, the S-CSCF replaces the existing Charging information with the information received from the HSS.

The SIP-Auth-Data-Item AVP is present if the command is sent to update SIP Digest Authentication information because of a password change.

- After successful update, the S-CSCF responds with a PPA with Result-Code DIAMETER_SUCCESS to the HSS.
- If the S-CSCF receives data that it cannot recognize, unsupported user data or more data than it can accept, it returns the corresponding error code in the Experimental-Result-Code AVP in the PPA to the HSS.

3.7.1 Use Cases – HSS Initiated User Profile Update

3.7.1.1 Successful HSS Initiated User Profile Update

A successful HSS initiated user profile update is shown in Figure 45.

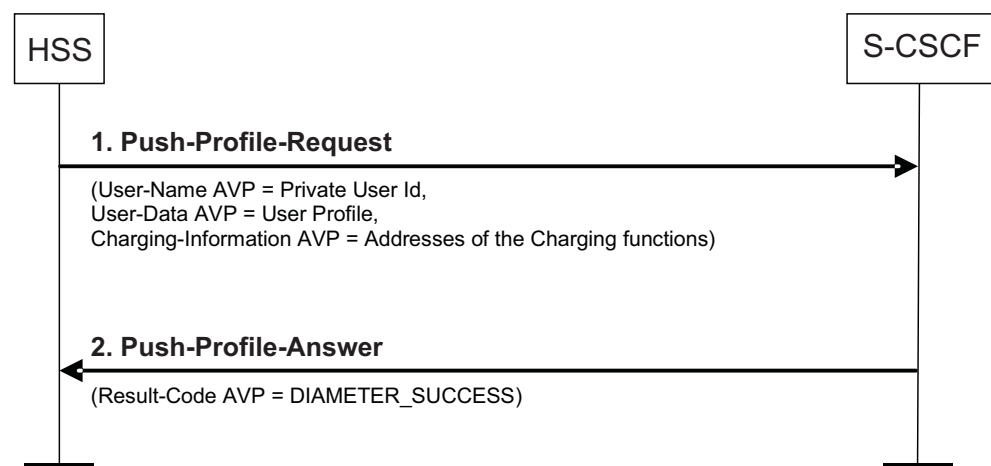


Figure 45 Successful HSS Initiated User Profile Update

The procedure is as follows:

- 1 The HSS sends a PPR to the S-CSCF to update the user service profile, including updating server profiles for IMPUs, adding IMPUs, removing IMPUs, and changing barring states of IMPUs in an IRS, Charging information.
- 2 The S-CSCF replaces the current information with the information received from the HSS. The S-CSCF includes the Result-Code DIAMETER_SUCCESS.

3.7.1.2 Unsuccessful HSS Initiated User Profile Update – Unsupported Data

An unsuccessful HSS initiated user profile update with unsupported data is shown in Figure 46.

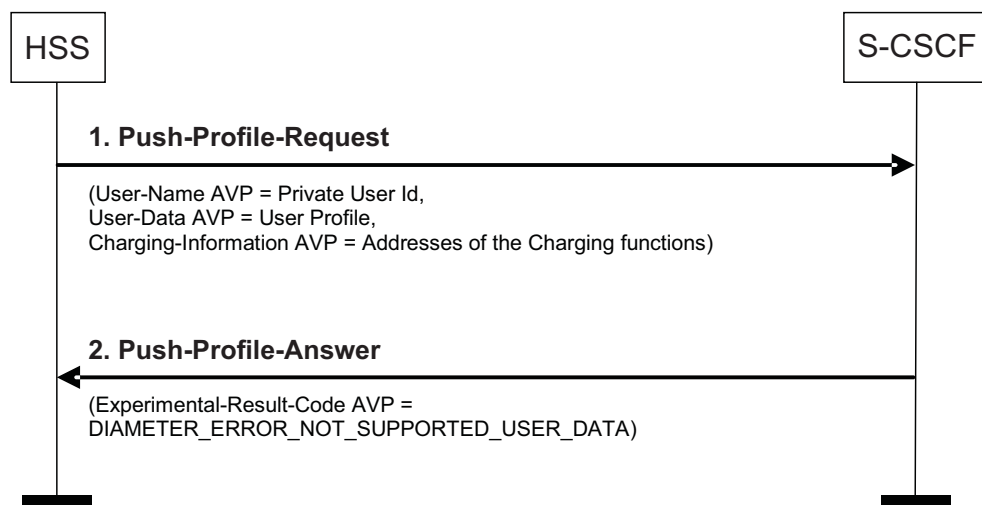


Figure 46 Unsuccessful HSS Initiated User Profile Update – Unsupported Data

The procedure is as follows:

- 1 The HSS sends a PPR to the S-CSCF to update the user profile. The request contains one, two or all of the following:
 - A change of the default IMPU: the IMPU has been removed, replaced, or has changed its barring state.
 - A wIMPU added to an Implicit Registration Set that has not previously been registered for any wIMPU.
 - A shared Initial Filter Criteria which is undefined in the S-CSCF.
- 2 The S-CSCF responds with the Experimental-Result-Code DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA in the PPA.

3.7.1.3 Unsuccessful HSS Initiated User Profile Update – Unsupported Feature

An unsuccessful HSS initiated user profile update with unsupported feature is shown in Figure 47.

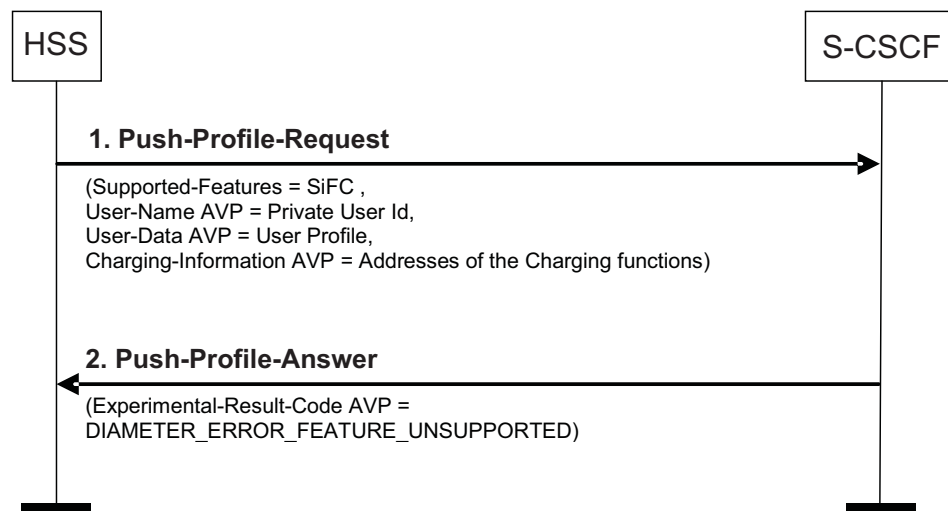


Figure 47 Unsuccessful HSS Initiated User Profile Update – Unsupported Feature

The procedure is as follows:

- 1 The HSS sends a PPR to the S-CSCF to update the user profile with a new user profile containing the Shared Initial Filter Criteria.
- 2 If the HSS requires support of the SiFC feature and this feature is disabled in the S-CSCF or if Alias Identity group is received, the S-CSCF responds with Experimental-Result-Code DIAMETER_ERROR_FEATURE_UNSUPPORTED in the Push-Profile-Answer to the HSS.

3.7.1.4

Successful HSS Initiated User Profile Update 2

A successful HSS initiated user profile update is shown in Figure 48.

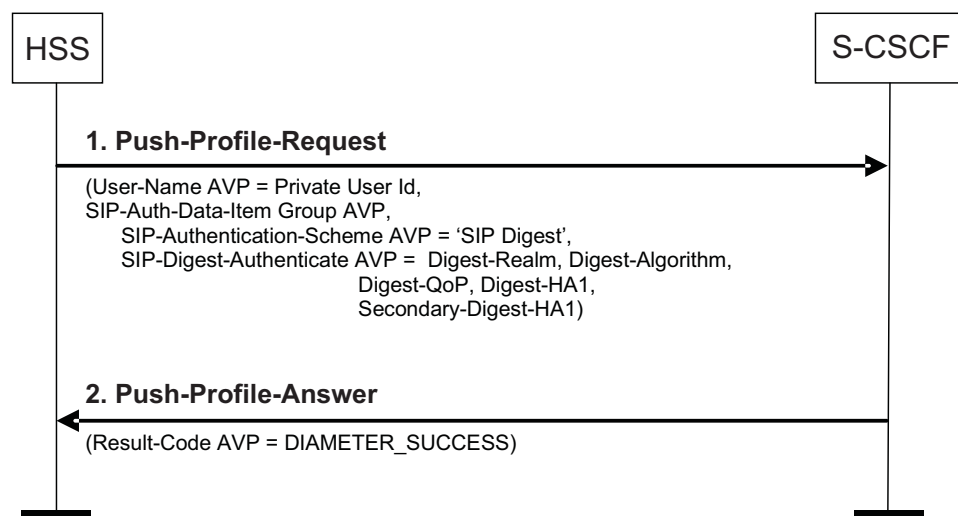


Figure 48 Successful HSS Initiated User Profile Update 2



The procedure is as follows:

- 1 The HSS sends a PPR to the S-CSCF if the used authentication scheme is SIP Digest and a password change has occurred in the HSS. The SIP-Auth-Data-Item grouped AVP includes the SIP-Digest-Authenticate grouped AVP. The Secondary-Digest-HA1 AVP can be included.
- 2 The S-CSCF updates the Digest Authentication data. If both the Digest-HA1 and the Secondary-Digest-HA1 are included, the S-CSCF determines which HA1 is applicable for the user based on the format of the digest username that the UE sent to the S-CSCF. The S-CSCF updates the applicable one and responds with Result-Code DIAMETER_SUCCESS in the PPA to the HSS.



4 Information Model

The command codes for the Cx/Dx interface application are taken from the range allocated by IANA®. For these commands, the Application-ID field is set to **16777216**, the application identifier of the Cx/Dx interface application, allocated by IANA.

The Command Codes are defined in Table 5.

Table 5 Command-Code Values

Command-Name	Abbreviation	Code	Direction
User-Authorization-Request	UAR	300	I-CSCF to HSS/SLF
User-Authorization-Answer	UAA	300	HSS/SLF to I-CSCF
Location-Info-Request	LIR	302	I-CSCF to HSS/SLF
Location-Info-Answer	LIA	302	HSS/SLF to I-CSCF
Server-Assignment-Request	SAR	301	S-CSCF to HSS/SLF
Server-Assignment-Answer	SAA	301	HSS/SLF to S-CSCF
Multimedia-Auth-Request	MAR	303	S-CSCF to HSS/SLF
Multimedia-Auth-Answer	MAA	303	HSS/SLF to S-CSCF
Registration-Termination-Request	RTR	304	HSS to S-CSCF
Registration-Termination-Answer	RTA	304	S-CSCF to HSS
Push-Profile-Request	PPR	305	HSS to S-CSCF
Push-Profile-Answer	PPA	305	S-CSCF to HSS

The presence of an information element, as defined in the P column, is defined as follows:

- **M** = Mandatory
- **C** = Conditional (Mandatory under certain circumstances)
- **O** = Optional

The following symbols are used in the Message Format:

- **< AVP >** indicates a mandatory AVP with a fixed position in the message.
- **{ AVP }** indicates a mandatory AVP in the message.
- **[AVP]** indicates an optional AVP in the message.
- *** AVP** indicates that multiple occurrences of an AVP are possible.



The symbols are according to the [RFC 3588 Diameter Base Protocol](#) specification.

4.1 Supported Diameter Cx/Dx Commands

4.1.1 UAR

The User-Authorization-Request (UAR) command, indicated by the Command-Code field set to **300** and the “R” bit set in the Command Flags field, is sent by the I-CSCF to the HSS to request the authorization of the registration of a user.

In the command, the I-CSCF includes the information elements shown in Table 6.

Table 6 UAR AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Auth-Session-State	M	Specifies whether the state is maintained for a particular session. The CSCF always sends NO_STATE_MAINTAINED.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Destination-Host	O	Present if the CSCF knows the address/name of the HSS for a certain user.
Destination-Realm	M	Contains the realm the message is to be routed to.
User-Name	M	Private User Identity.
Public-Identity	M	Public User Identity.
Visited-Network-Identifier	M	Identifier that allows the home network to identify the visited network.
User-Authorization-Type	M	Type of authorization requested by the I-CSCF.
Access-Network-Information	O	Present if the CSCF has received a PANI header.



Element	P	Description
Supported-Features	O	Informs the destination host about the features that the origin host supports. The I-CSCF supports restoration procedure; therefore the IMSRestorationInd bit is set.
UAR-Flags	O	Carries the following indication: - IMS Emergency Registration. The IMS Emergency Registration indication is set if the CSCF has received a sos parameter in the Contact header of the SIP REGISTER request.

The message format for Cx and Dx is as follows:

```
< User-Authorization-Request > ::=
    < Diameter Header: 300, REQ, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    { User-Name }
    { Public-Identity }
    { Visited-Network-Identifier }
    [ User-Authorization-Type ]
    [ Access-Network-Information ]
* [ Supported-Features ]
  [ UAR-Flags ]
```

4.1.2 User-Authorization-Answer

The User-Authorization-Answer (UAA) command, indicated by the Command-Code field set to **300** and the “R” bit cleared in the Command Flags field, is sent by an HSS in response to the User-Authorization-Request (UAR) command.

The HSS returns the parameters shown in Table 7.

Table 7 UAA AVPs, Cx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.



Element	P	Description
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Supported-Features	O	Informs the destination host about the features that the origin host supports. I-CSCF supports restoration procedure; therefore it accepts this AVP.
Server-Name	C	Contains the name of the assigned S-CSCF if the user is registered.
Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the IMS Subscription.
Failed-AVP	C	Provides debugging information in cases where a request is rejected.
3GPP-SGSN-MCC-MNC	O	Informs the destination host about roaming information.
GPRS-Roaming-Status	O	Informs the destination host if the user is attached to its home network or not.

The message format for Cx is as follows:



```

< User-Authorization-Answer > ::=
    < Diameter Header: 300, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    * [ Supported-Features ]
    [ Server-Name ]
    [ Server-Capabilities ]
    * [ Failed-AVP ]
    * [ AVP ]
    [ 3GPP-SGSN-MCC-MNC ]
    [ GPRS-Roaming-Status ]

```

Either the Server-Name AVP or the Server-Capabilities AVP can be present in the message, but not in both of them.

If both the Server-Name AVP and the Server-Capabilities AVP are not present, the I-CSCF can select any available S-CSCF.

The Result-Code AVP contains results defined in the Diameter Base Protocol and Experimental-Result AVP is used for Cx/Dx results. Only one of them must be present in the message.

The SLF returns the parameters shown in Table 8.

Table 8 UAA AVPs, Dx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.



Element	P	Description
Experimental-Result	C	<p>Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred.</p> <p>The Experimental-Result AVP must be present if the Result-Code AVP is not present.</p>
Auth-Session-State	M	<p>Specifies whether state is maintained for a particular session.</p>
Origin-Host	M	<p>Identifies the endpoint that originated the Diameter message.</p>
Origin-Realm	M	<p>Contains the Realm of the originator of the Diameter message.</p>
Redirect-Host	C	<p>Server name of the server selected by the service to handle the request.</p> <p>Must be present if the “E” bit of the answer message is set and the Result-Code is set to DIAMETER_REDIRECT_INDICATION.</p>
Redirect-Host-Usage	O	<p>Dictates how the routing entry resulting from the Redirect-Host is to be used.</p> <p>The Redirect-Host-Usage AVP is ignored by the CSCF. The CSCF does not cache the host received in the Redirect-Host AVP.</p>
Redirect-Max-Cache-Time	C	<p>Contains the maximum number of seconds that the peer and route table entries, created as a result of Redirect-Host, are cached.</p> <p>The Redirect-Max-Cache-Time AVP is ignored by the CSCF.</p>

The message format for Dx is as follows:



```

< User-Authorization-Answer > ::=
    < Diameter Header: 300, PXY, 16777216 >
< Session-Id >
{ Vendor-Specific-Application-Id }
[ Result-Code ]
[ Experimental-Result ]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[ Redirect-Host ]
[ Redirect-Host-Usage ]
[ Redirect-Max-Cache-Time ]

```

4.1.2.1 Successful Cases

The Result-Code AVP takes one of the values shown in Table 9.

Table 9 UAA Successful Result-Codes

Result-Code AVP	Successful Case
2001 DIAMETER_SUCCESS	The request was successfully completed for a deregistration scenario or a request for capabilities from the HSS.
3006 DIAMETER_REDIRECT_INDICATION	The operation was performed correctly. The server name to which the request must be routed is returned to the client. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.

The Experimental-Result AVP in successful cases takes one of the values shown in Table 10.

