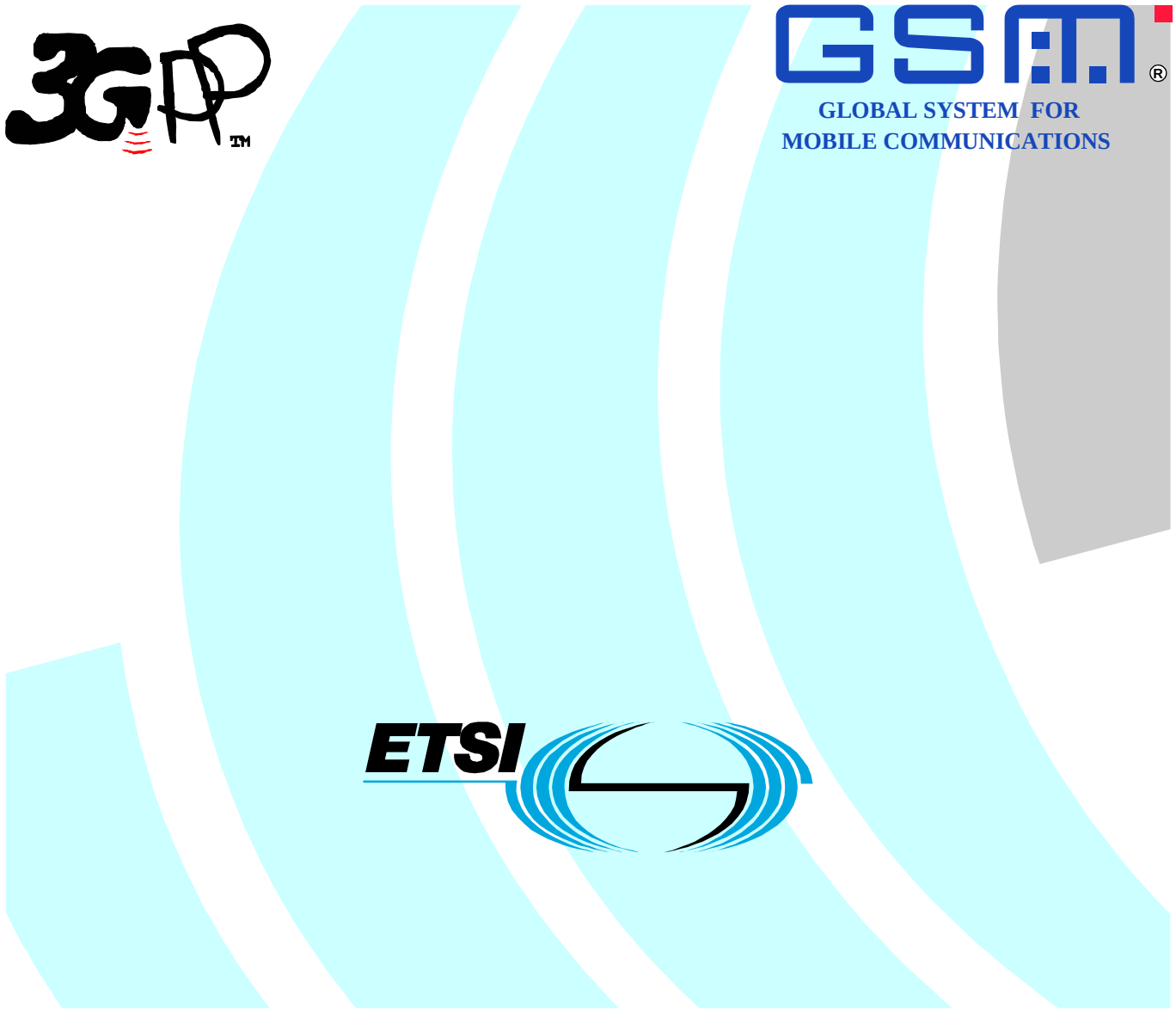
ETSI TS 129 228 V5.0.0 (2002-06)

Technical Specification

**Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
IP Multimedia (IM) Subsystem Cx and Dx Interfaces;
Signalling flows and message contents
(3GPP TS 29.228 version 5.0.0 Release 5)**



Reference
DTS/TSGN-0429228v500

Keywords
GSM, UMTS

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Intellectual Property Rights

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

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

Foreword

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

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

(1 presented to TSG for information;

(1 presented to TSG for approval;

(1 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This 3GPP Technical Specification (TS) specifies:

1. The interactions between the HSS (Home Subscriber Server) and the CSCF (Call Session Control Functions), referred to as the Cx interface.

2. The interactions between the CSCF and the SLF (Server Locator Function), referred to as the Dx interface.

The IP Multimedia (IM) Subsystem stage 2 is specified in 3GPP TS 23.228 [1] and the signalling flows for the IP multimedia call control based on SIP and SDP are specified in 3GPP TS 24.228 [2].

This document addresses the signalling flows for Cx and Dx interfaces.

2 References

[1] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2 (Release 5)".

[2] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP".

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

[4] 3GPP TS 23.002 "Network architecture".

[5] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details"

[6] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"

[7] Freed, N. and N. Borestein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

IP Multimedia session: IP Multimedia session and IP Multimedia call are treated as equivalent in this specification.