Table 10 UAA Successful Experimental-Result-Codes

Experimental-Result-Code AVP	Successful Case
2001 DIAMETER_FIRST_REGISTRATION	The user is authorized to register and there is no S-CSCF Location Data stored for the user.
2002 DIAMETER_SUBSEQUENT_REGISTRATION	The Public User Identity is registered and there is an S-CSCF Location Data stored for the user.

4.1.2.2 Error Cases

The Result-Code AVP takes one of the values shown in Table 11.



Table 11 UAA Unsuccessful Result-Codes

Result-Code AVP	Error Case
5003 DIAMETER_AUTHORIZATION_REJECTED	The Public Identity is barred, and does not belong to an Implicit Registration Set with at least one non-barred Public Identity.
DIAMETER_UNABLE_TO_COMPLY	The HSS cannot fulfill the received request, for example, because of a database error.
3003 DIAMETER_REALM_NOT_SERVED	The request failed because the user is not found in the Subscriptions database and the routing by realm is enabled, but the Diameter stack does not provide a purposed realm. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.

The Experimental-Result AVP in error cases takes one of the values shown in Table 12.

Table 12 UAA Unsuccessful Experimental-Result-Codes

Experimental-Result-Code AVP	Error Case
5001 DIAMETER_ERROR_USER_UNKNOWN	The received Public Identity or Private Identity is unknown.
5002 DIAMETER_ERROR_IDENTITYES_DONT_MATCH	The Private and Public Identities received in the request are not associated in the HSS.
5003 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED	Trying to deregister a not registered user.
5004 DIAMETER_ERROR_ROAMING_NOT_ALLOWED	The Public User Identity is not allowed to roam in the visited network.
5011 DIAMETER_ERROR_FEATURE_UNSUPPORTED	The feature is not supported by the CSCF.

4.1.3 Location-Info-Request

The LIR command, indicated by the Command-Code field set to **302** and the “R” bit set in the Command Flags field, is sent by the I-CSCF to the HSS to request the authorization of the registration of a user.



The I-CSCF includes the information elements in the command as shown in Table 13.

Table 13 LIR AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Auth-Session-State	M	Specifies whether state is maintained for a particular session. The CSCF always sends NO_STATE_MAINTAINED.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Destination-Host	O	Present if the CSCF knows the address/name of the HSS for a certain user.
Destination-Realm	M	Contains the realm the message is to be routed to.
Originating-Request	O	Indicates to the HSS that the request is related to an AS originating SIP request.
Public-Identity	M	Public User Identity.
Supported-Features	O	Informs the destination host about the features that the origin host supports. The I-CSCF supports restoration procedure; therefore the IMSRestorationInd bit is set.
User-Authorization-Type	O	A value of REGISTRATION_AND_CAPABILITIES is used in case of initial registration, reregistration, originating, or terminating SIP request and when the I-CSCF explicitly requests S-CSCF capability information from the HSS. The I-CSCF uses this value when the current S-CSCF of the user, which is stored in the HSS, cannot be contacted and a new S-CSCF must be selected.
Session-Priority	O	Indicates the priority of the session to the HSS. If it is not included, the request is treated as normal.

The message format for Cx and Dx is as follows:



```
< Location-Info-Request > ::=
    < Diameter Header: 302, REQ, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    { Originating-Request }
    { Public-Identity }
    [ User-Authorization-Type ]
    [ Session-Priority ]
    *[ Supported-Features ]
```

4.1.4 Location-Info-Answer

The LIA command, indicated by the Command-Code field set to 302 and the “R” bit cleared in the Command Flags field, is sent by an HSS in response to the LIR command.

The HSS returns the information elements in the command as shown in Table 14.

Table 14 LIA AVPs, Cx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.



Element	P	Description
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Supported-Features	O	<p>Informs the destination host about the features that the origin host supports.</p> <p>The I-CSCF supports the restoration procedure; therefore it accepts this AVP.</p>
Server-Name	C	Contains the name of the assigned S-CSCF if the user is registered.
Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the IMS Subscription.
Wildcarded-Public-Identity	C	If the request matches a wildcarded public identity, either a Wildcarded Public Service Identity (wPSI) or a Wildcarded Public User Identity (wIMPU), the HSS includes the corresponding wildcard public identity in this information element.
Failed-AVP	C	Provides debugging information in cases where a request is rejected.

The message format for Cx is as follows:

```

< Location-Info-Answer > ::=
    < Diameter Header: 302, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    * [ Supported-Features ]
    [ Server-Name ]
    [ Server-Capabilities ]
    [ Wildcarded-Public-Identity ]
    * [ Failed-AVP ]
    * [ AVP ]

```

Result-Code AVP contains results defined in the Diameter Base Protocol and Experimental-Result AVP is used for Cx/Dx results. Only one of them must be present in the message.

Either the Server-Name AVP or Server-Capabilities AVP can be present in the message, but not in both of them.



The Server-Capabilities AVP can be absent to indicate to the I-CSCF that it can select any available S-CSCF.

Note: According to 3GPP TS29.228 v8.8.0/v.9.3.0 or later releases, TS29.229 v8.9.0/v.9.3.0 or later releases, the Wildcarded-IMPU AVP (code 636) has been deprecated, to cope with a vendor who has implemented its Cx interface according to the old release before the previously stated releases, when the Wildcarded-IMPU AVP (code 636) is received from HSS in LIA message, it is processed by I-CSCF in the same way as if the Wildcarded-Public-Identity AVP (code 634) is received.

SLF returns the information elements in the command as shown in Table 15.

Table 15 LIA AVPs, Dx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Redirect-Host	C	Server name of the server selected by the service to handle the request. Must be returned if the E bit of the answer message is set and the Result-Code is set to DIAMETER_REDIRECT_INDICATION .



Element	P	Description
Redirect-Host-Usage	O	Dictates how the routing entry resulting from the Redirect-Host is to be used. The Redirect-Host-Usage AVP is ignored by the CSCF, the CSCF does not cache the host received in the Redirect-Host AVP.
Redirect-Max-Cache-Time	C	Contains the maximum number of seconds that the peer and route table entries, created as a result of Redirect-Host, are cached. The Redirect-Max-Cache-Time AVP is ignored by the CSCF.

The message format for Dx is as follows:

```
< Location-Info-Answer > ::=
    < Diameter Header: 302, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Max-Cache-Time ]
```

4.1.4.1

Successful Cases

The Result-Code AVP takes one of the values shown in Table 16.

Table 16 LIA Successful Result-Codes

Result-Code AVP	Successful Case
2001 DIAMETER_SUCCESS	The operation was performed correctly: the Public Identity or corresponding wildcarded public identity (wPSI or wIMPU) or the Distinct IMPU, is registered, by normal registration or because of services related to unregistered state, so there are location data stored for the user.
3006 DIAMETER_REDIRECT_INDICATION	The operation was performed correctly. The server name to which the request must be routed is returned to the client. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.



The Experimental-Result AVP in successful cases takes one of the values shown in Table 17.

Table 17 LIA Successful Experimental-Result-Codes

Experimental-Result-Code AVP	Successful Case
2003 DIAMETER_UNREGISTERED_SERV ICE	The Public Identity or corresponding is not registered but has services associated to unregistered state.

4.1.4.2

Error Cases

The Result-Code AVP takes one of the values shown in Table 18.

Table 18 LIA Unsuccessful Result-Codes

Result-Code AVP	Error Case
5012 DIAMETER_UNABLE_TO_COMPLY	The HSS cannot fulfill the received request, for example, because of a database error.
3003 DIAMETER_REALM_NOT_SERVED	The request failed because the user is not found in the Subscriptions database and the routing by realm is enabled but the Diameter stack does not provide a purposed realm. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.

The Experimental-Result AVP in error cases takes one of the values shown in Table 19.

Table 19 LIA Unsuccessful Experimental-Result-Codes

Experimental-Result-Code AVP	Error Case
5001 DIAMETER_ERROR_USER_UNKNO WN	Used when the Public or Private Identity of the user is unknown.
5003 DIAMETER_ERROR_IDENTITY_NO T_REGISTERED	The Public Identity is not registered and the Originating-Request AVP is not present and the Public Identity has no services associated to the unregistered state or, if having them, when the user or subscriber is barred for registration, or the Public Identity is barred for session establishment.



4.1.5 Server-Assignment-Request

The 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 S-CSCF to the HSS to request it to store or remove the name of the server that is serving the user and request download of the user profile.

The S-CSCF includes the information elements in the command as shown in Table 20.

Table 20 SAR AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Auth-Session-State	M	Specifies whether state is maintained for a particular session. The CSCF always sends NO_STATE_MAINTAINED.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Destination-Host	O	Present if the CSCF knows the address/name of the HSS for a certain user.
Destination-Realm	M	Contains the realm the message is to be routed to.
User-Name	C	Private User Identity. Is always to be present, if not unregistered public id. If deregistration and if no Public-Identity AVP is present, then the User-Name AVP is present.
Supported-Features	O	Informs the destination host about the features that the origin host supports. The S-CSCF supports the SiFC feature, the S-CSCF Restoration Procedure, and the P-CSCF Restoration Procedure. The S-CSCF includes this AVP when the related feature is enabled.



Element	P	Description
Public-Identity	C	Public User Identity. Only one Public Identity is present if the Server-Assignment-Type indicates REGISTRATION or UNREGISTERED_USER. If the Server-Assignment-Type indicates deregistration of some type and Private Identity is not present in the request at least one Public Identity is present.
Wildcarded-Public-Identity	O	If the request matches a wildcarded public identity, either a wPSI or a wIMPU, the S-CSCF includes the corresponding wildcarded public identity in this information element.
Server-Name	M	Name of the S-CSCF.
Server-Assignment-Type	M	Type of update that the S-CSCF requests in the HSS.
User-Data-Already-Available	M	Indicates if the user profile is already available in the S-CSCF.
Activity-Information	O	This grouped AVP contains one or more feature tags with corresponding time stamps when these features were used.
Multiple-Registration-Indication	O	Indicates to the HSS whether the request is related to a multiple registration. The S-CSCF sends it when SAT = Registration and when the restoration procedure is enabled. A value of MULTIPLE_REGISTRATION is used.
SCSCF-Restoration-Info	O	Contains the information required for an S-CSCF to reconstruct the user information so that request from a user can be handled. This AVP is used when restoration procedure is enabled. The S-CSCF stores and updates the restoration information with or without subscription information by sending this AVP to the HSS.
Session-Priority	O	Indicates priority of the session to the HSS. If it is not included, the request is treated as normal.
SAR-Flags	O	Indicates to the HSS that the P-CSCF Restoration Procedure is executed for the user.

The message format for Cx/Dx is as follows:



```

<Server-Assignment-Request > ::=
    < Diameter Header: 301, REQ, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    * [ Supported-Features ]
    [ User-Name ]
    * [ Public-Identity ]
    [ Wildcarded-Public-Identity ]
    { Server-Name }
    { Server-Assignment-Type }
    [ Multiple-Registration-Indication ]
    [ SCSCF-Restoration-Info ]
    [ Session-Priority ]
    { User-Data-Already-Available }
    * [ Activity-Information ]
    [ SAR-Flags ]

```

4.1.6 Server-Assignment-Answer

The SAA command, indicated by the Command-Code field set to **301** and the “R” bit cleared in the Command Flags field, is sent by an HSS in response to the SAR command.

The HSS returns the information elements in the command as shown in Table 21.

Table 21 SAA AVPs, Cx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type (authentication).
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.



Element	P	Description
Experimental-Result	C	<p>Indicates whether a particular vendor-specific request (Cx/Dx application) was completed successfully or whether an error occurred.</p> <p>The Experimental-Result AVP must be present if the Result-Code AVP is not present.</p>
Auth-Session-State	M	<p>Specifies whether state is maintained for a particular session.</p>
Origin-Host	M	<p>Identifies the endpoint that originated the Diameter message.</p>
Origin-Realm	M	<p>Contains the Realm of the originator of the Diameter message.</p>
User-Name	C	<p>Private User Identity. It is present in all successful responses.</p>
Supported-Features	O	<p>Informs the destination host about the features that the origin host supports.</p> <p>The S-CSCF supports and acts accordingly to the SiFC feature and the S-CSCF Restoration Procedure when enabled and ignores this AVP for any other feature.</p>
User-Data	C	<p>Contains the User profile.</p> <p>It is present when Server-Assignment-Type in the request is equal to REGISTRATION or UNREGISTERED_USER, and the User-Data-Already-Available is set to USER_DATA_NOT_AVAILABLE.</p> <p>It is also present when Server-Assignment-Type in the request is equal to REREGISTRATION or NO_ASSIGNMENT, and restoration is enabled, and the User-Data-Already-Available is set to USER_DATA_NOT_AVAILABLE.</p> <p>The HSS does not return any user profile data if User-Data-Already-Available is set to USER_DATA_ALREADY_AVAILABLE.</p>
Charging-Information	C	<p>Contains the addresses of the Charging functions. It is present when the User-Data AVP is sent to the S-CSCF.</p>



Element	P	Description
Associated-Identities	O	Contains the Private User Identities associated to an IMS subscription. Ignored by the CSCF.
Loose-Route-Indication	C	Indicates to the S-CSCF whether the loose route mechanism is required to serve the registered Public User Identities.
Failed-AVP	C	Provides debugging information in cases where a request is rejected.
SCSCF-Restoration-Info	O	Includes the information required for an S-CSCF to reconstruct the user information so that request from a user can be handled. This AVP is used when restoration procedure is enabled. The HSS sends this to the S-CSCF when restoration procedure is enabled.
Associated-Registered-Identities	C	Contains all Private Identities that are registered with the Public Identity received in the SAR command. The HSS sends this information element if the IMS Restoration Procedures are supported and the value of Server-Assignment-Type in the request is REGISTRATION or RE_REGISTRATION, and there are other Private Identities different from the Private Identity received in the SAR command being registered with the Public Identity received in the SAR command. Otherwise, this AVP is not present.

The message format for Cx is as follows:



```
< Server-Assignment-Answer > ::=
    < Diameter Header: 301, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    * [ Supported-Features ]
    [ User-Data ]
    [ Charging-Information ]
    [ Associated-Identities ]
    [ Loose-Route-Indication ]
    * [ Failed-AVP ]
    * [ SCSCF-Restoration-Info ]
    [ Associated-Registered-Identities ]
    * [ AVP ]
```

Result-Code AVP contains results defined in the Diameter Base Protocol and Experimental-Result AVP is used for Cx/Dx results. Only one of them must be present in the message.

The SLF returns the information elements in the command as shown in Table 22.

Table 22 SAA AVPs, Dx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.



Element	P	Description
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Redirect-Host	C	Server name of the server selected by the service to handle the request. Must be returned if the “E” bit of the answer message is set and the Result-Code is set to DIAMETER_REDIRECT_INDICATION.
Redirect-Host-Usage	O	Dictates how the routing entry resulting from the Redirect-Host is to be used. The Redirect-Host-Usage AVP is ignored by the CSCF, the CSCF does not cache the host received in the Redirect-Host AVP.
Redirect-Max-Cache-Time	C	Contains the maximum number of seconds that the peer and route table entries, created as a result of Redirect-Host, are cached. The Redirect-Max-Cache-Time AVP is ignored by the CSCF.

The message format for Dx is as follows:

```
< Server-Assignment-Answer > ::=
    < Diameter Header: 301, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Max-Cache-Time ]
```

4.1.6.1

Successful Cases

The Result-Code AVP takes one of the values shown in Table 23.



Table 23 SAA Successful Result-Codes

Result-Code AVP	Successful Case
2001 DIAMETER_SUCCESS	The operation was successfully performed.
3006 DIAMETER_REDIRECT_INDICATION	The operation was performed correctly. The server name to which the request must be routed is returned to the client. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.

The Experimental-Result AVP in successful cases takes one of the values shown in Table 24.

Table 24 SAA Successful Experimental-Result-Codes

Experimental-Result-Code AVP	Successful Case
2004 DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED	The S-CSCF can request the HSS to store the server name in some deregistration or registration expiry scenarios. If the HSS responds with this experimental result code, then the S-CSCF treats this as a successful case.

4.1.6.2

Error Cases

The Result-Code AVP takes one of the values shown in Table 25.

Table 25 SAA Unsuccessful Result-Codes

Result-Code AVP	Error Case
5009 DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	An AVP is displayed more often than permitted in the message definition.
5012 DIAMETER_UNABLE_TO_COMPLY	The HSS cannot fulfill the received request, for example, because of a database error.
3003 DIAMETER_REALM_NOT_SERVED	The request failed because the user is not found in the Subscriptions database and the routing by realm is enabled, but the Diameter stack does not provide a purposed realm. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.



The Experimental-Result AVP in error cases takes one of the values shown in Table 26.

Table 26 SAA Unsuccessful Experimental-Result-Codes

Experimental-Result-Code AVP	Error Case
5001 DIAMETER_ERROR_USER_UNKNOWN	The received Public Identity or Private Identity is unknown.
5002 DIAMETER_ERROR_IDENTITIES_DO_NOT_MATCH	The Public Identity does not correspond to the private identity.
5005 DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED	The Public Identity is already registered, but the S-CSCF name is different from the already stored in the HSS.
5007 DIAMETER_ERROR_IN_ASSIGNMENT_TYPE	Registration status of the identity in the HSS does not allow the received server assignment type in the request.
5011 DIAMETER_ERROR_FEATURE_UNSUPPORTED	The SiFC feature, S-CSCF Restoration Procedure, or P-CSCF Restoration Procedure not supported by the HSS.
5012 DIAMETER_ERROR_SERVING_NODE_FEATURE_UNSUPPORTED	The P-CSCF-Restoration-mechanism is supported by the HSS, but not by any user serving nodes, for example MME.

4.1.7

Multimedia-Auth-Request

The 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 S-CSCF to the HSS to request the security information.

The S-CSCF includes the information elements in the command as shown in Table 27.

Table 27 MAR AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Auth-Session-State	M	Specifies whether state is maintained for a particular session. The CSCF always sends NO_STATE_MAINTAINED.



Element	P	Description
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Destination-Host	O	Present if the CSCF knows the address/name of the HSS for a certain user.
Destination-Realm	M	Contains the realm the message is to be routed to.
User-Name	M	Private User Identity.
Public-Identity	M	Public User Identity.
SIP-Auth-Data-Item	M	Contains the authentication and authorization information, or both, for the Diameter client.
SIP-Number-Auth-Items	M	Indicates the number of authentication vectors the S-CSCF is requesting.
Server-Name	M	The name of the S-CSCF.

Authentication Data included in the SIP-Auth-Data-Item AVP sent in the request is shown in Table 28.

Table 28 SIP-Auth-Data-Item AVP

Element	P	Description
SIP-Authentication-Scheme	M	Authentication Scheme Digest-AKAv1-MD5 or NASS-Bundled or SIP Digest or Early-IMS-Security is supported.
SIP-Authentication-Context	C	Contains authentication-related information relevant for authentication. It is not present for Authentication Scheme Digest-AKAv1-MD5.

Authentication Data included in the SIP-Auth-Data-Item AVP sent in the request when Synchronization Failure is shown in Table 29.

Table 29 SIP-Auth-Data-Item AVP, Synchronization Failure

Element	P	Description
SIP-Authentication-Scheme	M	Authentication Scheme Digest-AKAv1-MD5.
SIP-Authorization	M	Contains the concatenation of RAND, as sent to the terminal, and AUTS as received from the terminal. RAND and AUTS are both to be binary encoded.



The message format for Cx/Dx is as follows:

```
< Multimedia-Auth-Request > ::=
    < Diameter Header: 303, REQ, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Destination-Host ]
    { Destination-Realm }
    { User-Name }
    { Public-Identity }
    { SIP-Auth-Data-Item }
    { SIP-Number-Auth-Items }
    { Server-Name }
```

4.1.8 Multimedia-Auth-Answer

The MAA command, indicated by the Command-Code field set to **303** and the “R” bit cleared in the Command Flags field, is sent by an HSS in response to the MAR command.

The HSS returns the information elements in the command as shown in Table 30.

Table 30 MAA AVPs, Cx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.

Element	P	Description
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
User-Name	C	Private User Identity. It must be present when the result is DIAMETER_SUCCESS.
Public Identity	C	Public User Identity. It must be present when the result is DIAMETER_SUCCESS.
SIP-Number-Auth-Items	C	Indicates the number of authentication vectors the S-CSCF is requesting. It must be present when the result is DIAMETER_SUCCESS.
SIP-Auth-Data-Item	C	Contains the authentication and authorization information, or both, for the Diameter client. If the SIP-Number-Auth-Items AVP is equal to 0 or it is not present, then this AVP is not present.
Supported-Features	O	Informs the destination host about the features that the origin host supports. The CSCF ignores this AVP.
Failed-AVP	C	Provides debugging information in cases where a request is rejected.

Authentication Data included in the SIP-Auth-Data-Item AVP received in the response for AKA Authentication is shown in Table 31.

Table 31 SIP-Auth-Data-Item AVP in Response for AKA Authentication

Element	P	Description
SIP-Item-Number	C	Contains the Item number and is present when multiple occurrences of SIPAuth-Data-Item AVPs exist, and the order in which they are processed is significant.
SIP-Authentication-Scheme	M	Authentication Scheme Digest-AKAv1-MD5.
SIP-Authenticate	M	Contains the concatenation of the authentication challenge RAND and the token AUTN, binary encoded.



Element	P	Description
SIP-Authorization	M	Contains the expected response XRES, binary encoded.
Confidentiality-Key	O	Contains the confidentiality key, binary encoded.
Integrity-Key	M	Contains the integrity key, binary encoded.

Authentication Data included in the SIP-Auth-Data-Item AVP received in the response for NASS Bundled Authentication is shown in Table 32.

Table 32 SIP-Auth-Data-Item AVP in Response for NASS-Bundle Authentication

Element	P	Description
SIP-Authentication-Scheme	M	Authentication Scheme NASS-Bundled.
Line-Identifier	M	Contains one of the following: <ul style="list-style-type: none"> • The fixed broadband access line identifier associated to the user. Can be repeated. • String equal to Line_Profile. Is not repeated.

Authentication Data included in the SIP-Auth-Data-Item AVP received in the response for SIP Digest Authentication is shown in Table 33.

Table 33 SIP-Auth-Data-Item AVP in Response for SIP Digest Authentication

Element	P	Description
SIP-Authentication-Scheme	M	Authentication Scheme SIP Digest.
SIP-Digest-Authenticate	M	Contains the grouped AVP for SIP digest authentication. See Table 35 for contents of this AVP.

Authentication Data included in the SIP-Auth-Data-Item AVP received in the response for GIBA is shown in Table 34.

Table 34 SIP-Auth-Data-Item AVP in Response to GIBA Authentication

Element	P	Description
SIP-Authentication-Scheme	M	Authentication Scheme Early-IMS-Security.
Framed-IP-Address	M	IPv4 address of the user.

SIP-Digest-Authenticate content is shown in Table 35.



Table 35 SIP-Digest-Authenticate AVP

Element	P	Description
Digest-Realm	M	Corresponds to the realm parameter as defined in RFC 2617 .
Digest-Algorithm	O	Contains the algorithm as defined in RFC 2617 . If this information element is not present, then MD5 is assumed. If this information element is present, it contains MD5.
Digest-QoP	M	Contains the Quality of Protection (QoP) as defined in RFC 2617 . Set to a value of “auth” by the HSS.
Digest-HA1	M	Contains the H(A1) as defined in RFC 2617 . It holds the digested value of username, the authentication realm, and the user password. The username can be with or without a realm.
Ericsson-Secondary-Digest-HA1	O	Holds the digested value of the username without its realm part, the authentication realm, and the user password.

The message format for Cx is as follows:

```
< Multimedia-Auth-Answer > ::=
    < Diameter Header: 303, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ User-Name ]
    [ Public-Identity ]
    [ SIP-Number-Auth-Items ]
    * [ SIP-Auth-Data-Item ]
    * [ Supported-Features ]
    * [ Failed-AVP ]
    * [ AVP ]
```

Result-Code AVP contains results defined in the Diameter Base Protocol and Experimental-Result AVP is used for Cx/Dx results. Only one of them must be present in the message.

The SLF returns the information elements in the command as shown in Table 36.



Table 36 MAA AVPs, Dx

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Redirect-Host	C	Server name of the server selected by the service to handle the request. Must be returned if the “E” bit of the answer message is set and the Result-Code is set to DIAMETER_REDIRECT_INDICATION .
Redirect-Host-Usage	O	Dictates how the routing entry resulting from the Redirect-Host is to be used. The Redirect-Host-Usage AVP is ignored by the CSCF. The CSCF does not cache the host received in the Redirect-Host AVP.
Redirect-Max-Cache-Time	C	Contains the maximum number of seconds that the peer and route table entries, created as a result of Redirect-Host, are cached. The Redirect-Max-Cache-Time AVP is ignored by the CSCF.

The message format for Dx is as follows:



```
< Multimedia-Auth-Answer > ::=
    < Diameter Header: 303, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    [ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Max-Cache-Time ]
```

4.1.8.1 Successful Cases

The Result-Code AVP takes one of the values shown in Table 37.

Table 37 MAA Successful Result-Codes

Result-Code AVP	Successful Case
2001 DIAMETER_SUCCESS	The operation was successfully performed.
3006 DIAMETER_REDIRECT_INDICATION	The operation was performed correctly. The server name to which the request must be routed is returned to the client. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.

4.1.8.2 Error Cases

The Result-Code AVP takes one of the values shown in Table 38.

Table 38 MAA Unsuccessful Result-Codes

Result-Code AVP	Error Case
5012 DIAMETER_UNABLE_TO_COMPLY	The HSS cannot fulfill the received request, for example, because of a database error.
3003 DIAMETER_REALM_NOT_SERVED	The request failed because the user is not found in the Subscriptions database and the routing by realm is enabled, but the Diameter stack does not provide a purposed realm. (1)

(1) The SLF replies the corresponding answer message with the “E” bit set.



The Experimental-Result AVP in error cases takes one of the values shown in Table 39.

Table 39 MAA Unsuccessful Experimental-Result-Codes

Experimental-Result-Code AVP	Error Case
5001 DIAMETER_ERROR_USER_UNKNOWN	The received Public Identity or Private Identity is unknown.
5002 DIAMETER_ERROR_IDENTITIES_DO_NOT_MATCH	The Public Identity does not correspond to the Private Identity.
5005 DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED	The authentication scheme indicated in the authentication request is not supported.

4.1.9

Registration-Termination-Request

The RTR command, indicated by the Command-Code field set to **304** and the “R” bit set in the Command Flags field, is sent by the HSS to the S-CSCF to request network initiated deregistration.

The HSS includes the information elements in the command as shown in Table 40.

Table 40 RTR AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Destination-Host	M	Contains the endpoint the message is to be routed to.
Destination-Realm	M	Contains the realm the message is to be routed to.



Element	P	Description
User-Name	M	Private User Identity. It is present if the deregistration Reason Code is NEW_SERVER_ASSIGNED. It can be present with other reason codes.
Public-Identity	C	Public User Identity. It must be present if the deregistration Reason Code is NEW_SERVER_ASSIGNED. It can be present with other reason codes. If deregistrating an IRS including a wIMPU, it can contain one or more Distinct IMPUs from the IRS.
Deregistration-Reason	M	The HSS sends a reason for deregistration to the client. The possible deregistration reasons are as follows: <ul style="list-style-type: none">• PERMANENT_TERMINATION• NEW_SERVER_ASSIGNED• SERVER_CHANGE• REMOVE_S-CSCF
Associated-Identities	O	Contains the Private User Identities associated to an IMS subscription. Ignored by the CSCF.
Supported-Features	O	Informs the destination host about the features that the origin host supports. The CSCF does not support any extended features in RTR command. If the “M” bit is set for the supported feature, the CSCF answers with Experimental-Result-Code DIAMETER_ERROR_FEATURE_UNSUPPORTED. Otherwise, the CSCF accepts the command.
Proxy-Info	O	Contains the identity of the host that added this AVP and the state local information.
Route-Record	O	The identity received in the Origin-Host AVP in the Capability-Exchange-Request. This AVP is ignored by the CSCF.



Deregistration reason includes the Reason Code AVP that can have the following values:

— PERMANENT_TERMINATION:

The IMS subscription or service profiles has been permanently terminated. It is used when a user or a Public Identity is deleted.

— NEW_SERVER_ASSIGNED:

A new S-CSCF has been allocated to the user, replacing the previously assigned S-CSCF. This deregistration reason is sent for the Public Identity in the SAR where the new S-CSCF name is received and for the Public User Identities belonging to the same Implicit Registration Set.

— SERVER_CHANGE:

It is indicated for the rest of Public User Identities of a user for which a new S-CSCF has been assigned. It is also used when the user or service S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for an updated User Profile upon execution PPR.

— REMOVE_S-CSCF:

The HSS indicates to the S-CSCF that the S-CSCF is no longer to be used for a given user. It is used in cases of operator initiated user/Public Identity deregistration, when a user or subscriber is barred for registration, when a Public Identity that does not belong to an Implicit Registration Set is barred and when a user is locked because of several authentication failures.

All the Public Identities in an RTR command must belong to the same private identity.

If deregistration of a registered/unregistered Public Identity in an Implicit Registration Set, one or several Public User Identities in the Implicit Registration Set are included in the message.

The message format is as follows:



```
< Registration-Termination-Request> ::=
    < Diameter Header: 304, REQ, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Host }
    { Destination-Realm }
    { User-Name }
    * [ Public-Identity ]
    { Deregistration-Reason }
    [ Associated-Identities ]
    * [ Supported-Features ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ AVP ]
```

4.1.10 Registration-Termination-Answer

The 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 S-CSCF in response to the RTR command.

The S-CSCF returns the information elements in the command as shown in Table 41.

Table 41 RTA AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.



Element	P	Description
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Failed-AVP	C	Provides debugging information in cases where a request is rejected.
Identity-with-Emergency-Registration	C	Indicates a list of pairs of Private and Public User Identities which have not been deregistered because of emergency registration.
Activity-Information	O	This grouped AVP contains one or more feature tags with corresponding time stamps when these features were used.

The message format is as follows:

```
< Registration-Termination-Answer > ::=
    < Diameter Header: 304, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    * [ Failed-AVP ]
    * [ Identity-with-Emergency-Registration ]
    * [ Activity-Information ]
```

Result-Code AVP contains results defined in the Diameter Base Protocol and Experimental-Result AVP is used for Cx/Dx results. Only one of them must be present in the message.

If the Associated-Identities AVP is received, the S-CSCF ignores the AVP and it is not returned in the RTA.



4.1.10.1 Successful Cases

The Result-Code AVP takes one of the values shown in Table 42.

Table 42 RTA Successful Result-Codes

Result-Code AVP	Successful Case
2001 DIAMETER_SUCCESS	The operation was performed correctly: the user or specified Public Identities are deregistered by the S-CSCF.
2002 DIAMETER_LIMITED_SUCCESS	The identities were partially deregistered. The Identity-with-Emergency-Registration AVP includes the list of Private/Public Identity pairs that have been requested to be deregistered by the HSS through RTR, but remain emergency registered in the S-CSCF.

4.1.10.2 Error Cases

The Result-Code AVP in error cases takes one of the values shown in Table 43.

Table 43 RTA Unsuccessful Result-Codes

Result-Code AVP	Error Case
3004 DIAMETER_TOO_BUSY	The CSCF system is overloaded.
5012 DIAMETER_UNABLE_TO_COMPLY	<p>The request failed.</p> <p>The reason for the failure can indicate that all identities to be deregistered where emergency registered in the S-CSCF and none of the identities have been deregistered.</p> <p>The Identity-with-Emergency-Registration AVP includes the list of Private/Public Identity pairs that have been requested to be deregistered by the HSS through RTR, but remain emergency registered in the S-CSCF.</p>

The Experimental-Result AVP in error cases takes one of the values shown in Table 44.



Table 44 RTA Unsuccessful Experimental-Result-Codes

Experimental-Result-Code AVP	Error Case
5001 DIAMETER_ERROR_USER_UNKNOW	The received Public Identity or Private Identity is unknown.
5011 DIAMETER_ERROR_FEATURE_UNSUPPORTED	The feature is not supported by the CSCF.

4.1.11

Push-Profile-Request

The 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 S-CSCF to request update of the user profile, or to inform S-CSCF that all GIBA information in the HSS has become invalid.

The HSS includes the information elements in the command as shown in Table 45.

Table 45 PPR AVP

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Destination-Host	M	Contains the endpoint the message is to be routed to.
Destination-Realm	M	Contains the realm the message is to be routed to.
User-Name	M	Private User Identity, or a private string, see Table 48.
User-Data	C	Contains the User data required to give service to a user. It is present if the user profile is changed in the HSS. If the User-Data AVP is not present, the SIP-Auth-Data-Item or the Charging-Information AVP is present.



Element	P	Description
Charging-Information	C	Contains the addresses of the Charging functions. It is present if the Charging addresses are changed in the HSS. If the Charging-Information AVP is not present, the SIP-Auth-Data-Item or the User-Data AVP is present.
SIP-Auth-Data-Item	C	<p>Present if the following apply:</p> <ul style="list-style-type: none">• The used authentication scheme is SIP Digest and the password change has occurred in the HSS. See Table 46.• The used authentication scheme is “Early-IMSSecurity”, User-Name is @ALL, and all GIBA information in HSS has become invalid. See Table 47. <p>If the SIP-Auth-Data-Item AVP is not present, the Charging-Information or User-Data AVP is present.</p>
Supported-Features	O	<p>Notifies the destination host about the features that the origin host supports.</p> <p>The CSCF supports only the SiFC feature. Any other extended feature is answered with Experimental-Result-Code DIAMETER_ERROR_FEATURE_UNSUPPORTED if the “M” bit is set.</p>
Proxy-Info	O	Contains the identity of the host that added this AVP and the state local information.
Route-Record	O	The identity received in the Origin-Host AVP in the Capability-Exchange-Request. This AVP is ignored by the CSCF.