3.2 Abbreviations

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

AVP	Attribute Value Pair
C	Conditional
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IE	Information Element
IP	Internet Protocol
I-CSCF	Interrogating CSCF
IM	IP Multimedia
IMS	IP Multimedia Subsystem
M	Mandatory
MO	Mobile Originating
MT	Mobile Terminating
(1	Optional
P-CSCF	Proxy CSCF

SIP	Session Initiation Protocol
SLF	Server Locator Function
S-CSCF	Serving CSCF

4 Main Concept

This document presents the Cx interface related functional requirements of the communicating entities.

It gives a functional classification of the procedures and describes the procedures and message parameters.

Error handling flows, protocol version identification, etc. procedures are also included.

5 General Architecture

This clause further specifies the architectural assumptions associated with the Cx reference point, building on 3GPP TS 23.228 [1].

5.1 Functional requirements of network entities

5.1.1 Functional requirements of P-CSCF

There is no requirement for the interaction between the P-CSCF and the HSS.

5.1.2 Functional requirements of I-CSCF

The I-CSCF communicates with the HSS over the Cx interface.

For functionality of the I-CSCF refer to 3GPP TS 23.002 [4].

5.1.3 Functional requirements of S-CSCF

The S-CSCF communicates with the HSS over the Cx interface.

For functionality of the S-CSCF refer to 3GPP TS 23.002 [4].

5.1.4 Functional requirements of HSS

The HSS communicates with the I-CSCF and the S-CSCF over the Cx interface.

For functionality of the HSS refer to 3GPP TS 23.002 [4].

5.1.5 Functional classification of Cx interface procedures

Operations on the Cx interface are classified in functional groups:

1. Location management procedures
   - The operations regarding registration and de-registration.
   - Location retrieval operation.
2. User data handling procedures
   - The download of user information during registration and to support recovery mechanisms.
   - Operations to support the updating of user data and recovery mechanisms.

Editor's Note: Recovery mechanisms have not been specified in SA2 yet.

3. User authentication procedures

6 Procedure Descriptions

In the tables that describe the information elements transported by each command, each Information Element is marked as (M) Mandatory, © Conditional or (O) Optional. A mandatory information element shall always be present. A conditional information shall be present if certain conditions are fulfilled; if those conditions are not fulfilled it shall be absent. An optional information element may be present or absent in the command, at the discretion of the application at the sending entity.

6.1 Location management procedures

6.1.1 User registration status query

This procedure is used between the I-CSCF and the HSS during SIP registrations. The procedure is invoked by the I-CSCF, corresponds to the combination of the functional level operations Cx-Query and Cx-Select-Pull (see 3GPP TS 23.228 [1]) and is used:

- To authorize the registration of the user, checking multimedia subsystem access permissions and roaming agreements.
- To perform a first security check, determining whether the public and private identities sent in the message belong to the same user.
- To obtain either the S-CSCF where the user is registered or unregistered (i.e. registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), or the list of capabilities that the S-CSCF has to support.

This procedure is mapped to the commands User-Authorization-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.1.1 and 6.1.1.2 detail the involved information elements.

Table 6.1.1.1 : User registration status query

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	User public identity to be registered
Visited Network Identifier (See 7.1)	Visited-Network-Identifier	M	Identifier that allows the home network to identify the visited network
Type of Authorization (See 7.14)	User-Authorization-Type	C	Type of authorization requested by the I-CSCF. If the request corresponds to a de-registration, i.e. Expires field in the REGISTER method is equal to zero, this AVP shall be present in the command and the value shall be set to DE-REGISTRATION. If the request corresponds to an initial registration or a re-registration, i.e. Expires field in the REGISTER method is not equal to zero then this AVP may not be present in the command. If present its value shall be set to REGISTRATION.
Private User Identity (See 7.3)	User-Name	M	User private identity

Routing Information (See 7.13)	Destination-Host, Destination-Realm	C	If the I-CSCF knows HSS name Destination-Host AVP shall be present in the command. Otherwise, only Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the I-CSCF.

Table 6.1.1.2 : User registration status response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of the operation
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the user.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

6.1.1.1 Detailed behaviour

The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the user exists in the HSS. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check that the private and public identities received in the request belong to the same user. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR _IDENTITIES_DONT_MATCH.

3. Check the User-Authorization-Type received in the request:

   + If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not Vendor-Specific-Result shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). Continue to step 4.

   + If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 4.

   + If it is REGISTRATION_AND_CAPABILITIES, the HSS shall check that the user is allowed to roam in the visited network (if not Vendor-Specific-Result shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). The HSS shall return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy the most restrictive service profile of the user. The list of capabilities may be empty, to indicate to the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name.

4. Check the state of the public identity received in the request:

   + If it is registered or unregistered (i.e. registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

   + If it is not registered yet, the HSS shall check if at least there is at least one identity of the user with an S-CSCF name assigned.

     -- If so the HSS shall return the S-CSCF name assigned for the user and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

-- If there is not , the HSS shall return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy the most restrictive service profile of the user. The list of capabilities may be empty, to indicate to the I-CSCF that it can select any available S-CSCF. Vendor-Specific-Result be set to DIAMETER_FIRST_REGISTRATION. The HSS shall not return any S-CSCF name.

If the HSS cannot fulfil received request, e.g. due to database error, it shall set Result-Code to DIAMETER_UNABLE_TO_COMPLY. No S-CSCF name or S-CSCF capabilities shall be present in the response.

6.1.2 S-CSCF registration/deregistration notification

This procedure is used between the S-CSCF and the HSS. The procedure is invoked by the S-CSCF, corresponds to the combination of the operations Cx-Put and Cx-Pull (see 3GPP TS 23.228 [1]) and is used:

- To assign an S-CSCF to a public identity, or to clear the name of the S-CSCF assigned to one or more public identities.

- To download from HSS the relevant user profile information that the S-CSCF needs to serve the user.

This procedure is mapped to the commands Server-Assignment-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.2.1 and 6.1.2.2 describe the involved information elements.

Table 6.1.2.1: S-CSCF registration/deregistration notification request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	C	User public identity or list of user public identities. At least one public identity shall be present if User-Name is not present in the request.
S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity (See 7.3)	User-Name	C	User private identity. It shall be present if it is available when the S-CSCF issues the request. It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER. In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present. This indicates that all public identities shall be de-registered.
Server Assignment Type (See 7.8)	Server-Assignment-Type	M	Type of update the S-CSCF requests in the HSS (e.g: de-registration). See 3GPP TS 29.229 [5] for all the possible values.
User Data Request Type (See 7.15)	User-Data-Request-Type	M	Part of the user profile the S-CSCF requests from the HSS (e.g: complete profile). See 3GPP TS 29.229 [5] for all the possible values.
User Data Already Available (See 7.16)	User-Data-Already-Available	M	This indicates if the user profile is already available in the S-CSCF.

Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command. This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent in case of the terminating the session for unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	M	User private identity.
Registration result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of registration.
User Profile (See 7.7)	User-Data	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT. If the Server-Assignment-Type in the request is equal to REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER the User-Data AVP shall be present according to the rules defined in the section 6.6.
Charging Information (See 7.12)	Charging-Information	O	Addresses of the charging functions.

6.1.2.1 Detailed behaviour

On registering/deregistering a public identity the S-CSCF shall inform the HSS. The same procedure is used by the S-CSCF to get the user profile. The relevant user profile downloaded is described in more detailed in the section 6.6. The HSS holds information about the state of registration of all the identities of the user. The S-CSCF uses this procedure to update such state. The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the user is known. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS may check whether the private and public identities received in the request belong to the same user. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

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

   + If it indicates REGISTRATION or RE_REGISTRATION, the HSS shall download the relevant user public identity information. If set, the flag that indicates that the identity is pending of the confirmation of the authentication shall be cleared. The Result-Code shall be set to DIAMETER_SUCCESS.

Only one identity can be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and no user information shall be returned.

+ If it indicates UNREGISTERED_USER, the HSS shall store the S-CSCF name, set the registration state of the public identity as unregistered, i.e. registered as a consequence of a terminating call and download the relevant user public identity information. The Result-Code shall be set to DIAMETER_SUCCESS.

  Only one identity can be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and the modifications specified in the previous paragraph shall not be performed.

+ If it indicates TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, the HSS shall clear the S-CSCF name for all the public identities that the S-CSCF indicated in the request and set the registration state of the identities as not registered. If no public identity is present in the request, the private identity shall be present; the HSS shall clear the S-CSCF name for all the identities of the user and set their registration state to not registered. The Result-Code shall be set to DIAMETER_SUCCESS.

+ If it indicates TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME or USER_DEREGISTRATION_STORE_SERVER_NAME the HSS decides whether to keep the S-CSCF name stored or not for all the public identities that the S-CSCF indicated in the request and set the registration state of the identities as unregistered. If no public identity is present in the request, the private identity shall be present. If the HSS decided to keep the S-CSCF name stored the HSS keeps the S-CSCF name stored for all the identities of the user and set their registration state to unregistered.

  If the HSS decides to keep the S-CSCF name the Result-Code shall be set to DIAMETER_SUCCESS.

  If the HSS decides not to keep the S-CSCF name the Result-Code shall be set to DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED.

+ If it indicates NO_ASSIGNMENT, the HSS checks whether the user is assigned for the S-CSCF requesting the data and download the user public identity information requested in the User-Data-Request-Type AVP. The Result-Code shall be set to DIAMETER_SUCCESS. If the requesting S-CSCF is not the same as the assigned S-CSCF, the Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY.

+ If it indicates AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the HSS shall clear the S-CSCF name for the public identity that the S-CSCF indicated in the request and set the registration state of the identity as not registered. The flag that indicates that the identity is pending of the confirmation of the authentication shall be cleared. The Result-Code shall be set to DIAMETER_SUCCESS.

  Only one identity can be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and the modifications specified in the previous paragraph shall not be performed. See chapter 9.1 for the description on the behaviour of the HSS when the name of the S-CSCF received in the request is different from the name already stored in the HSS.

See chapter 8.1.2 for the description of the handling of the error situations: reception of an S-CSCF name different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible with the registration state of the user.

6.1.3 Network initiated de-registration by the HSS, administrative

In case of network initiated de-registration of the user initiated by the HSS, the HSS shall de-register the user and send a notification to the S-CSCF indicating the identities that shall be de-registered. The procedure is invoked by the HSS, corresponds to the functional level operation Cx-Deregister (see 3GPP TS 23.228 [1]).

HSS may decide to de-register:

- Only one public identity or a list of public identities
- All the public identities of a user.

This procedure is mapped to the commands Registration-Termination-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.3.1 and 6.1.3.2 describe the involved information elements.

Table 6.1.3.1 : Network Initiated Deregistration by HSS request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	O	It contains the list of public user identities that are de-registered, in the form of SIP URL or TEL URL.
Private User Identity (See 7.3)	User-Name	M	It contains the private user identity in the form of a NAI.
Reason for de-registration (See 7.11)	Deregistration -Reason	M	The HSS shall send to the S-CSCF a reason for the de-registration. The de-registration reason is composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [5]) that determines the behaviour of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given multimedia user. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

Table 6.1.3.2 : Network Initiated Deregistration by HSS response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	This information element indicates the result of de-registration.