SIP-Auth-Data-Item AVP for Digest Authentication is shown in Table 46.

Table 46 SIP-Auth-Data-Item for SIP Digest Authentication

Element	P	Description
SIP-Authentication-Scheme	M	Indicates the authentication scheme. It contains SIP Digest.
SIP-Digest-Authenticate	M	Contains the grouped AVP for SIP digest authentication. See Table 35 for contents of this AVP.

SIP-Auth-Data-Item for GIBA is shown in Table 47.



Table 47 SIP-Auth-Data-Item for GPRS IMS Bundled Authentication

Element	P	Description
SIP-Authentication-Scheme	M	Indicates the authentication scheme. It contains Early-IMS-Authentication.
SSO-Status	M	Contains the GIBA Status. See Table 34 for contents of this AVP.

User-Name AVP for GPRS IMS Bundled Authentication is shown in Table 48.

Table 48 User-Name AVP for GPRS IMS Bundled Authentication

Element	P	Description
User-Name	M	Contains @ALL, see Section 5.1.20 User-Name on page 108.

The message format is as follows:

```
< Push-Profile-Request> ::=
    < Diameter Header: 305, REQ, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    { Destination-Host }
    { Destination-Realm }
    { User-Name }
    [ User-Data ]
    [ Charging-Information ]
    [ SIP-Auth-Data-Item]
* [ Supported-Features ]
* [ Proxy-Info ]
* [ Route-Record ]
* [ AVP ]
```

4.1.12

Push-Profile-Answer

The 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 S-CSCF in response to the PPR command.

The S-CSCF returns the information elements in the command as shown in Table 41.



Table 49 PPA AVPs

Element	P	Description
Session-Id	M	Identifies the session between the CSCF and the HSS.
Vendor-Specific-Application-Id	M	Indicates the vendor, 3GPP, owning the application and the application type, authentication.
Result-Code	C	Indicates whether the request was completed successfully or whether an error occurred. The Result-Code AVP must be present if the Experimental-Result AVP is not present.
Experimental-Result	C	Indicates whether a particular vendor-specific request, Cx/Dx application, was completed successfully or whether an error occurred. The Experimental-Result AVP must be present if the Result-Code AVP is not present.
Auth-Session-State	M	Specifies whether state is maintained for a particular session.
Origin-Host	M	Identifies the endpoint that originated the Diameter message.
Origin-Realm	M	Contains the Realm of the originator of the Diameter message.
Failed-AVP	O	Provides debugging information in cases where a request is rejected.
Supported-Features	O	Informs the destination host about the features that the origin host supports. The CSCF supports only the SiFC feature in PPR and PPA commands. It includes this AVP when the SiFC feature is enabled.

The message format is as follows:



```

< Push-Profile-Answer > ::=
    < Diameter Header: 305, PXY, 16777216 >
    < Session-Id >
    { Vendor-Specific-Application-Id }
    [ Result-Code ]
    [ Experimental-Result ]
    { Auth-Session-State }
    { Origin-Host }
    { Origin-Realm }
    * [ Supported-Features ]
    * [ Failed-AVP ]

```

The Result-Code AVP contains results defined in the Diameter Base Protocol and Experimental-Result AVP is used for Cx/Dx results. Only one of them must be present in the message.

4.1.12.1 Successful Cases

The Result-Code AVP takes one of the values shown in Table 50.

Table 50 PPA Successful Result-Codes

Result-Code AVP	Successful Case
2001 DIAMETER_SUCCESS	The operation was performed correctly: the user profile is successfully updated.

4.1.12.2 Error Cases

The Result-Code AVP in error cases takes one of the values shown in Table 43.

Table 51 RTA Unsuccessful Result-Codes

Result-Code AVP	Error Case
3004 DIAMETER_TOO_BUSY	The CSCF system is overloaded.
5012 DIAMETER_UNABLE_TO_COMPLY	The request failed.

The Experimental-Result AVP in error cases takes one of the values shown in Table 52.

Table 52 PPA Unsuccessful Experimental-Result-Codes

Experimental-Result-Code AVP	Error Case
5001 DIAMETER_ERROR_USER_UNKNOW WN	The received Public Identity or Private Identity is unknown.



Experimental-Result-Code AVP	Error Case
5008 DIAMETER_ERROR_TOO_MUCH_DATA	The S-CSCF does not have enough memory to store the received data.
5009 DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	The received subscription data contained information, which was not recognized or supported by the S-CSCF.
5011 DIAMETER_ERROR_FEATURE_UNSUPPORTED	The feature is not supported by the CSCF.



5 Formal Syntax

5.1 Diameter Base AVPs

The Diameter Base Protocol AVPs, their AVP Code values, and types are described in tables. The Vendor-ID header is not to be included for these AVPs. These are defined in the [RFC 3588 Diameter Base Protocol](#) and [RFC 5090 RADIUS Extension for Digest Authentication](#) specifications.

A summary of the attributes is listed in Table 53.

Table 53 Diameter Base Protocol AVPs

AVP	AVP Code	Value Type
Auth-Application-Id	258	Unsigned32
Auth-Session-State	277	Enumerated
Destination-Host	293	Diameter Identity
Destination-Realm	283	Diameter Identity
Digest-Algorithm	111	UTF8String
Digest-HA1	121	UTF8String
Digest-QoP	110	UTF8String
Digest-Realm	104	UTF8String
Event-Timestamp	55	Time
Experimental-Result	297	Grouped
Experimental-Result-Code	298	Unsigned32
Origin-Host	264	Diameter Identity
Origin-Realm	296	Diameter Identity
Redirect-Host	292	DiameterURI
Redirect-Host-Usage	261	Enumerated
Redirect-Max-Cache-Time	262	Unsigned32
Result-Code	268	Unsigned32
Session-Id	263	UTF8String
User-Name	1	UTF8String
Vendor-Id	266	Unsigned32
Vendor-Specific-Application-Id	260	Grouped
Framed-IP-Address	8	OctetString



5.1.1 Auth-Application-Id

The Auth-Application-Id AVP attribute, as shown in Table 54, is used to advertise support of the Authentication and Authorization portion of an application.

The Diameter application identifier assigned by IANA to the Cx/Dx interface application is 16777216.

Table 54 Auth-Application-Id

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	258	12	Unsigned32

5.1.2 Auth-Session-State

The Auth-Session-State AVP attribute, as shown in Table 55, indicates whether state is maintained for a particular session.

The value is set to NO_STATE_MAINTAINED (1) to indicate that the CSCF does not maintain any state information about this session and that the CSCF does not send any Session-Termination-Request.

Table 55 Auth-Session-State

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	277	12	Enumerated

5.1.3 Destination-Host

The Destination-Host AVP attribute, as shown in Table 56, is present when the CSCF knows the address/name of the HSS for a certain user.

Example:

neighbour1.remote.example.com

Table 56 Destination-Host

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	293	> 8	Diameter Identity

5.1.4 Destination-Realm

The Destination-Realm AVP attribute, as shown in Table 57, contains the realm the message is to be routed to.

**Example:**

```
remote.example.com
```

Table 57 Destination-Realm

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	283	> 8	Diameter Identity

5.1.5**Digest-Algorithm**

The Digest-Algorithm AVP attribute, as shown in Table 58, holds the algorithm parameter that influences the HTTP Digest calculation. If the information element is missing, the value MD5 is assumed. Also if any value other MD5 is specified, the value is ignored and MD5 is used.

The Digest-Algorithm AVP is defined in the [RFC 4740 Diameter Session Initiation Protocol \(SIP\) Application](#) and [RFC 5090 RADIUS Extension for Digest Authentication \(Feb 2008\)](#) specifications.

Table 58 Digest-Algorithm

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	111	> 12	UTF8String

5.1.6**Digest-HA1**

The Digest-HA1 AVP attribute, as shown in Table 59, holds the digested value of the username, authentication realm, and user password.

The Digest-HA1 AVP is defined in the [RFC 4740 Diameter Session Initiation Protocol \(SIP\) Application](#) and [RFC 5090 RADIUS Extension for Digest Authentication \(Feb 2008\)](#) specifications.

Table 59 Digest-HA1

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	121	> 12	UTF8String

5.1.7**Digest-QoP**

The Digest-QoP AVP attribute, as shown in Table 60, holds the Quality of Protection parameter that influences the HTTP Digest calculation. The value of “auth” is always assumed.



The Digest-QoP AVP is defined in the [RFC 4740 Diameter Session Initiation Protocol \(SIP\) Application](#) and [RFC 5090 RADIUS Extension for Digest Authentication \(Feb 2008\)](#) specifications.

Table 60 Digest-QoP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	110	> 12	UTF8String

5.1.8

Digest-Realm

The Digest-Realm AVP, as shown in Table 61, contains a string to be displayed to users so they know which username and password to use. This string contains at least the name of the authenticating host.

Example:

“Welcome to the ims.XYZ.net network,
please insert your username and password”

The Digest-Realm AVP is defined in the following [RFC 4740 Diameter Session Initiation Protocol \(SIP\) Application](#) and [RFC 5090 RADIUS Extension for Digest Authentication \(Feb 2008\)](#) specifications.

Table 61 Digest-Realm

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	104	> 12	UTF8String

5.1.9

Event-Timestamp

The Event-Timestamp AVP attribute, as shown in Table 62, is of type Time and contains the time at which the reported event occurred. The Time format is derived from the OctetString AVP Base Format. The string must contain four octets, in the same format as the first 4 bytes are in the NTP time stamp format. This represents the number of seconds since 0h on 1 January 1900 regarding the Coordinated Universal Time (UTC).

Example corresponding to 2010-04-20 15.00.00: 3480850800

The Event-Timestamp AVP and the NTP time stamp are defined in the [RFC3588 Diameter Base Protocol \(Sept 2003\)](#) and [Section 3 in RFC 2030 Simple Network Time Protocol](#) specifications.

Table 62 Event-Timestamp

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	55	12	Time

5.1.10 Experimental-Result

The `Experimental-Result` AVP attribute, as shown in Table 63, is used to indicate whether a particular vendor-specific request (Cx/Dx application) is completed successfully or whether an error occurs.

AVP Format:

```
Experimental-Result ::= < AVP Header: 297 >
{ Vendor-Id }
{ Experimental-Result-Code }
```

Table 63 Experimental-Result

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	297	32	Grouped

5.1.11 Experimental-Result-Code

The `Experimental-Result-Code` AVP attribute, as shown in Table 64, contains a vendor-assigned value representing the result of processing the request.

Table 64 Experimental-Result-Code

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	298	12	Unsigned32

The 3GPP Cx/Dx Application result code values that must be supported are shown in Table 65.

Result codes that fall within the Success category are used to inform a peer that a request has been successfully completed.

Table 65 Successful Result Codes

Successful Result Code	Description
DIAMETER_FIRST_REGISTRATION (2001)	<p>The HSS informs the I-CSCF of the following:</p> <ul style="list-style-type: none"> The user is authorized to register this Public Identity An S-CSCF must be assigned to the user



Successful Result Code	Description
DIAMETER_SUBSEQUENT_REGISTRATION (2002)	The HSS informs the I-CSCF of the following: <ul style="list-style-type: none">• The user is authorized to register this Public Identity• An S-CSCF is already assigned and there is no need to select a new one
DIAMETER_UNREGISTERED_SERVICE (2003)	The HSS informs the I-CSCF of the following: <ul style="list-style-type: none">• The Public Identity is not registered but has services related to unregistered state• An S-CSCF must be assigned to the user
DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED (2004)	The HSS informs the S-CSCF of the following: <ul style="list-style-type: none">• The deregistration is completed• The S-CSCF name is not stored in the HSS

Errors that fall within the Permanent Failure category, as shown in Table 66, are used to inform the peer that the request failed, and must not be attempted again.

Table 66 Unsuccessful Result Codes

Unsuccessful Result Code	Description
DIAMETER_ERROR_USER_UNKNOWN (5001)	A message was received for a user that is unknown.
DIAMETER_ERROR_IDENTITYES_DONT_MATCH (5002)	A message was received with a Public Identity and a private identity, and the server determines that the Public Identity does not correspond to the private identity.
DIAMETER_ERROR_IDENTITY_NOT_REGISTERED (5003)	A query for location information is received from a Public Identity that has not been registered before.
DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)	The user is not allowed to roam in the visited network.
DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED (5005)	The identity being registered already has a server assigned and the registration status does not allow that it is overwritten.



Unsuccessful Result Code	Description
DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED (5006)	The authentication scheme indicated in an authentication request is not supported.
DIAMETER_ERROR_IN_ASSIGNMENT_TYPE (5007)	The identity being registered already has the same server assigned and the registration status does not allow the server assignment type.
DIAMETER_ERROR_TOO_MUCH_DATA (5008)	The volume of the data pushed to the receiving entity exceeds its capacity.
DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA (5009)	The S-CSCF informs the HSS that the received subscription data contained information, which was not recognized or supported.
DIAMETER_ERROR_FEATURE_UNSUPPORTED (5011)	A request application message was received indicating that the origin host requests that the command pair would be handled using a feature which is not supported by the destination host.

5.1.12 Framed-IP-Address

The Framed-IP-Address contains the IPv4 address of the user as shown in Table 67.

Table 67 Framed-IP-Address

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	8	> 12	OctetString

The Framed-IP-Address is defined in the [RFC 4005 Diameter Network Access Server Application \(Aug 2005\)](#) specification.

5.1.13 Origin-Host

The Origin-Host AVP attribute, as shown in Table 68, identifies the endpoint that originated the Diameter message.

The Origin-Host is a configurable value in the CSCF.

Example:

scscf.example.com



Table 68 Origin-Host

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	264	> 8	Diameter Identity

5.1.14 Origin-Realm

The Origin-Realm AVP attribute, as shown in Table 69, contains the realm of the originator of the Diameter message.

The Origin-Realm is a configurable value in the CSCF.

Example:

example.com

Table 69 Origin-Realm

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	296	> 8	Diameter Identity

5.1.15 Redirect-Host

The Redirect-Host AVP attribute, as shown in Table 70, contains the HSS host address.

This AVP must be present if the answer messages “E” bit is set and the Result-Code AVP is set to DIAMETER_REDIRECT_INDICATION.

Upon receiving this, the receiving Diameter node must forward the request directly to the host identified in the AVP. The server contained in the selected Redirect-Host AVP must be used for all messages pertaining to this session.

Table 70 Redirect-Host

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	292	> 8	DiameterURI

5.1.16 Redirect-Host-Usage

The Redirect-Host-Usage AVP attribute, as shown in Table 71, dictates how the routing entry resulting from the Redirect-Host is to be used. If not received the Redirect-Host must not be cached.

This AVP can be present if the answer messages “E” bit is set and the Result-Code AVP is set to DIAMETER_REDIRECT_INDICATION.



The Redirect-Host-Usage AVP is ignored by the CSCF. The CSCF does not cache the host received in the Redirect-Host AVP.

Table 71 Redirect-Host-Usage

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	261	12	Enumerated

5.1.17 Redirect-Max-Cache-Time

The Redirect-Max-Cache-Time AVP attribute, as shown in Table 72, contains the maximum number of seconds that the peer and route table entries, created as a result of the Redirect-Host, are cached.

This AVP must be present if the answer messages “E” bit is set and the Result-Code AVP is set to DIAMETER_REDIRECT_INDICATION and the Redirect-Host-Usage AVP is set to a non-zero value.

The Redirect-Max-Cache-Time AVP is ignored by the CSCF.

Table 72 Redirect-Max-Cache-Time

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	262	12	Unsigned32

5.1.18 Result-Code

The Result-Code AVP attribute, as shown in Table 73, indicates whether the request was completed successfully or whether an error occurred. This information element is used to indicate errors defined in the Diameter Base Protocol. This information element must not be present in case the Experimental-Result is included in the response.

The values of the Result-Code AVP are described in the [RCF3588 Diameter Base Protocol \(Sept 2003\)](#) specification.

Table 73 Result-Code

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	268	12	Unsigned32

5.1.19 Session-Id

The Session-Id AVP attribute, as shown in Table 74, identifies the session between the CSCF and the HSS.

Note: The session is implicitly terminated after the response.



The format of the Session-Id generated by the CSCF is as follows:

```
<DiameterIdentity>; <Unique string>
```

DiameterIdentity = CSCF domain name

Unique string = CSCF generated globally unique (over space and time) string

Example:

```
cscf.example.com;46d7f635;049cca;2286243985
```

Table 74 Session-Id

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	263	> 8	UTF8String

5.1.20

User-Name

The User-Name AVP, as shown in Table 75, can have one of the following two possible strings:

- Private User Identity string
- Proprietary string @ALL, see Section 4.1.11 Push-Profile-Request on page 93.

In a UAR and MAR request, this AVP is populated by the value of the username included in the SIP request Authentication header, or, if not available, derived from the SIP request To header.

The User-Name included in a Cx response or Cx HSS initiated request is the Private User Identity of the user as stored in the HSS.

Table 75 User-Name

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	1	> 8	UTF8String

5.1.21

Vendor-Id

The Vendor-Id AVP attribute, as shown in Table 76, contains the IANA value assigned to the vendor of the Diameter application. Value assigned to 3GPP is 10415.

Table 76 Vendor-Id

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	266	12	Unsigned32



5.1.22 Vendor-Specific-Application-Id

The Vendor-Specific-Application-Id AVP attribute, as shown in Table 77, indicates the vendor, 3GPP, owning the application and the application type, authentication.

The vendor identifier assigned by IANA to 3GPP is 10415.

The Diameter application identifier assigned by IANA to the Cx/Dx interface application is 16777216.

Table 77 Vendor-Specific-Application-Id

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	260	> 32	Grouped

The AVP Format is as follows:

```
Vendor-Specific-Application-Id ::= < AVP Header: 260 >
  1* [Vendor-Id]
  0*1 { Auth-Application-Id }
  0*1 { Acct-Application-Id }
```

5.2 3GPP Cx/Dx Diameter Applications AVPs

The Diameter AVPs defined for the Cx interface protocol, their AVP Code values, and types are described in Table 78. The Vendor-ID header of all AVPs defined is set to 3GPP (10415).

Table 78 3GPP Cx/Dx Diameter Application AVPs

AVP	AVP Code	Value Type
Access-Network-Information	1263	OctetString
Associated-Identities	632	Grouped
Associated-Registered-Identities	647	Grouped
Charging-Information	618	Grouped
Confidentiality-Key	625	OctetString
Deregistration-Reason	615	Grouped
Feature-List-ID	629	Unsigned32
Feature-List	630	Unsigned32
Identity-with-Emergency-Registration	651	Grouped
Integrity-Key	626	OctetString
Loose-Route-Indication	638	Enumerated



Table 78 3GPP Cx/Dx Diameter Application AVPs

AVP	AVP Code	Value Type
Mandatory-Capability	604	Unsigned32
Multiple-Registration-Indication	648	Enumerated
Optional-Capability	605	Unsigned32
Originating-Request	633	Enumerated
Primary-Charging-Collection-Function-Name	621	DiameterURI
Primary-Event-Charging-Function-Name	619	DiameterURI
Public-Identity	601	UTF8String
Reason-Code	616	Enumerated
Reason-Info	617	UTF8String
Restoration-Info	649	Grouped
SAR-Flags	655	Unsigned32
SCSCF-Restoration-Info	639	Grouped
Secondary-Charging-Collection-Function-Name	622	DiameterURI
Secondary-Event-Charging-Function-Name	620	DiameterURI
Server-Assignment-Type	614	Enumerated
Server-Capabilities	603	Grouped
Server-Name	602	UTF8String
SIP-Authenticate	609	OctetString
SIP-Authentication-Context	611	OctetString
SIP-Authentication-Scheme	608	UTF8String
SIP-Auth-Data-Item	612	Grouped
SIP-Authorization	610	OctetString
SIP-Digest-Authenticate	635	Grouped
SIP-Item-Number	613	Unsigned32
SIP-Number-Auth-Items	607	Unsigned32
Supported-Applications	631	Grouped
Supported-Features	628	Grouped
UAR-Flags	637	Unsigned32
User-Authorization-Type	623	Enumerated
User-Data	606	OctetString



Table 78 3GPP Cx/Dx Diameter Application AVPs

AVP	AVP Code	Value Type
User-Data-Already-Available	624	Enumerated
Visited-Network-Identifier	600	OctetString
Wildcarded-Public-Identity	634	UTF8String
Wildcarded-Public-User-Identity	636	UTF8String
3GPP-SGSN-MCC-MNC	18	UTF8String
Subscription-Info	642	Grouped

5.2.1 Access-Network-Information

The Access-Network-Information AVP attribute, as shown in Table 79, contains information about the current location data of a user. The value contains the complete SIP header P-Access-Network-Info, excluding the header name. The token used to indicate empty access-type is the character “-”, only one access-type is supported.

Table 79 Access-Network-Information

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	1263	>12	OctetString	10415

5.2.2 Associated-Identities

The Associated-Identities AVP attribute, as shown in Table 80, contains the Private User Identities associated to an IMS subscription.

The AVP format is as follows:

```
Associated-Identities:: = < AVP Header : 632 10415 >
*[ User-Name ]
*[ AVP ]
```

This information element is ignored by the CSCF.

Table 80 Associated-Identities

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	632	>12	Grouped	10415



5.2.3 Charging-Information

The Charging-Information AVP attribute, as shown in Table 81, contains the addresses of the Charging functions.

The AVP format is as follows:

```
Charging-Information ::= < AVP Header : 618 10415 >
[ Primary-Event-Charging-Function-Name ]
[ Secondary-Event-Charging-Function-Name ]
[ Primary-Charging-Collection-Function-Name ]
[ Secondary-Charging-Collection-Function-Name ]
*[ AVP ]
```

Table 81 Charging-Information

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	618	>12	Grouped	10415

5.2.4 Primary-Event-Charging-Function-Name

This Primary-Event-Charging-Function-Name AVP attribute, as shown in Table 82, contains the address of the Primary Online Charging Function.

Table 82 Primary-Event-Charging-Function-Name

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	619	>12	DiameterURI	10415

5.2.5 Secondary-Event-Charging-Function-Name

The Secondary-Event-Charging-Function-Name AVP attribute, as shown in Table 83, contains the address of the Secondary Online Charging Function.

Table 83 Secondary-Event-Charging-Function-Name

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	620	>12	DiameterURI	10415

5.2.6 Primary-Charging-Collection-Function-Name

The Primary-Charging-Collection-Function-Name AVP attribute, as shown in Table 84, contains the address of the Primary Charging Data Function.

Table 84 Primary-Charging-Collection-Function-Name

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	621	>12	DiameterURI	10415

5.2.7 Secondary-Charging-Collection-Function-Name

The Secondary-Charging-Collection-Function-Name AVP attribute, as shown in Table 85, contains the address of the Secondary Charging Data Function.

Table 85 Secondary-Charging-Collection-Function-Name

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	622	>12	DiameterURI	10415

5.2.8 Deregistration-Reason

The Deregistration-Reason AVP attribute, as shown in Table 86, indicates the reason for a deregistration operation.

The AVP format is as follows:

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

Table 86 Deregistration-Reason

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	615	>12	Grouped	10415

5.2.9 Reason-Code

The Reason-Code AVP attribute, as shown in Table 87, defines the reason for the network initiated deregistration. The following values are defined:

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



The detailed behavior of the S-CSCF is defined in the [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#) specification.

Table 87 Reason-Code

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	616	16	Enumerated	10415

5.2.10

Reason-Info

The Reason-Info AVP attribute, as shown in Table 88, contains textual information to inform the user about the reason for a deregistration.

Table 88 Reason-Info

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	617	>12	UTF8String	10415

5.2.11

Originating-Request

The Originating-Request AVP attribute, as shown in Table 89, indicates to the HSS that the request is related to an AS originating SIP request. The following value is defined:

— ORIGINATING (0)

Table 89 Originating-Request

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	633	16	Enumerated	10415

5.2.12

Public-Identity

The Public-Identity AVP attribute, as shown in Table 90, contains the Public User Identity of a user in the IMS. The syntax corresponds either to a SIP URI or a tel URI.

Table 90 Public-Identity

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	601	>12	UTF8String	10415



5.2.13 Server-Assignment-Type

The Server-Assignment-Type AVP attribute, as shown in Table 91, indicates the type of server update being performed in an SAR operation. The following values are defined as:

— NO_ASSIGNMENT (0)

This value is used to request, from the HSS, the user profile assigned to one or more public identities and to retrieve the S-CSCF restoration information for a registered Public User Identity, without affecting the registration state of those identities.

— REGISTRATION (1)

The request is generated as a consequence of a first registration of an identity.

— RE_REGISTRATION (2)

The request corresponds to the reregistration of an identity or update of the S-CSCF Restoration Information.

— UNREGISTERED_USER (3)

The request is generated because the S-CSCF received an INVITE for a Public Identity that is not registered.

— TIMEOUT_DEREGISTRATION (4)

The SIP registration timer of an identity has expired.

— USER_DEREGISTRATION (5)

The S-CSCF has received a user initiated deregistration request.

— TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME (6)

The SIP registration timer of an identity has expired. The S-CSCF keeps the user data stored in the S-CSCF and requests the HSS to store the S-CSCF name.

— USER_DEREGISTRATION_STORE_SERVER_NAME (7)

The S-CSCF has received a user initiated deregistration request. The S-CSCF keeps the user data stored in the S-CSCF and requests the HSS to store the S-CSCF name.

— ADMINISTRATIVE_DEREGISTRATION (8)

The S-CSCF, because of administrative reasons, has deregistered of an identity.



Table 91 Server-Assignment-Type

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	614	16	Enumerated	10415

5.2.14

Server-Capabilities

The Server-Capabilities AVP attribute, as shown in Table 92, contains the required capabilities of the S-CSCF to be assigned to the IMS Subscription.

The AVP format is as follows:

```
Server-Capabilities ::= < AVP Header: 297 10415 >
* [ Mandatory-Capability ]
* [ Optional-Capability ]
* [ Server-Name ]
* [ AVP ]
```

Table 92 Server-Capabilities

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	603	>12	Grouped	10415

5.2.15

Mandatory-Capability

The Mandatory-Capability AVP attribute, as shown in Table 93, contains a specific service capability of an S-CSCF.

The exact meaning of each value is defined by the operator.

Table 93 Mandatory-Capability

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	604	16	Unsigned32	10415

5.2.16

Optional-Capability

The Optional-Capability AVP attribute, as shown in Table 94, contains a specific service capability of an S-CSCF.

The exact meaning of each value is defined by the operator.



Table 94 Optional-Capability

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	605	16	Unsigned32	10415

5.2.17

Server-Name

The Server-Name AVP attribute, as shown in Table 95, contains the name of the assigned S-CSCF or an AS name defined as a SIP URI.

Table 95 Server-Name

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	602	>12	UTF8String	10415

5.2.18

Session-Priority

The Session-Priority AVP, as shown in Table 96, indicates the priority level of the session to the HSS. It is of type Enumerated.

The following values are defined, where PRIORITY-0 is the highest priority:

- PRIORITY-0 (0)
- PRIORITY-1 (1)
- PRIORITY-2 (2)
- PRIORITY-3 (3)
- PRIORITY-4 (4)

Table 96 Session-Priority

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	650	16	Enumerated	10415

5.2.19

SIP-Auth-Data-Item

The SIP-Auth-Data-Item AVP attribute, as shown in Table 97, contains the authentication and authorization information, or both, for the Diameter client.

The AVP format is as follows:



```
SIP-Auth-Data-Item ::= < AVP Header : 612 10415 >
[ SIP-Item-Number ]
[ SIP-Authentication-Scheme ]
[ SIP-Authenticate ]
[ SIP-Authorization ]
[ SIP-Authentication-Context ]
[ Confidentiality-Key ]
[ Integrity-Key ]
* [ Line-Identifier ]
[ SIP-Digest-Authenticate ]
* [ AVP ]
```

Table 97 SIP-Auth-Data-Item

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	612	>12	Grouped	10415

5.2.20

SIP-Authenticate

The SIP-Authenticate AVP attribute, as shown in Table 98, contains specific parts of the data portion of the WWW-Authenticate or Proxy-Authenticate SIP headers that are to be present in a SIP response.

Table 98 SIP-Authenticate

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	609	>12	OctetString	10415

5.2.21

SIP-Authentication-Context

The SIP-Authentication-Context AVP attribute, as shown in Table 99, contains authentication-related information relevant for authentication, but that is not part of the SIP Authentication Headers.

Table 99 SIP-Authentication-Context

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	611	>12	OctetString	10415

5.2.22

SIP-Authentication-Scheme

The Authentication-Scheme AVP attribute, as shown in Table 100, indicates the authentication scheme used in the authentication of SIP messages.

The following values are defined:

- Digest-AKAv1-MD5
Indicates that IMS-AKA authentication is to be used.
- NASS-Bundled
Indicates that NASS Bundled Authentication is to be used.
- SIP Digest
Indicates that SIP Digest Authentication is to be used.
- Early-IMS-Security
Indicates that GPRS IMS Bundled Authentication is to be used.

Table 100 SIP-Authentication-Scheme

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	608	>12	UTF8String	10415

5.2.23 SIP-Authorization

The SIP-Authorization AVP attribute, as shown in Table 101, contains specific parts of the data portion of the Authorization or Proxy-Authorization SIP headers suitable for inclusion in a SIP request.

Table 101 SIP-Authorization

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	610	>12	OctetString	10415

5.2.24 SIP-Digest-Authenticate

The SIP-Digest-Authenticate AVP attribute, as shown in Table 102, is a grouped AVP and contains AVPs used for digest authentication.

This AVP is specified in the following specifications:

- [RFC 2617 HTTP Authentication: Basic and Digest Access Authentication \(Jun 1999\)](#)
- [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#)
- [3GPP TS 29.229 \(V 8.1.0\) 3Cx and Dx interfaces based on the Diameter Protocol](#)



The AVP format is as follows:

```
SIP-Digest-Authenticate ::= < AVP Header: 635 10415 >
{ Digest-Realm }
[ Digest-Algorithm ]
{ Digest-QoP }
{ Digest-HA1 }
[ Secondary-Digest-HA1 ]
*[ AVP ]
```

Table 102 SIP-Digest-Authenticate

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	635	>12	Grouped	10415

5.2.25

SIP-Item-Number

The SIP-Item-Number AVP attribute, as shown in Table 103, is included in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVP, and the order in which they are processed is significant. In this scenario, the SIP-Auth-Data-Item AVP with a low SIP-Item-Number value is processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.

Table 103 SIP-Item-Number

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	613	16	Unsigned32	10415

5.2.26

SIP-Number-Auth-Items

The SIP-Number-Auth-Items AVP attribute, as shown in Table 104, indicates the number of authentication vectors the S-CSCF is requesting when used in a request. This can be used, for example, when the client is requesting several precalculated authentication vectors. SIP Digest and GIBA support one set of authentication vectors. 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.

Table 104 SIP-Number-Auth-Items

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	607	16	Unsigned32	10415

5.2.27 Confidentiality-Key

The Confidentiality-Key AVP attribute, as shown in Table 105, contains the Confidentiality Key (CK).

Table 105 Confidentiality-Key

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	625	>12	OctetString	10415

5.2.28 Integrity-Key

The Integrity-Key AVP attribute, as shown in Table 106, contains the Integrity Key (IK).

Table 106 Integrity-Key

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	626	>12	OctetString	10415

5.2.29 Supported-Applications

The Supported-Applications AVP attribute, as shown in Table 107, contains the supported application identifiers of a Diameter node.

The AVP format is as follows:

```
Supported-Applications ::= < AVP header: 631 10415 >
*[ Auth-Application-Id ]
*[ Acct-Application-Id ]
*[ Vendor-Specific-Application-Id ]
*[ AVP ].
```

Table 107 Supported-Applications

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	631	>12	Grouped	10415

5.2.30 Supported-Features

The Supported-Feature AVP attribute, as shown in Table 108, informs the destination host about the features that the origin host supports. The S-CSCF supports the SiFC feature, the S-CSCF Restoration Procedure, and the P-CSCF



Restoration Procedure. It includes this AVP in SAR and PPA messages when the feature is enabled.

The CSCF supports the SiFC feature, the S-CSCF Restoration Procedure, and the P-CSCF Restoration Procedure. Diameter request including indication of any other extended feature is rejected with DIAMETER_ERROR_FEATURE_UNSUPPORTED.

The AVP format is as follows:

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

Table 108 Supported-Features

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	628	>44	Grouped	10415

5.2.31

Feature-List

The Feature-List AVP attribute, as shown in Table 109, contains a bit mask indicating the supported features of an application.

Table 109 Feature-List

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	630	16	Unsigned32	10415

The meaning of the bits is shown in Table 110.