6.1.3.1 Detailed behaviour

The HSS shall de-register the affected identities and invoke this procedure to inform the S-CSCF. The HSS can determine in different cases that the user (only one public identity, one or more public identities or all the public identities registered) has to be de-registered.

The HSS may de-register:

- Only one public identity or a list of public identities. In this case the S-CSCF shall remove all the information stored in the S-CSCF for those public identities.

- The user with all his/her public identities (no public identity sent in the Cx-Deregister request). In this case the S-CSCF shall remove all the information stored for that user.

The HSS shall send in the Deregistration-Reason AVP the reason for the de-registration, composed by a textual message (if available) aimed for the user and a reason code that determines the action the S-CSCF has to perform. The possible reason codes are:

- PERMANENT_TERMINATION: The IMS subscription or service profile(s) has been permanently terminated. The S-CSCF should start the network initiated de-registration towards the user.

- NEW_SERVER_ASSIGNED: A new S-CSCF has been allocated to the user due to some reason, e.g. an error case, where the SIP registration is terminated in a new S-CSCF. The S-CSCF shall not start the network initiated de-registration towards the user but only clears its registration state and information regarding the user, i.e. all service profiles are cleared.

- SERVER_CHANGE: A new S-CSCF shall be allocated to the user. The S-CSCF should start the network initiated de-registration towards the user, i.e. all registrations are de-registered and the user is asked to re-register to all existing registrations.

- REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF should no longer be used for a given user. The S-CSCF shall not start the network initiated de-registration towards the user when the user is not currently registered but clears all information regarding the user and responds to the HSS. The HSS then removes the S-CSCF for that user.

6.1.4 User location query

This procedure is used between the I-CSCF and the HSS to obtain the name of the S-CSCF where a public identity is registered. The procedure is invoked by the I-CSCF, is performed per public identity, and corresponds to the functional level operation Cx-Location-Query (see 3GPP TS 23.228 [1]).

This procedure is mapped to the commands Location Info Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.4.1 and 6.1.4.2 detail the involved information elements.

Table 6.1.4.1 : User Location query

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	M	User public identity
Routing information (See 7.13)	Destination-Host, Destination-Realm	C	If the I-CSCF knows HSS name Destination-Host AVP shall be present in the command. Otherwise, only Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the I-CSCF.

Table 6.1.4.2 : User Location response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of the operation
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	It contains the information to help the I-CSCF in the selection of the S-CSCF.

6.1.4.1 Detailed behaviour

The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the user is known. If not the Vendor-Specific-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check the state of the public identity received in the request.

+ If it is registered or unregistered (i.e. registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name. The Server-Name AVP shall contain the SIP URL of the server. The Server-Capabilities AVP shall not be present. The Result-Code AVP shall be set to DIAMETER_SUCCESS.

+ If it is not registered, but has services related to unregistered state, the HSS shall check if at least there is at least one identity or the user with an S-CSCF name assigned:

  -- If this is the case the HSS shall return the S-CSCF name assigned for that user. The Server-Name AVP shall contain the SIP URL of the server. The Server-Capabilities AVP shall not be present. The Result-Code shall be set to DIAMETER_SUCCESS.

  -- If there is not any S-CSCF name assigned for that user, the HSS may return information about the required S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The Server-Capabilities AVP may be present. The HSS shall send the same server capability set that is sent in the user registration status response during the registration. If Server-Capabilities AVP is not present, the I-CSCF shall understand that any S-CSCF is suitable to serve the user. The Server-Name AVP shall not be present. The Vendor-Specific-Result shall be set to DIAMETER_UNREGISTERED_SERVICE.

+ If it is not registered and has no unregistered services related data the response shall contain Vendor-Specific-Result set to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

If the HSS cannot fulfil received request, e.g. due to database error, it shall set Result-Code to DIAMETER_UNABLE_TO_COMPLY. No S-CSCF name or S-CSCF capabilities shall be present in the response.

6.2 User data handling procedures

6.2.1 User Profile download

As part of the registration procedure (3GPP TS 23.228 [1]) S-CSCF obtains user data and service related information by means of the Cx-Put Resp operation (see 6.1.2).

6.2.2 HSS initiated update of User Profile

This procedure is initiated by the HSS to update user profile information in the S-CSCF. This procedure corresponds to the functional level operation Cx-Update_Subscr_Data (see 3GPP TS 23.228 [1]).

This procedure is mapped to the commands Push-Profile-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.2.2.1 and 6.2.2.2 describe the involved information elements.

Table 6.2.2.1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	M	User private identity.
User profile (See 7.7)	User-Data	M	Updated service profile, with the format defined in chapter 8.8.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given multimedia user. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

Table 6.2.2.2: User Profile Update response

Information	Mapping to	Cat.	Description

element name	Diameter AVP		
Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	This information element indicates the result of the update of User Profile in the S-CSCF.

6.2.2.1 Detailed behaviour

The HSS shall make use of this procedure to update relevant user profile information in the S-CSCF.

The S-CSCF shall overwrite, for the identities indicated in the request, current information with the information received from the HSS. Table 6.2.2.1.1 details the valid result codes that the S-CSCF can return in the response.