Table 110 Feature-List Bit Description

Feature bit ⁽¹⁾	Feature ⁽²⁾	Description
0	SiFC	<p>Shared iFC sets</p> <p>This feature is applicable for the SAR/SAA and PPR/PPA command pairs.</p> <p>If the HSS and the S-CSCF both support this feature, subsets of Initial Filter Criteria can be shared by several service profiles and the HSS downloads the SiFC sets implicitly by downloading the unique identifiers of the SiFC sets to the S-CSCF. Through a locally administered database, the S-CSCF then maps the downloaded identifiers onto the SiFC sets.</p> <p>If the S-CSCF does not support this feature, the HSS does not download identifiers of SiFC sets. Instead as a default behavior the HSS, through a locally administered database, downloads the Initial Filter Criteria of an SiFC set explicitly. If the HSS does not support this feature, no special default behavior is required for the S-CSCF.</p> <p>(3)</p>
1	AliasInd	<p>Alias Indication</p> <p>This feature is applicable for the SAR/SAA and PPR/PPA command pairs.</p> <p>This feature is not supported by the S-CSCF.</p>



Feature bit ⁽¹⁾	Feature ⁽²⁾	Description
2	IMSRestorationInd	IMS Restoration Indication This feature is applicable for the UAR/UAA, LIR/LIA, SAR/SAA command pairs. If both the HSS and the I-CSCF support this feature and the I-CSCF is not able to contact the S-CSCF that is assigned in the HSS, the I-CSCF triggers the assignment of a new S-CSCF. If the HSS and the S-CSCF both support this feature, the S-CSCF sends S-CSCF Restoration Information to the HSS. The HSS sends this information element in SAA to the S-CSCF when required. If the S-CSCF does not support this feature, the HSS does not send the IMS Restoration Information to the S-CSCF.
3	P-CSCF-Restoration-mechanism	HSS-based P-CSCF Restoration mechanism This feature is applicable for the SAR/SAA command pair. If the S-CSCF supports this feature, the S-CSCF sends the P-CSCF-Restoration-Indication in SAR-Flags AVP to the HSS when the P-CSCF Restoration Procedure is triggered.

(1) The order number of the bit within the Supported-Features AVP, for example, “1”.

(2) A short name that can be used to refer to the bit and to the feature, for example, “SiFC”.

(3) When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and the HSSs consistent.

5.2.32 Feature-List-ID

The Feature-List-ID AVP attribute, as shown in Table 111, contains the identity of a feature list.

The CSCF only supports Feature-List-ID 1. A Diameter request including Feature-List-ID of any other value is rejected with DIAMETER_ERROR_FEATURE_UNSUPPORTED.



Table 111 Feature-List-ID

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	629	16	Unsigned32	10415

5.2.33

User-Authorization-Type

The User-Authorization-Type AVP attribute, as shown in Table 112, contains the type of authorization requested by the I-CSCF.

The I-CSCF includes the following information elements in the command:

— REGISTRATION (0)

If registration or reregistration. I-CSCF determines this.

— DE-REGISTRATION (1)

If Deregistration

— REGISTRATION_AND_CAPABILITIES (2)

When the S-CSCF is assigned to the Public User Identity in the HSS, it cannot be contacted and a new S-CSCF must be selected.

Table 112 User-Authorization-Type

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	623	16	Enumerated	10415

5.2.34

User-Data

The User-Data AVP attribute, as shown in Table 113, contains the user data required to give service to a user.

The exact content and format of this AVP is described in the [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#) specification.

Table 113 User-Data

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	606	>12	OctetString	10415



5.2.35 User-Data-Already-Available

The User-Data-Already-Available AVP attribute, as shown in Table 114, indicates to the HSS whether the S-CSCF already has the part of the user profile that it needs to serve the user.

The following values are defined:

— USER_DATA_NOT_AVAILABLE (0)

The S-CSCF does not have the data that it needs to serve the user.

— USER_DATA_ALREADY_AVAILABLE (1)

The S-CSCF already has the data that it needs to serve the user

Table 114 User-Data-Already-Available

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	624	16	Enumerated	10415

5.2.36 Visited-Network-Identifier

The Visited-Network-Identifier AVP attribute, as shown in Table 115, contains the identifier that allows the home network to identify the visited network.

Table 115 Visited-Network-Identifier

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	600	> 12	OctetString	10415

5.2.37 Wildcarded-Public-Identity

The Wildcarded-Public-Identity AVP attribute, as shown in Table 116, contains a Wildcarded Public User Identity provisioned in the HSS.

Table 116 Wildcarded-Public-Identity

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	634	> 12	UTF8String	10415



5.2.38 Wildcarded-Public-User-Identity

The Wildcarded-Public-User-Identity AVP attribute is shown in Table 117.

Table 117 Wildcarded-Public-User-Identity

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	636	> 12	UTF8String	10415

The Wildcarded-IMPU AVP has been deprecated for 3GPP TS29.228 v8.8.0/v9.3.0 and later releases and TS29.229 v8.9.0/v9.3.0 and later releases, to cope with vendors who have implemented its Cx interface according to the old release before the previously stated releases, when the Wildcarded-IMPU AVP (code 636) is received from the HSS in the LIA message, it is processed by the I-CSCF in the same way as if the Wildcarded-Public-Identity AVP (code 634) is received.

5.2.39 3GPP-SGSN-MCC-MNC

The 3GPP-SGSN-MCC-MNC AVP attribute, as shown in Table 118, contains the UTF-8 encoding of the Routing Area Identity MCC-MNC values, which are the SGSN information where the user is roaming. The MCC is three digits and the MNC is either two or three digits. There is to be no padding characters between the MCC and MNC.

The 3GPP-SGSN-MCC-MNC AVP is defined in the [3GPP TS 23.003 Numbering, addressing and identification](#) and [3GPP TS 29.060 GPRS Tunnelling Protocol \(GTP\) across the Gn and Gp interface](#) specifications.

Table 118 3GPP-SGSN-MCC-MNC

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	18	19–20	UTF8String	10415

5.2.40 Loose-Route-Indication

The Loose-Route-Indication AVP, as shown in Table 119, is of type Enumerated and indicates to the S-CSCF whether the loose route mechanism is required to serve the registered Public User Identities.

Table 119 Loose-Route-Indication

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	638	16	Enumerated	10415



The following values are defined:

- LOOSE_ROUTE_NOT_REQUIRED (0)
- LOOSE_ROUTE_REQUIRED (1)

5.2.41 SCSCF-Restoration-Info

The SCSCF-Restoration-Info AVP attribute, as shown in Table 120, is a grouped AVP that contains restoration information of an IMPI/IMPU pair or an IMPI/IRS pair.

The AVP format is as follows:

```
SCSCF-Restoration-Info ::= < AVP Header: 639, 10415 >
{ User-Name }
1*{ Restoration-Info }
[ SIP-Authentication-Scheme ]
*[ AVP ]
```

Table 120 SCSCF-Restoration-Info

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	639	>828	Grouped	10415

5.2.42 Path

The Path AVP, as shown in Table 121, is an AVP that contains list of SIP proxies (URIs). Refer to the [3GPP TS 29.229 Cx and Dx interfaces based on the Diameter Protocol](#) and [RFC 3327 SIP Extension Header Field for Registering Non-Adjacent Contacts](#) specifications.

The AVP format is as follows:

```
Path ::= < AVP Header: 640, 10415 >
{<SIP Proxy1 URI>, <SIP Proxy2 URI>, ... <SIP Proxyn URI>}
```

Table 121 Path

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	640	>12	OctetString	10415

5.2.43 Restoration-Info

Restoration-Info AVP attribute, as shown in Table 122, is a grouped AVP that contains restoration information of a contact.

```

Restoration-Info ::= < AVP Header: 649, 10415 >
{ Path }
{ Contact }
[ Subscription-Info ]
*[ AVP ]

```

Table 122 Restoration-Info

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	649	>820	Grouped	10415

5.2.44 Multiple-Registration-Indication

The Multiple-Registration-Indication AVP attribute, as shown in Table 123, is of type Enumerated and indicates to the HSS whether the request is related to a multiple registration.

The following values are defined:

- NOT_MULTIPLE_REGISTRATION (0)
- MULTIPLE_REGISTRATION (1)

Table 123 Multiple-Registration-Indication

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	648	16	Enumerated	10415

5.2.45 Identity-with-Emergency-Registration

The Identity-with-Emergency-Registration AVP, as shown in Table 124, is of type Grouped and it contains a pair of PrivatePublic User Identity which is emergency registered.

AVP format:

```

Identity-with-Emergency-Registration ::=
  < AVP header: 651, 10415 >
  { User-Name }
  { Public-Identity }

```

The Restoration-Info AVP is not included in this grouped AVP.



Table 124 Identity-with-Emergency-Registration

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	651	>20	Grouped	10415

5.2.46

UAR-Flags

The UAR-Flags AVP, as shown in Table 125, is of type Unsigned32 and it contains a bit mask.

Table 125 UAR-Flags

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	637	16	Unsigned32	10415

The meaning of the bits is defined in Table 126:

Table 126 Bit Mask

Bit	Name	Description
0	IMS Emergency Registration	This bit, when set, indicates that the request corresponds to an IMS Emergency Registration.
Bits not defined in this table are to be cleared by the sending I-CSCF and discarded by the receiving HSS.		

5.2.47

SAR-Flags

The SAR-Flags AVP, as shown in Table 127, is of type Unsigned32 and it contains a bit mask.

Table 127 SAR-Flags

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	655	16	Unsigned32	10415

The meaning of the bits is defined in Table 128:



Table 128 Bit Mask

Bit	Name	Description
0	P-CSCF Restoration Indication	This bit, when set, indicates that the P-CSCF-Restoration-mechanism feature shall be executed. This AVP is present only when Server-Assignment-Type takes the value ADMINISTRATIVE_DEREGISTRATION or UNREGISTERED_USER.
Bits not defined in this table are to be cleared by the sending S-CSCF and discarded by the receiving HSS.		

5.2.48 Associated-Registered-Identities

The Associated-Registered-Identities AVP, as shown in Table 129, is of type Grouped and it contains the Private User Identities registered with the Public User Identity received in the request command.

Table 129 Associated-Registered-Identities

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	647	> 12	Grouped	10415

The AVP format is as follows:

```
Associated-Registered-Identities ::=
  < AVP Header : 647 10415 >
* [ User-Name ]
* [ AVP ]
```

5.2.49 Subscription-Info

The Subscription-Info AVP attribute, as shown in Table 130, is a grouped AVP that contains subscription information of a contact.

AVP format:

```
Subscription-Info ::= < AVP Header: 642, 10415 >
{ Call-ID-SIP-Header }
{ From-SIP-Header }
{ To-SIP-Header }
{ Record-Route }
{ Contact }
*[ AVP ]
```



Table 130 Subscription-Info

V	M	P	AVP Code	AVP Length	AVP data type	Vendor-ID
1	0	0	642	>12	Grouped	10415

5.2.50 Call-ID-SIP-Header

The Call-ID-SIP-Header AVP attribute, as shown in Table 131, is of type OctetString and it contains the information in the Call-ID header as defined in [RFC 3261](#).

Table 131 Call-ID-SIP-Header

V	M	P	AVP Code	AVP Length	AVP data type	Vendor-ID
1	0	0	643	>12	OctetString	10415

5.2.51 From-SIP-Header

The From-SIP-Header AVP attribute, as shown in Table 132, is of type OctetString and it contains the information in the From header as defined in [RFC 3261](#).

Table 132 From-SIP-Header

V	M	P	AVP Code	AVP Length	AVP data type	Vendor-ID
1	0	0	644	>12	OctetString	10415

5.2.52 To-SIP-Header

The To-SIP-Header AVP attribute, as shown in Table 133, is of type OctetString and it contains the information in the To header as defined in [RFC 3261](#).

Table 133 To-SIP-Header

V	M	P	AVP Code	AVP Length	AVP data type	Vendor-ID
1	0	0	645	>12	OctetString	10415

5.2.53 Record-Route

The Record-Route AVP attribute, as shown in Table 134, is of type OctetString and it contains a list of Record Route header separated by \n as defined in [RFC 3261](#).



Table 134 Record-Route

V	M	P	AVP Code	AVP Length	AVP data type	Vendor-ID
1	0	0	646	>12	OctetString	10415

5.2.54

Contact

The Contact AVP attribute, as shown in Table 135, is of type OctetString and it contains Contact header as defined in [RFC 3261](#).

Table 135 Contact

V	M	P	AVP Code	AVP Length	AVP data type	Vendor-ID
1	0	0	641	>12	OctetString	10415

5.3

ETSI Diameter Applications AVPs

The Diameter AVPs defined for the Cx interface protocol, their AVP Code values and types are defined in Table 136. The Vendor-ID header of all AVPs defined must be set according to the ETSI (13019).

Table 136 ETSI Diameter Application AVPs

Attribute Name	AVP Code	Value Type
Line-Identifier	500	OctetString

5.3.1

Line-Identifier

The Line-Identifier AVP attribute, as shown in the following table, contains a fixed broadband access line identifier associated with the user or string value containing Line_Profile.

Table 137 Line-Identifier

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	500	>12	OctetString	13019



5.4 Ericsson Diameter Applications AVPs

The Diameter AVPs defined for the Cx interface protocol, their AVP Code values and types are defined in Table 138. The Vendor-ID header of all AVPs defined must be set to Ericsson (193).

Table 138 Ericsson Diameter Application AVPs

Attribute Name	AVP Code	Value Type
GPRS-Roaming-Status	333	Enumerated
Activity-Information	288	Grouped
Feature-Tag	289	UTF8String
SSO-Status	280	Enumerated
Secondary-Digest-HA1	1192	UTF8String

5.4.1 GPRS-Roaming-Status

The GPRS-Roaming-Status AVP attribute, as shown in the following table, is of type Enumerated and states if the user is attached to its home network or not.

The values considered for the GPRS-Roaming-Status AVP are the following:

- HOME (0)
- VISITED (1)

Table 139 GPRS-Roaming-Status

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	333	16	Enumerated	193

5.4.2 Activity-Information

The Activity-Information AVP attribute, as shown in Table 140, is of type Grouped, and contains AVPs that store the time and feature tag when the user was considered as active for the specific feature, expressed in seconds.

The AVP format is as follows:

```
Activity-Information ::= < AVP Header: 288 193 >
{ Feature-Tag }
{ Event-Timestamp }
[ Public-Identity ]
* [ AVP ]
```



Table 140 Activity-Information

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	288	>44	Grouped	193

5.4.3

Feature-Tag

The Feature-Tag AVP attribute, as shown in Table 141, is a string that contains the name of the feature whose activity information (time stamp) is received. The feature tags are received in Accept-contact header.

Table 141 Feature-Tag

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	289	>12	UTF8String	193

5.4.4

SSO-Status

The SSO-Status AVP attribute, as shown in Table 142, is of type Enumerated and states that GIBA information for all GIBA users in the HSS has become invalid. It can only be used together with the SIP-Authentication-Scheme set to **Early-IMSSecurity** and User-Name AVP set to **@ALL**.

The values considered for the SSO-Status AVP are as follows:

- NON-VALID (0) (not used)
- NON-TRUSTED (1)

Table 142 SSO-Status

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	280	16	Enumerated	193

5.4.5

Secondary-Digest-HA1

This AVP attribute, as shown in Table 143, holds the digested value of the username without its realm part, the authentication realm, and the user password.

Table 143 Secondary-Digest-HA1

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	0	0	1192	>12	UTF8String	193

5.5 User Profile

5.5.1 User Profile in UML Model

An IMS Subscription class is shown in Figure 49.

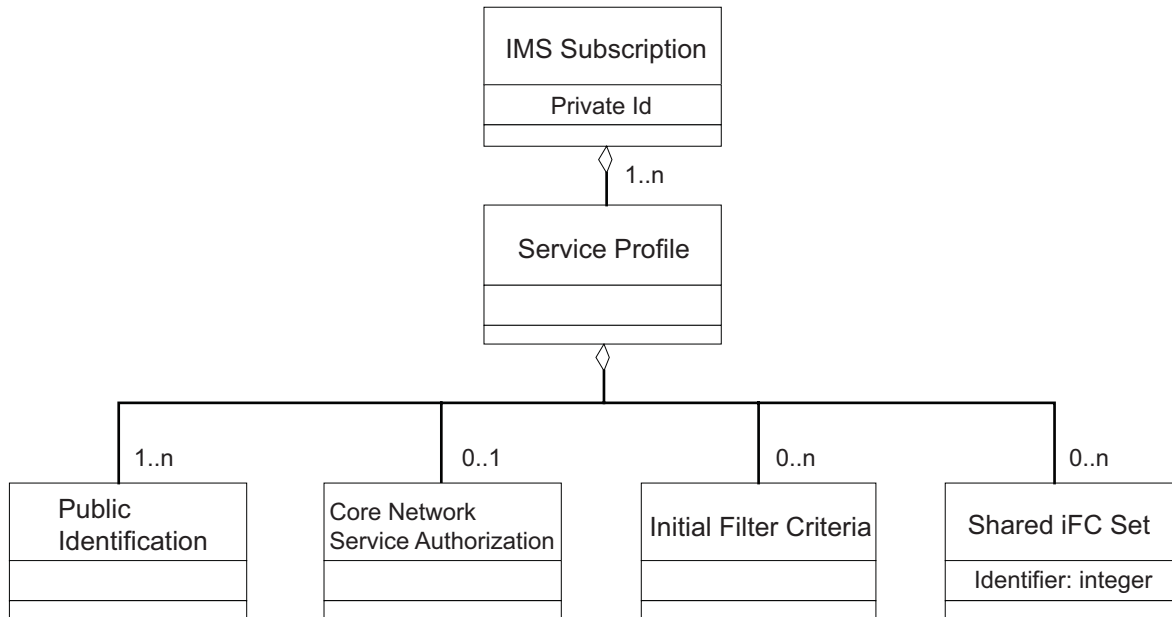


Figure 49 IMS Subscription Class

The IMS Subscription class contains as a parameter the Private User Identity of the user in NAI address format.