Table 6.2.2.1.1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_SUCCESS_NOT SUPPORTED_USER_DATA	The request succeeded. However, the S-CSCF informs the HSS that the received subscription data contained information, which was not recognised or supported.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

6.3 Authentication procedures

This procedure is used between the S-CSCF and the HSS to exchange information to support the authentication between the end user and the home IMS network. The procedure is invoked by the S-CSCF, corresponds to the combination of the operations Cx-AV-Req and Cx-Put (see 3GPP TS 33.203 [3]) and is used:

- To retrieve authentication vectors from the HSS.
- To resolve synchronization failures between the sequence numbers in the UE and the HSS.

This procedure is mapped to the commands Multimedia-Auth-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.3.1 – 6.3.5 detail the involved information elements.

Table 6.3.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	This information element contains the public identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the user private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested

Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Tables 6.3.2 and 6.3.3 for the contents of this information element. The content shown in table 6.3.2 shall be used for a normal authentication request; the content shown in table 6.3.3 shall be used for an authentication request after synchronization failure.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name this AVP shall be present. This information is available if the MAR belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent in case of the initial registration. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the client.

Table 6.3.2: Authentication Data content – request

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	This information element indicates the authentication scheme. For 3GPP R5 it shall contain “Digest-AKAv1-MD5”.

Table 6.3.3: Authentication Data content – request, synchronization failure

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain “Digest-AKAv1-MD5”.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of nonce and AUTS, base 64 encoded. S-CSCF shall include the nonce sent to the terminal and the auts directive received from the terminal. See 3GPP TS 33.203 [3] for further details about RAND and AUTS. See [7] for further details about based 64 encoding. One example of content is: ‘nonce=” dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 ”, auts=”5ccc069c403ebaf9f0171e9517f40e41”’ where nonce “dcd98b7102dd2f0e8b11d0f600bfb0c093” contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1) and auts “5ccc069c403ebaf9f0171e9517f40e41” contains, base 64 encoded, AUTS.

Routing Information (See 7.13)	Destination-Host	M	In this case the MAR belongs to an already existing registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.

Table 6.3.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	User public identity
Private User Identity (See 7.3)	User-Name	M	User private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	Number of authentication vectors delivered
Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of the operation

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be included present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, Base 64 encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. One example of the format of the SIP-Authenticate AVP is: 'nonce=" dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 "' where the nonce " dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 " contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1).

Authorization Information (See 7.9.4)	SIP-Authorization	M	In shall contain, base 64 encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES. One example of the format of the SIP-Authorization AVP is: 'response="6629fae49393a05397450978507c4ef1"' where response="6629fae49393a05397450978507c4ef1" contains, base64 encoded, XRES.
Confidentiality Key (See 7.9.5)	NAS-Session-Key	O	This information element may contain the confidentiality key. NAS-Session-Key is a grouped AVP. When present the following describes its content: - NAS-Key-Direction equal to BIDIRECTIONAL. - NAS-Key-Type equal to CIPHER_KEY. - NAS-Key is the confidentiality key.
Integrity Key (See 7.9.6)	NAS-Session-Key	M	This information element shall contain the integrity key. NAS-Session-Key is a grouped AVP. When present the following describes its content: - NAS-Key-Direction equal to BIDIRECTIONAL. - NAS-Key-Type equal to INTEGRITY_KEY. - NAS-Key is the integrity key.

6.3.1 Detailed behaviour

The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the user exists in the HSS. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS may check that the private and public identities belong to the same user. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. Check that the authentication scheme indicated in the request is supported. If not Vendor-Specific-Result shall be set to DIAMETER_ERROR_AUTH_SCHEME_UNSUPPORTED.

4. If the request indicates there is a synchronization failure, the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

5. Check the registration status of the public identity received in the request:

   + If it is registered, the HSS shall return the requested authentication information to the S-CSCF. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

   + If it is not registered or if it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored), the HSS shall store the S-CSCF name. It will also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication and shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

   If the S-CSCF name received in the request is different from the one stored in the HSS, the HSS shall overwrite the stored S-CSCF name.

Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

6.4 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the I-CSCF and the S-CSCF to find the address of the HSS, that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS. An example for a single HSS solution is server farm architecture.

The resolution mechanism described in 3GPP TS 23.228 is based on the Subscription Locator Function (SLF). The subscription locator is accessed via the Dx interface. The Dx interface is always used in conjunction with the Cx interface. The Dx interface is based on Diameter. Its functionality is implemented by means of the routing mechanism provided by an enhanced Diameter redirect agent, which is able to extract the identity of the user from the received requests.

To get the HSS address the I-CSCF and the S-CSCF send to the SLF the Cx requests aimed for the HSS. On receipt of the HSS address from the SLF, the I-CSCF and S-CSCF shall send the Cx requests to the HSS. While the I-CSCF is stateless, the S-CSCF shall store the HSS address/name, as specified in 3GPP TS 23.228. Further requests associated to the same user shall make use the stored HSS address.

In networks where the use of the user identity to HSS resolution mechanism is required, each I-CSCF and S-CSCF shall be configured with the address/name of the SLF implementing this resolution mechanism.

6.5 Implicit registration

Implicit registration is the mechanism by which a user is allowed to register simultaneously more than one of his/her public identities. The HSS knows the identities that are to be implicitly registered when it receives the indication of the registration of an individual identity.

What follows is an extension of the affected basic procedures.

6.5.1 S-CSCF initiated procedures

The result of the S-CSCF initiated procedures affects all the public identities that are configured in the HSS to be registered implicitly.

6.5.1.1 Registration

The notification of a registration of a public identity affects all the public identities that are configured in the HSS to be registered implicitly. The profile information downloaded in the response contains the list of implicitly registered public identities. This allows the S-CSCF to know the implicitly registered public identities.

6.5.1.2 De-registration

The de-registration of a public identity implies the de-registration of all the corresponding implicitly registered public identities, both in the HSS and in the S-CSCF. The S-CSCF shall include in the request all the corresponding implicitly registered public identities.

6.5.2 HSS initiated procedures

6.5.2.1 User profile updating

A request sent by the HSS to update user profile information in the S-CSCF shall include all the corresponding public identities and their profile information.

6.5.2.2 De-registration

A request sent by the HSS to de-register a public identity shall include all the corresponding public identities.

6.6 Download of relevant user data

The download of the relevant user data from the HSS to the S-CSCF depends on whether the user data is already stored in the S-CSCF and/or on the user data requested from the S-CSCF and/or whether the requested user data is up-to-date in the S-CSCF.

If User-Data-Already-Available is set to USER_DATA_NOT_AVAILABLE the HSS shall download the requested profile, according to the value of User-Data-Request-Type.

If User-Data-Already-Available is set to USER_DATA_ALREADY_AVAILABLE and the requested profile is not up-to-date (according to the indications stored in HSS defined in 6.6.3) the HSS shall download the requested profile, according to the value of User-Data-Request-Type.

Otherwise, the HSS shall not return any user profile data.

6.6.1 HSS initiated update of User Profile

If the user is registered, the HSS shall immediately push to the S-CSCF the changes in the registered part of the user profile.

If the user is unregistered (i.e. registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall immediately push to the S-CSCF changes in the unregistered part of the user profile.

If the HSS has decided to keep the S-CSCF name after a de-registration and there is a change in the registered part of the user profile, the HSS shall set a flag indicating that the registered part of the profile is not up-to-date in the S-CSCF. The HSS shall not initiate any push toward the S-CSCF.

6.6.2 S-CSCF operation

The S-CSCF shall store the user data if it sends Server-Assignment-Request command including Server-Assignment-Type AVP set to value USER_DEREGISTRATION_STORE_SERVER_NAME or TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME and the HSS responds with DIAMETER_SUCCESS. Otherwise the S-CSCF shall not keep user data.

6.7 S-CSCF Selection by the I-CSCFAssignment

The list of mandatory and optional capabilities received by an I-CSCF from the HSS The contents of this IE shall allows operators to distribute users between S-CSCFs attending to mandatory and optional capabilities required per user by each operator, depending on the different capabilities (features, role, etc.) that each S-CSCF may have. Alternatively, an operator has the possibility to steer users to certain S-CSCFs.

The operator shall define (possibly based on the functionality offered by each S-CSCF installed in the network) the exact meaning of the mandatory and optional capabilities. It is a configuration task for the operator to ensure that the I-CSCF has a correct record of the capabilities of each S-CSCF available in his network. The I-CSCF does not need to know the semantic of the capabilities received from the HSS. This semantic is exclusively an operator issue.

The I-CSCF shall match the required capabilities to the capabilities of each S-CSCF of which it has knowledge. As a first choice, tThe I-CSCF shall first try to select an S-CSCF that has all the mandatory and optional capabilities required for the subscriberuser. Only if that is not possible shall the I-CSCF apply a ‘best-fit’ algorithm. If more than one S-CSCF is identified that supports all mandatory capabilities the I-CSCF may then consider optional capabilities in selecting a specific S-CSCF. The ‘best-fit’ algorithm is implementation dependent and out of the scope of this specification.

The operator shall define (possibly based on the functionality offered by each S-CSCF installed in the network) the exact meaning of the mandatory and optional capabilities. It is a configuration task for the operator to ensure that the I-CSCF has a correct record of the capabilities of each S-CSCF available in his network. The I-CSCF does not need to know the semantic of the capabilities received from the HSS. This semantic is exclusively an operator issue.

It is the responsibility of the operator to ensure that there are S-CSCFs which have the meet the “mandatory” requirements capabilities indicated by the HSS for any given user. However, configuration errors may occur. If such

errors occur and they prevent the I-CSCF from selecting an S-CSCF which meets the “mandatory” requirementscapabilities indicated by the HSS, the I-CSCF shall inform the HSS via the O&M subsystem.

In additionAlternatively to the possibility As an alternative to selecting an S-CSCF based on the list of capabilities received from the HSS, it is possible to steer users to certain S-CSCFs. In order toTo do this, the operator wouldmay include one or more S-CSCF names as part of the capabilities of the user profile. This is an operator issue; tThe reason for the selection (e.g. all the users belonging to the same company/group could be in the same S-CSCF to implement a VPN service) and the method of selection are operator issues and out of the scope of this specification.

7 Information element contents

7.1 Visited Network Identifier

This information element contains the domain name of the visited network.

7.2 Public User Identity

This information element contains the public identity of the user.

7.3 Private User Identity

This information element contains the private identity of the user.

7.4 S-CSCF Name

This information element contains the SIP Address of S-CSCF.

7.5 S-CSCF Capabilities

This information element carries information to assist the I-CSCF during the process of selecting an S-CSCF for a certain user.

7.6 Result

This information element contains result of an operation. See 3GPP TS 29.229 [5] for the possible values.

7.7 User Profile

This information element contains the profile of a user as an XML documents conformant to the XML schema defined in Annex D.