For more information about the Private User Identity of the user in NAI address format, refer to the [RFC 2486 The Network Access Identifier](#) specification.

The IMS subscription optionally contains an ESRN value to use for emergency calls originated by a user associated with the subscription. The Subscription class can contain optional Ericsson extensions, of type `EricssonIMSSubscriptionExtension`, for Roaming Awareness information and Subscription Identity information. Each instance of the IMS Subscription class contains one or several instances of the Service Profile class.

Each instance of the Service Profile class consists of one or several instances of the Public Identification class. The Public Identification class contains the Public Identities with that service profile. The information in the Core Network Service Authorization, Initial Filter Criteria, and SiFC Set classes apply to all Public Identification instances, which are included in one Service Profile class.

Each instance of the Service Profile class contains zero or one instance of the Core Network Service Authorization class which contains the Subscribed Media Profile Id class. Each instance of the Service Profile class contains zero or more instances of the Initial Filter Criteria class.



Each instance of the Service Profile class contains zero or more instances of the class SiFC Set. An SiFC Set points to a set of Initial Filter Criteria locally administered and stored at the S-CSCF. SiFC Sets can be shared by several Service Profiles.

The Service Profile class can contain Ericsson extensions (`EricssonServiceProfileExtension`) for Maximum Number of Simultaneous Sessions and Phone-Context information.

The Public Identification class can contain Ericsson extensions (`EricssonPublicIdentityExtension`) for Maximum Number of Contacts.

A Public Identification with the Identity Type set to Wildcarded-PSI has some limitation to the allowed data structure, as follows:

- Only one Public Identification object is allowed in the Service Profile (the Wildcarded-PSI).
- Only one Service Profile object is allowed in the IMS Subscription for a Wildcarded-PSI.
- The S-CSCF generates a SIP “500 Service Execution Error” if more than one Public Identification or Service Profile is received from the HSS for a Wildcarded-PSI.

5.5.1.1 Initial Filter Criteria

An Initial Filter Criteria class is shown in Figure 50.

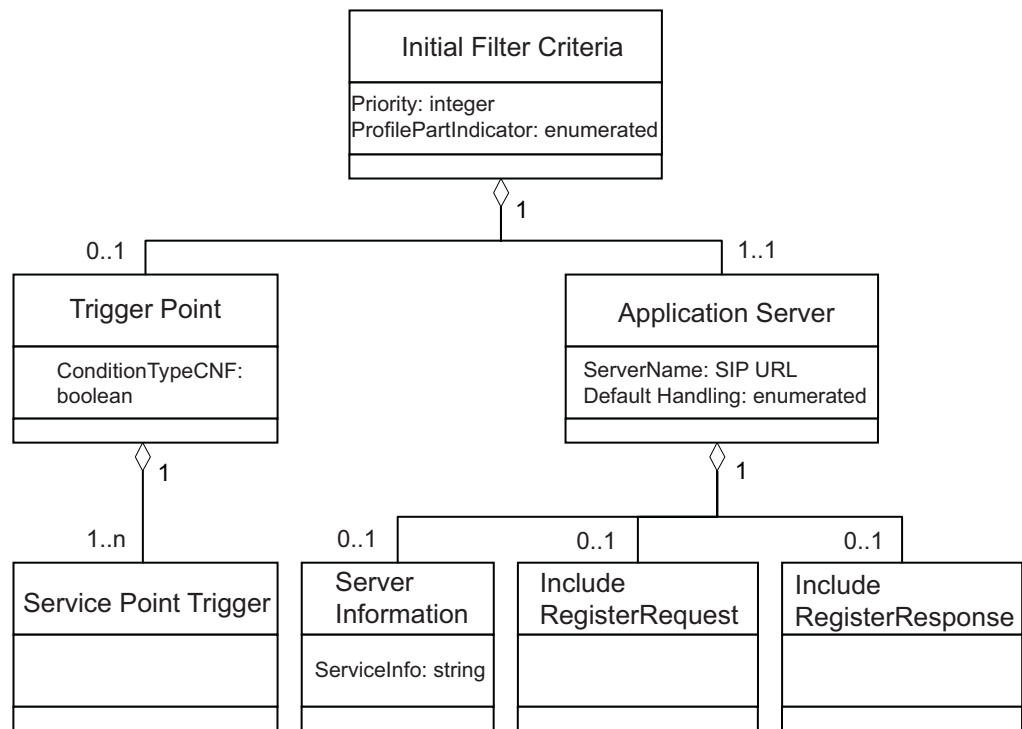


Figure 50 Initial Filter Criteria Class

Each instance of the Initial Filter Criteria class is composed of zero or one instance of a Trigger Point class and one instance of an Application Server class. Priority indicates the priority of the Filter Criteria, where the value 0 has highest priority and then the priority decreases with higher priority values. The S-CSCF ignores the ProfilePartIndicator as the use of this attribute is unclear in the standard. The S-CSCF assumes that the HSS always includes all Initial Filter Criteria in the downloaded user profile (registered and unregistered).

The Trigger Point class describes the trigger points that are checked to find out if the indicated Application Server is contacted or not. Each TriggerPoint is a boolean expression in Conjunctive or Disjunctive Normal form (CNF or DNF). The absence of Trigger Point instance indicates an unconditional triggering to Application Server.

Each Trigger Point is composed by one to several instances of the Service Point Trigger class.

The Application Server class defines the application server, which is contacted, if the trigger points are met. Server Name is the SIP URI of the application server to contact. Default Handling determines whether the dialog is to be released if the Application Server could not be reached or not; it is of type enumerated and can take the values: SESSION_CONTINUED or SESSION_TERMINATED.

The Application Server class contains zero or one instance of the Service Information class. The S-CSCF does not support Service Information.

The Application Server class includes 0–1 classes of include register request and include register response. The include register request class indicates to the S-CSCF that the incoming SIP REGISTER request is to be included in the message body of the third-party REGISTER request and transferred to an Application Server when the trigger points of a filter criterion are satisfied. The include register response class indicates to the S-CSCF that the final SIP response to the incoming SIP REGISTER request is to be included in the message body of the third-party REGISTER request and transferred to an Application Server when the trigger points of a filter criterion are satisfied.

5.5.1.2 Service Point Trigger

The Service Point Trigger class is shown in Figure 51.

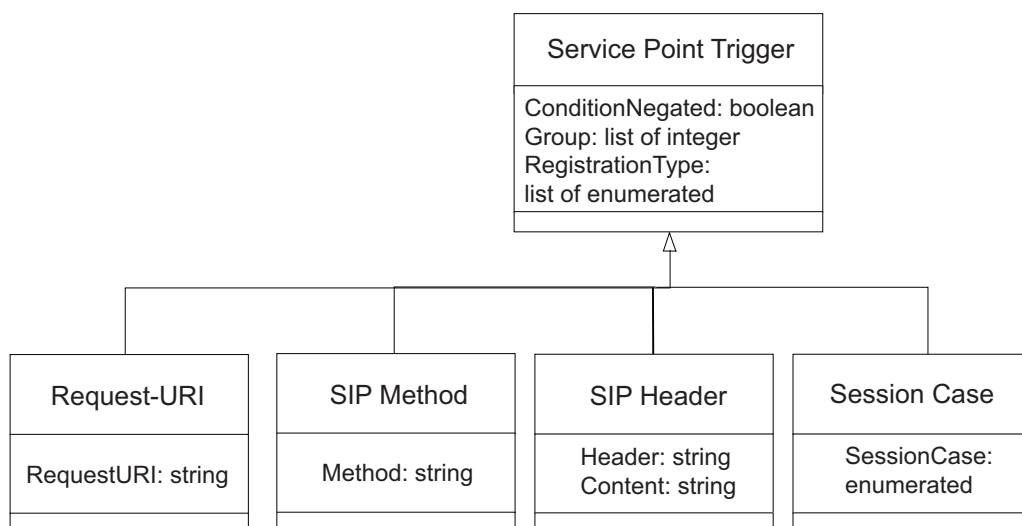


Figure 51 Service Point Trigger Class

The Request-URI class defines Service Point Trigger (SPT) for the Request-URI. Request-URI contains the attribute RequestURI.

The SIP Method class defines the SPT for the SIP method. The SIP Method contains the attribute Method which holds the name of any SIP method.

The SIP Header class defines the SPT for the presence or absence of any SIP header or for the content of any SIP header. The SIP Header contains the attribute Header which identifies the SIP Header, which is the SPT, and the Content attribute defines the value of the SIP Header if necessary.

The S-CSCF supports Regular expression in the Content tag, but not for the Header tag.

The absence of the Content attribute and ConditionNegated = TRUE indicates that the SPT is the absence of a determined SIP header.

Session Case class represents an enumerated type, with possible values, as follows:

- Originating_Session
- Originating_Unregistered
- Terminating_Registered
- Terminating_Unregistered
- Originating_CDIV

These indicate whether the filter is to be used by the S-CSCF while handling the Originating services for a registered end user, Originating services for an unregistered end user, Terminating services for a registered end user, Terminating services for an unregistered end-user, or Originating services after retargeting for a terminating Served user.

The Session Description Information class defines the SPT for the content of any SDP field within the body of a SIP Method. SDP triggering is not supported by the S-CSCF and is ignored if received.

5.5.2

User Profile in XML Format

The user profile received in the User-Data AVP is in XML[®] format. The user profile XML is valid against the user profile XML schema defined in the following tables. The way the information is to be transferred through the Cx interface can be seen from a high-level point of view in Figure 52.

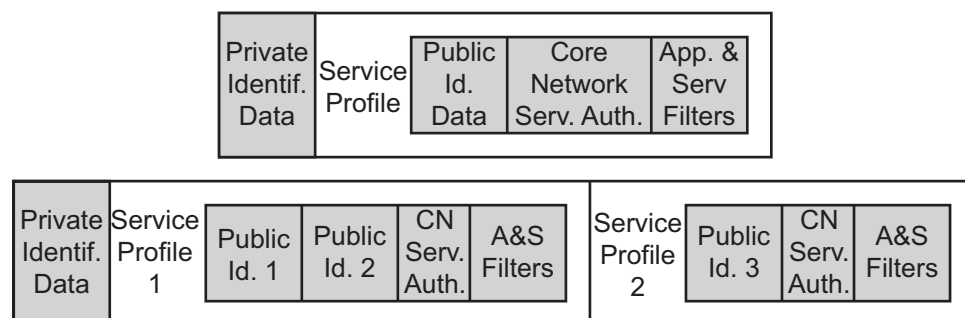


Figure 52 Examples of In-Line Format of User Profile

The schema used for the User-Data AVP complies with the schema file, CxDataType_Re17.xsd, attached to the [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#) specification.

The simple and complex data types and the dependencies among them are described in Table 144 and Table 145.



5.5.3

Simple Data Types

The simple data types are defined in Table 144.

Table 144 XML Schema for Cx Interface User Profile: Simple Data Types

Data Type	Tag	Base Type	Comments
tPriority	Priority	integer	≥ 0
tProfilePartIndicator ⁽¹⁾	ProfilePartIndicator	enumerated	Possible values are as follows: <ul style="list-style-type: none"> 0 (REGISTERED) 1 (UNREGISTERED)
tSharedIFCSetID	SharedIFCSetID	integer	≥ 0
tGroupID	Group	integer	≥ 0
tRegistrationType	RegistrationType	enumerated	Possible values are as follows: <ul style="list-style-type: none"> 0 (INITIAL_REGISTRATION) 1 (RE-REGISTRATION) 2 (DE-REGISTRATION)
tDefaultHandling	DefaultHandling	enumerated	Possible values are as follows: <ul style="list-style-type: none"> 0 (SESSION_CONTINUED) 1 (SESSION_TERMINATED)
tDirectionOfRequest	SessionCase	enumerated	Possible values are as follows: <ul style="list-style-type: none"> 0 (ORIGINATING_SESSION) 1 (TERMINATING_REGISTERED) 2 (TERMINATING_UNREGISTERED) 3 (ORIGINATING_UNREGISTERED) 4 (ORIGINATING_CDIV)
tPrivateID	PrivateID	anyURI	Syntax described in IETF [RFC 2486]
tSIP_URL	Identity	anyURI	Syntax described in IETF [RFC 3261]
tTEL_URL	Identity	anyURI	Syntax described in IETF [RFC 3966]
tIdentity	Identity	(union)	Union of tSIP_URL and tTEL_URL and tWildcardedIMPU (tWildcardedIMPU is ignored).
tIdentityType	IdentityType	enumerated	Possible values are as follows: <ul style="list-style-type: none"> 0 (PUBLIC_USER_IDENTITY) 1 (DISTINCT_PSI) 2 (WILDCARDED_PSI) 3 (WILDCARDED_IMPU)⁽²⁾⁽³⁾ 4 (IMPU_WILDCARD)⁽²⁾



Data Type	Tag	Base Type	Comments
tWildcardedPSI	WildcardedPSI	anyURI	Syntax described in 3GPP [TS23.003] .
tServiceInfo ⁽¹⁾	ServiceInfo	string	
tString	RequestURI, Method, Header, Content, Line, SgsnMccMnc, PhoneContext, SubscriptionIdData, FeatureTag	string	
tBool	ConditionTypeCNF, ConditionNegated, BarringIndication	boolean	Possible values are as follows: <ul style="list-style-type: none">• 0 (false)• 1 (true)
tSubscribedMediaProfileId	SubscribedMediaProfileId	integer	>=0
tDisplayName ⁽¹⁾	DisplayName	string	
tAliasIdentityGroupID ⁽¹⁾	AliasIdentityGroupID	string	
tServiceLevelTraceInfo ⁽¹⁾	ServiceLevelTraceInfo	string	Syntax described in clause 14 within IETF draft-dawes-sipping-debug
tServicePriorityLevel	ServicePriorityLevel	enumerated	Possible values: 0 (Highest priority) 1 2 3 4 (Lowest priority)
tPriorityNamespace ⁽¹⁾	PriorityNamespace	string	Possible values are those of the namespaces that are defined in RFC 4412 or defined according to the IANA registration procedure described in RFC 4412 for Resource-Priority Namespaces.
tPriorityLevel ⁽¹⁾	PriorityLevel	string	Possible values depend on the PriorityNamespace and are specified with the associated namespace that is defined in RFC 4412 or defined according to the IANA registration procedure described in RFC 4412 for Resource-Priority Namespaces.
tIMSI ⁽¹⁾	IMSI	string	Syntax described in 3GPP TS 23.003.
tMaxNumOfAllowedSimultRegistrations ⁽¹⁾	MaxNumOfAllowedSimultRegistrations	integer	>= 1
tSubscriptionIdType	SubscriptionIdType	enumerated	Possible value: 0 (END_USER_E164)
tGPRSRoamingStatus	GPRSRoamingStatus	enumerated	Possible values are as follows: <ul style="list-style-type: none">• 0 (HOME)• 1 (VISITED)
tMaxNoSimultaneousSessions	MaxNoSimultaneousSessions	integer	>=0 ⁽⁴⁾



Data Type	Tag	Base Type	Comments
tMaxNoOfContacts	MaxNoOfContacts	integer	≥ 0
tDiameterTime	EventTimeStamp	integer	≥ 0

(1) Datatype/Tag is ignored.

(2) WILDCARDED_IMPU indicates that it is a distinct Public User Identity matching a Wildcarded Public User Identity. IMPU_WILDCARD indicates that the content of the identity in the "Identity" tag is a Wildcarded Public User Identity.

(3) If IdentityType is WILDCARDED_IMPU, WildcardedIMPU is mandatory. If IdentityType is IMPU_WILDCARD, WildcardedIMPU is optional.

(4) When the value 0 is received, the session limit enforcement is disabled.

When the value 65535 is received, the session limit enforcement is disabled, and the release of dialogs when contacts are deregistered is also disabled. The number of dialogs per Service Profile is unlimited.

When any other value is received, a limit on the number of simultaneous sessions is enforced. The recommended maximum values are as follows:

- For a Service Profile without wIMPU, use 300
- For a Service Profile with one or more wIMPU, use $65536 / (\text{lengthOfCallID} + 26)$. When the average Call-Id length is unknown, use 300 or 65535 as applicable.

With exception of 65535:

- Dialogs are limited to 8000 per Service Profile.
- For an Implicit Registration Set without wIMPU, deregistration of a contact releases the associated dialogs of that contact.
- For an Implicit Registration Set with one or more wIMPU, dialogs are only released at deregistration of the last contact.

5.5.4

Complex Data Types

The complex data type is defined in Table 145.