Annex B specifies the UML logical model of the user profile downloaded via the Cx interface.

Annex C contains and informative, high level representation, of the wire representation of user profile data.

7.8 Server Assignment Type

Indicates the type of server assignment. See 3GPP TS 29.229 [5] for the list of existing values.

7.9 Authentication Data

This information element is composed of the following sub-elements.

7.9.1 Item Number

This information element indicates the order in which the authentication vectors are to be consumed.

7.9.2 Authentication Scheme

This information element contains the authentication scheme, which is used to encode the authentication parameters.

For 3GPP Release 5 this scheme is “Digest-AKAv1-MD5”.

7.9.3 Authentication Information

This information element is used to convey the challenge and authentication token user during the authentication procedure. See 3GPP TS 33.203 [3] for details.

7.9.4 Authorization Information

This information element is used, in an authentication request, to indicate a failure of synchronization. In a response, it is used to convey the expected response to the challenge used to authenticate the user. See 3GPP TS 33.203 [3].

7.9.5 Confidentiality Key

This information element contains the confidentiality key. See 3GPP TS 33.203 [3].

7.9.6 Integrity Key

This information element contains the integrity key. See 3GPP TS 33.203 [3].

7.10 Number Authentication Items

This information element contains the number of authentication vectors requested or delivered.

7.11 Reason for de-registration

This information element contains the reason for a de-registration procedure.

7.12 Charging information

Addresses of the charging functions (primary event charging function name, secondary event charging function name, primary charging collection function name, primary charging collection function name).

7.13 Routing information

Information to route requests.

7.14 Type of authorization

Type of authorization requested by the I-CSCF. See 3GPP TS 29.229 [5] for a list of values.

7.15 User Data Request Type

Part of the user profile the S-CSCF requests from the HSS. See 3GPP TS 29. 229 [5] for a list of values.

7.16 User Data Already Available

This information element indicates to the HSS if the user profile is already available in the S-CSCF. See 3GPP TS 29. 229 [5] for a list of values.

8 Error handling procedures

8.1 Registration error cases

This section describes the handling of the error, which can occur during the registration process, by which the name of the S-CSCF received in a request is different from the one stored in HSS.

8.1.1 Cancellation of the old S-CSCF

It is possible that in certain situations the HSS receives a Multimedia-Auth-Request (MAR) command including a S-CSCF name, which is not the same as the previously assigned S-CSCF for the user. This can happen e.g. in case the new S-CSCF is selected due to a failure in the re-registration if the previously assigned S-CSCF does not respond to REGISTER message sent from the I-CSCF after a timeout.

In this case the new S-CSCF is assigned for the user and if registrations in the previously assigned S-CSCF exist for the user, these registrations in the old S-CSCF are handled locally in the old S-CSCF, e.g. re-registration timers in the old S-CSCF will cancel the registrations. Alternatively, the HSS may de-register the registrations in the old S-CSCF by using the Registration-Termination-Request command. In this case the de-registration must be done in the following order:

1. Deregistration-Reason AVP value set to NEW_SERVER_ASSIGNED, for the public identity, which is registered in the new S-CSCF.

2. Deregistration-Reason AVP value set to SERVER_CHANGE, for the user public identities, which are not registered in the new S-CSCF.

8.1.2 Error in S-CSCF name

If the new and previously assigned S-CSCFs are different, the HSS shall not overwrite the S-CSCF name unless it is sent in the Multimedia-Auth-Request command but send a response to the S-CSCF indicating error. The Result-Code value is set to:

- DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED if the S-CSCF name sent in the Server-Assignment-Request command is different than assigned S-CSCF name, and therefore the request cannot be successfully processed.

- DIAMETER_ERROR_IN_ASSIGNMENT_TYPE if the S-CSCF name sent in the Server-Assignment-Request command is the same S-CSCF name as the assigned S-CSCF name, but Server-Assignment-Type is not allowed, e.g. the user is registered and the S-CSCF sends Server-Assignment-Request indicating the assignment for the unregistered user.

9 Protocol version identification

See 3GPP TS 29.229 [5].

10 Operational Aspects

See 3GPP TS 29.229 [5].

Annex A (normative): Mapping of Cx operations and terminology to Diameter

A.1 Introduction

This appendix gives mappings from Cx to Diameter protocol elements. Diameter protocol elements are defined in 3GPP TS 29.229 [5].

A.2 Cx message to Diameter command mapping

The following table defines the mapping between stage 2 operations and Diameter commands:

Table A.2.1: Cx message to Diameter command mapping

Cx message	Source	Destination	Command-Name	Abbreviation
Cx-Query + Cx-Select-Pull	I-CSCF	HSS	User-Authorization-Request	UAR
Cx-Query Resp + Cx-Select-Pull Resp	HSS	I-CSCF	User-Authorization-Answer	UAA
Cx-Put + Cx-Pull	S-CSCF	HSS	Server-Assignment-Request	SAR
Cx-Put Resp + Cx-Pull Resp	HSS	S-CSCF	Server-Assignment-Answer	SAA
Cx-Location-Query	I-CSCF	HSS	Location-Info-Request	LIR
Cx-Location-Query Resp	HSS	I-CSCF	Location-Info-Answer	LIA
Cx-AuthDataReq	S-CSCF	HSS	Multimedia-Authentication-Request	MAR
Cx-AuthDataResp	HSS	S-CSCF	Multimedia-Authentication-Answer	MAA
Cx-Deregister	HSS	S-CSCF	Registration-Termination-Request	RTR
Cx-Deregister Resp	S-CSCF	HSS	Registration-Termination-Answer	RTA
Cx-Update_Subscr_Data	HSS	S-CSCF	Push-Profile-Request	PPR
Cx-Update_Subscr_Data Resp	S-CSCF	HSS	Push-Profile-Answer	PPA