Table 145 XML Schema for Cx Interface User Profile: Complex Data Types

Data Type	Tag	Compound Of		
		Tag	Type	Cardinality
tIMSSubscription	IMSSubscription	PrivateID	tPrivateID	1
		ServiceProfile	tServiceProfile	(1 to n)
		EricssonIMSSubscriptionExtension	tEricssonIMSSubscriptionExtension	(0 to 1)
		ESRN ⁽¹⁾	tString	(0 to 1)
tServiceProfile	Service Profile	PublicIdentity	tPublicIdentity	(1 to n)
		InitialFilterCriteria	tInitialFilterCriteria	(0 to n)
		CoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	(0 to 1)
		Extension	tServiceProfileExtension	(0 to 1)
		EricssonServiceProfileExtension	tEricssonServiceProfileExtension	(0 to 1)
tServiceProfileExtension	Extension	SharedIFCSetID	tSharedIFCSetID	(0 to n)



Data Type	Tag	Compound Of		
		Tag	Type	Cardinality
tCoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	SubscribedMediaProfileId	tSubscribedMediaProfileId	(0 to 1)
		Extension	tCNServicesAuthorizationExtension	(0 to 1)
tEricssonServiceProfileExtension	EricssonServiceProfileExtension	MaxNoSimultaneousSessions	tMaxNoSimultaneousSessions	(0 to 1) ⁽²⁾
		PhoneContext	tString	(0 to 1)
tEricssonIMSSubscriptionExtension	EricssonIMSSubscriptionExtension	SubscriptionId	tSubscriptionId	(0 to 1)
		RoamingAwarenessInfo	tRoamingAwarenessInfo	(0 to 1)
tSubscriptionId	SubscriptionId	SubscriptionIdType	tSubscriptionIdType	1
		SubscriptionIdData	tString	1
tRoamingAwarenessInfo	RoamingAwarenessInfo	SgsnMccMnc	tString	1
		GPRSRoamingStatus	tGPRSRoamingStatus	1
tPublicIdentity	PublicIdentity	BarringIndication	tBool	(0 to 1)
		Identity	tIdentity	1
		Extension	tPublicIdentityExtension	(0 to 1)
		EricssonPublicIdentityExtension	tEricssonPublicIdentityExtension	(0 to 1)
tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1
		TriggerPoint	tTrigger	(0 to 1)
		ApplicationServer	tApplicationServer	1
		ProfilePartIndicator	tProfilePartIndicator	(0 to 1)
tTrigger	TriggerPoint	ConditionTypeCNF	tBool	1
		SPT	tSePoTri	(1 to n)
tSePoTri	SPT	ConditionNegated	tBool	(0 to 1)
		Group	tGroupID	(1 to n)
		Choice of	RequestURI	tString
			Method	tString
			SIPHeader	tHeader
			SessionCase	tDirectionOfRequest
			Session Description ₍₄₎	1
		Extension	tSePoTriExtension	(0 to 1)
tSePoTriExtension	Extension	RegistrationType	tRegistrationType	(0 to 2)
tHeader	SIPHeader	Header	tString	1
		Content	tString	(0 to 1)



Data Type	Tag	Compound Of		
		Tag	Type	Cardinality
tSessionDescription ⁽⁴⁾	Session Description	Line	tString	1
		Content	tString	(0 to 1)
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	(0 to 1)
		ServiceInfo	tServiceInfo	(0 to 1)
		Extension	tApplicationServerExtension	(0 to 1)
tApplicationServerExtension	Extension	IncludeRegisterRequest	tIncludeRegisterRequest	(0 to 1)
		IncludeRegisterResponse	tIncludeRegisterResponse	(0 to 1)
tIncludeRegisterRequest	Include Register Request	(3)	(3)	(0 to 1)
tIncludeRegisterResponse	Include Register Response	(3)	(3)	(0 to 1)
PublicIdentityExtension	Extension	IdentityType	tIdentityType	(0 to 1)
		WildcardedPSI	tWildcardedPSI	(0 to 1)
		Extension	tPublicIdentityExtension2	(0 to 1)
tPublicIdentityExtension2	Extension	DisplayName ⁽⁴⁾	tDisplayName	(0 to 1)
		AliasIdentityGroupID ⁽⁴⁾	tAliasIdentityGroupID	(0 to 1)
		Extension	tPublicIdentityExtension3	(0 to 1)
tPublicIdentityExtension3	Extension	WildcardedIMPU	anyURI	(0 to 1)
		ServiceLevelTraceInfo ⁽⁴⁾	tServiceLevelTraceInfo	(0 to 1)
		ServicePriorityLevel	ServicePriorityLevel	(0 to n)
tEricssonPublicIdentityExtension	Ericsson PublicIdentityExtension	ActivityInformation	tActivityInformation	(0 to n)
		MaxNoOfContacts	tMaxNoOfContacts	(0 to 1)
tActivityInformation	Activity Information	FeatureTag	tString	1
		EventTimeStamp	tDiameterTime	1
tCNServicesAuthorizationExtension ⁽⁴⁾	Extension	ListOfServiceIds	tListOfServiceIds	(0 to 1)
tListOfServiceIds ⁽⁴⁾	ListOfServiceIds	ServiceId	tString	(0 to n)

(1) The ESRN tag is not part of the 3GPP standard. Only the ESRN tag associated to the www.huawei.com/ims/hss namespace is supported.

(2) For the possible values of MaxNoSimultaneousSessions, see Table 144.

(3) Empty cells are to be interpreted as complex XML elements without defined content. The content of this attribute is irrelevant and ignored by CSCF. Only the presence or absence of the attribute is relevant for CSCF.

(4) Datatype/Tag is ignored.



Note: “n” is interpreted as non-bounded.

5.5.5 Regular Expressions in User Profile

The following values of SPTs are interpreted as regular expressions:

- The Content tag of a SIP Header
- The Request-URI

An example of a SIP Header Content tag that contains a regular expression is as follows:

```
<Content>sip:some.*name.*$</Content>
```

It is possible to make the regular expression case insensitive by including the ignore case flag. This is done by embedding the regular expression with the “/” character followed by the flag “i”, for example, as follows:

```
<RequestURI>/^.*SomeName/i</RequestURI>
```

Note: It is possible to embed the regular expression with the “/” character without including the ignore case flag, as in the following example:

```
<RequestURI>/^.*SomeName/</RequestURI>
```

This format is interpreted like the format without the “/” character.

5.5.6 Private Extension to IMS Subscription

The IMS subscription received in the User-Data AVP can be extended with non-standard parameters. Extension parameters must be allocated to a vendor-specific name space to avoid collision with the implementation of another vendor.

5.5.6.1 ESRN

The ESRN non-standard parameter contained within the `http://www.huawei.com/ims/hss` namespace is a supported extension to the IMS subscription.

The ESRN consists of a string containing a seven or ten digits number used to route emergency calls to the Public Safety Answering Point (PSAP).

5.5.7 XML Schema Definition for Proprietary Features

Ericsson proprietary information on IMS Subscription level is conveyed within the **EricssonIMSSubscriptionExtension** element (in bold), as follows:

```
<xs:complexType name="tIMSSubscription">  
  <xs:sequence>
```



```

        <xs:element name="PrivateID" type="tPrivateID" />
        <xs:element maxOccurs="unbounded" name="ServiceProfile"
type="tServiceProfile" />
        <xs:element minOccurs="0" name="Extension"
type="tExtension" />
        <xs:element minOccurs="0" maxOccurs="1"
name="EricssonIMSSubscriptionExtension" type="tEricssonIMSSubscri
ptionExtension" /> <xs:any minOccurs="0" maxOccurs="unbounded"
namespace="##other" processContents="lax" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tEricssonIMSSubscriptionExtension">
    <xs:sequence>
        <xs:element minOccurs="0"
name="SubscriptionId" type="tSubscriptionId" />
        <xs:element minOccurs="0"
name=" RoamingAwarenesInfo " type="
tRoamingAwarenesInfo " />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tSubscriptionId">
    <xs:sequence>
        <xs:element minOccurs="1"
name="SubscriptionIdType"
type="tSubscriptionIdType" />
        <xs:element minOccurs="1"
name="SubscriptionIdData "
type="xs:string" />
    </xs:sequence>
</xs:complexType>

<xs:simpleType name=" tSubscriptionIdType ">
    <xs:restriction base="xs:unsignedByte">
        <xs:minInclusive value="0" />
        <xs:maxInclusive value="0" />
        <xs:enumeration value="0">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en"> END_USER_E164</label>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>
<xs:complexType name="tRoamingAwarenesInfo">
    <xs:sequence>
        <xs:element minOccurs="1"
name=" SgsnMccMnc " type="xs:string " />
        <xs:element minOccurs="1"

```



```
name=" GPRSRoamingStatus "
  type="tGPRSRoamingStatus " />
</xs:sequence>
</xs:complexType>

<xs:simpleType name=" tGPRSRoamingStatus ">
  <xs:restriction base="xs:unsignedByte">
    <xs:minInclusive value="0" />
    <xs:maxInclusive value="1" />
    <xs:enumeration value="0">
      <xs:annotation>
        <xs:documentation>
          <label xml:lang="en">HOME</label>
        </xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="1">
      <xs:annotation>
        <xs:documentation>
          <label xml:lang="en">VISITED</label>
        </xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>
```

Ericsson proprietary information on Service Profile level is conveyed within the EricssonServiceProfileExtension element (in bold), as follows:

```
<xs:complexType name="tServiceProfile">
  <xs:sequence>
    <xs:element maxOccurs="unbounded"
name="PublicIdentity" type="tPublicIdentity" />
    <xs:element minOccurs="0"
name="CoreNetworkServicesAuthorization"
type="tCoreNetworkServicesAuthorization" />
    <xs:element minOccurs="0" maxOccurs="unbounded"
name="InitialFilterCriteria" type="tInitialFilterCriteria" />
    <xs:element minOccurs="0" name="Extension"
type="tServiceProfileExtension"
/>
    <xs:element minOccurs="0" minOccurs="1" name="EricssonServiceProf
ileExtension" type="tEricssonServiceProfileExtension " />
    <xs:any minOccurs="0" maxOccurs="unbounded"
namespace="##other" processContents="lax" />
  </xs:sequence>
</xs:complexType>

<xs:complexType
name="tEricssonServiceProfileExtension ">
  <xs:sequence>
```




```

        <xs:element minOccurs="0"
name=" MaxNoSimultaneousSessions "
type="tMaxNoSimultaneousSessions " />
        <xs:element minOccurs="0"
name=" PhoneContext" type="xs:string" />
    </xs:sequence>
</xs:complexType>

<xs:simpleType name=t MaxNoSimultaneousSessions ">
    <xs:restriction base="xs:int">
        <xs:minInclusive value="0" />
    </xs:restriction>
</xs:simpleType>

```

Ericsson proprietary information on Public Identity level is conveyed within the EricssonPublicIdentityExtension element (in bold), as follows:

```

<xs:complexType name="tPublicIdentity">
    <xs:sequence>
        <xs:element minOccurs="0" default="0"
name="BarringIndication" type="tBool"/>
        <xs:element name="Identity" type="tIdentity" />
        <xs:element minOccurs="0" name="Extension"
type="tPublicIdentityExtension"/>
        <xs:element minOccurs="0" name=" EricssonPublicIdentityExtension
" type="tEricssonPublicIdentityExtension " />          <xs:any
minOccurs="0" maxOccurs="unbounded"
namespace="##other" processContents="lax" />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tEricssonPublicIdentityExtension">
    <xs:sequence>
        <xs:element minOccurs="0" name="ActivityInformation"
type="tActivityInformation" />
        <xs:element minOccurs="0" name="MaxNoOfContacts"
type="tMaxNoOfContacts " />
    </xs:sequence>
</xs:complexType>

<xs:complexType name="tActivityInformation">
    <xs:sequence>
        <xs:element minOccurs="0"
name="FeatureTag" type="tFeatureTag" />
        <xs:element minOccurs="0"
name="EventTimeStamp" type="tDiameterTime " />
    </xs:sequence>
</xs:complexType>

<xs:simpleType name="tFeatureTag">
    <xs:restriction base="xs:string">
        <xs:minLength value="0" />
    </xs:restriction>
</xs:simpleType>

```



```

        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="tDiameterTime">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0" />
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="tMaxNoOfContacts">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0" />
        </xs:restriction>
    </xs:simpleType>

```

5.5.8 Example of User Profile

The XML representation of a user profile is as follows:

```

<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="C:\ \CxPlusPlus.xsd">
    <PrivateID>IMPI1@homedomain.com</PrivateID>
    <ServiceProfile>
        <PublicIdentity>
            <BarringIndication>1</BarringIndication>
            <Identity> sip:IMPU1@homedomain.com </Identity>
            <EricssonPublicIdentityExtension>
                <ActivityInformation>
                    <Feature-Tag> *;+g.poc.talkburst
                    </Feature-Tag>
                    <Event-Timestamp>3480850800
                    </Event-Timestamp>
                </ActivityInformation>
                <MaxNoOfContacts>3</MaxNoOfContacts>
            </EricssonPublicIdentityExtension>
        </PublicIdentity>
        <PublicIdentity>
            <Identity> sip:IMPU2@homedomain.com </Identity>
        </PublicIdentity>
        <InitialFilterCriteria>
            <Priority>0</Priority>
            <TriggerPoint>
                <ConditionTypeCNF>1</ConditionTypeCNF>
                <SPT>
                    <ConditionNegated>0</ConditionNegated>
                    <Group>0</Group>
                    <Method>INVITE</Method>
                </SPT>
            </TriggerPoint>
        </InitialFilterCriteria>
    </ServiceProfile>
</IMSSubscription>

```



```

    <SPT>
      <ConditionNegated>0</ConditionNegated>
      <Group>0</Group>
      <Method>SUBSCRIBE</Method>
    </SPT>
    <SPT>
      <ConditionNegated>1</ConditionNegated>
      <Group>1</Group>
      <SIPHeader>
        <Header>From</Header>
        <Content>"joe"</Content>
      </SIPHeader>
    </SPT>
  </TriggerPoint>
  <ApplicationServer>
    <ServerName>sip:AS1@homedomain.com
    </ServerName>
    <DefaultHandling>0</DefaultHandling>
    <Extension>
      <IncludeRegisterRequest>
      </IncludeRegisterRequest>
      <IncludeRegisterResponse>
      </IncludeRegisterResponse>
    </Extension>
  </ApplicationServer>
</InitialFilterCriteria>
<EricssonServiceProfileExtension>
  <MaxNoSimultaneousSessions>2
  </MaxNoSimultaneousSessions>
  <Phone-Context>cscf.com</ Phone-Context>
</EricssonServiceProfileExtension>
</ServiceProfile>
<EricssonIMSSubscriptionExtension>
  <SubscriptionId>
    <SubscriptionIdType>0</SubscriptionIdType>
    <SubscriptionIdData>00001000</SubscriptionIdData>
  </SubscriptionId>
  <RoamingAwarenessInfo>
    <SgsnMccMnc>
      SGSN1B34. MNC0092.MCC0167.3gppnetwork.org
    </SgsnMccMnc>
    <GPRSRoamingStatus>0</GPRSRoamingStatus>
  </RoamingAwarenessInfo>
</EricssonIMSSubscriptionExtension>
  <ESRN xmlns="http://www.huawei.com/ims/hss">1234567</ESRN>
</IMSSubscription>

```





6 Security Considerations

The communication between the CSCF and the HSS/SLF can be secured using IPsec (Zb interface) on the IP transport layer, as described in the [3GPP TS 29.328 IP Multimedia \(IM\) Subsystem Sh interface; Signalling flows and message contents](#) specification.

IPsec tunnels can be defined between the two nodes. IKEv1 performs mutual authentication between the two nodes and establishes an IKE Security Association that includes shared secret information used to establish IPsec SAs. Different forms of authentication and encryptions can be selected when defining the IPsec tunnels. For the native CSCF, refer to *Security Management User Guide*, and for the virtual CSCF, refer to *eVIP Management Guide*.





7

Related Standards

The following standard specifications apply:

- [RFC 3588 Diameter Base Protocol](#)
- [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#)
- [3GPP TS 29.229 3Cx and Dx interfaces based on the Diameter Protocol](#)

The NASS Bundled Authentication follows the standards given in the following specifications:

- [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#)
- [3GPP TS 29.229 3Cx and Dx interfaces based on the Diameter Protocol](#)

CSCF Support for Wildcarded IMPU follows the standards given in the [3GPP TS 29.228 IP Multimedia Subsystem Cx and Dx interfaces](#) and [3GPP TS 29.229 Cx and Dx interfaces based on the Diameter Protocol](#) specifications.

The security of the communication between the CSCF and the HSS/SLF using IPsec follows the standards given in the [3GPP TS 29.328 IP Multimedia \(IM\) Subsystem Sh interface; Signalling flows and message contents](#) specification.

3GPP extended features that are not supported are the following:

- Alias Identity Group ID (PublicIdentityExtensions)
- Display Name (PublicIdentityExtensions)
- List of Service IDs (CNServicesAuthorizationExtensions)
- Profile Part Indicator (InitialFilterCriteria)
- Service Information (ApplicationServer)
- Session Description (SPT)