A.3 Cx message parameters to Diameter AVP mapping

The following table gives an overview about the mapping:

Table A.3.1: Cx message parameters to Diameter AVP mapping

Cx parameter	AVP Name
Visited Network Identifier	Visited-Network-Identifier
Public User ID	Public-Identity
Private User ID	User-Name
S-CSCF name	Server-Name
S-CSCF capabilities	Server-Capabilities
Result	Result-Code / Vendor-Specific-Result
User profile	User-Data
Server Assignment Type	Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item Number	SIP-Item-Number
Authentication Scheme	SIP-Authentication-Scheme
Authentication Information	SIP-Authenticate
Authorization Information	SIP-Authorization
Confidentiality Key	NAS-Session-Key
Integrity Key	NAS-Session-Key
Number Authentication Items	SIP-Number-Auth-Items
Reason for de-registration	Deregistration-Reason
Charging Information	Charging-Information
Routing Information	Destination-Host
Type of Authorization	Authorization-Type

A.4 Message flows

The following message flows give examples regarding which Diameter messages shall be sent in scenarios described in 3GPP TS 23.228 [1].

A.4.1 Registration– user not registered

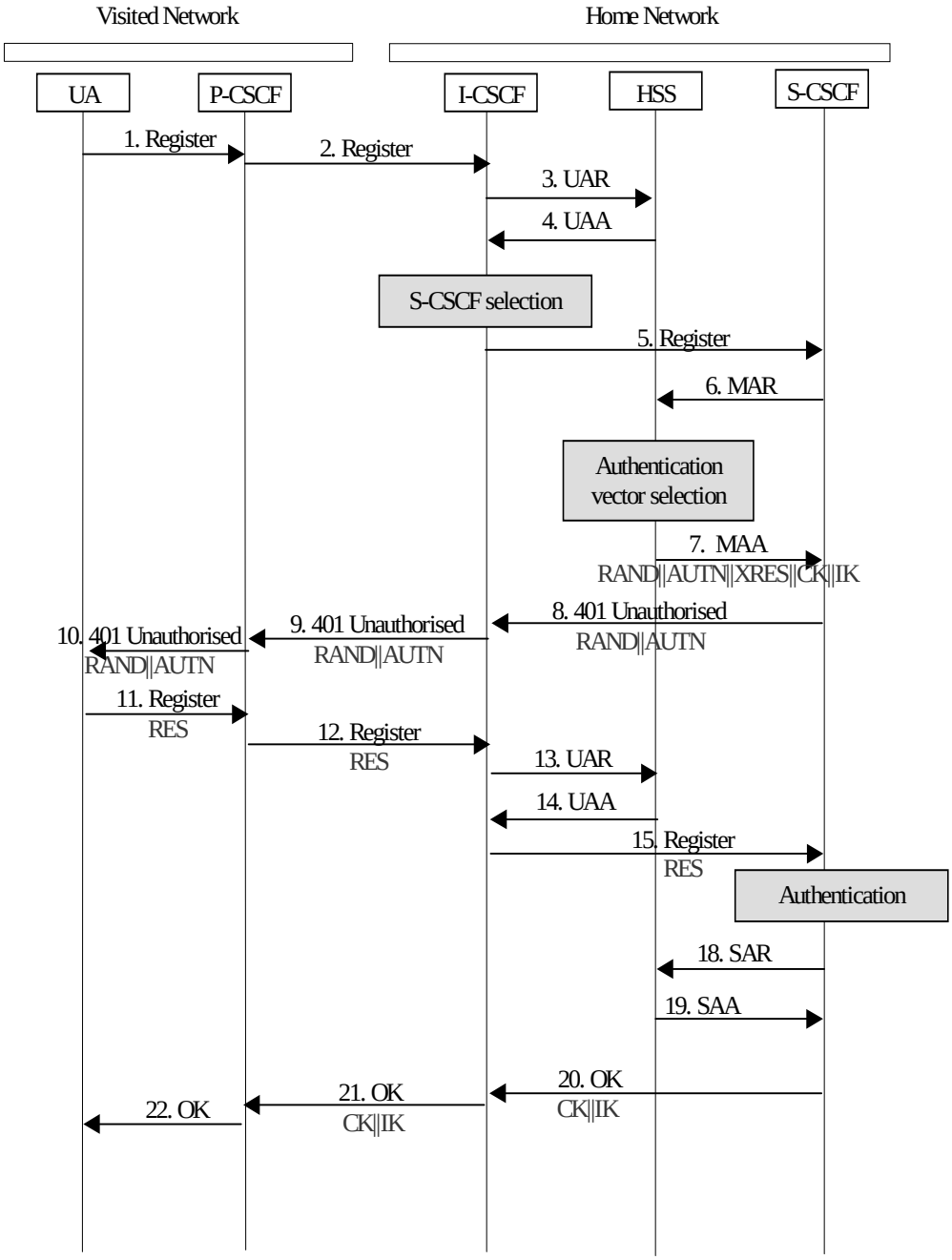


Figure A.4.1.1: Registration – user not registered

A.4.2 Registration – user currently registered

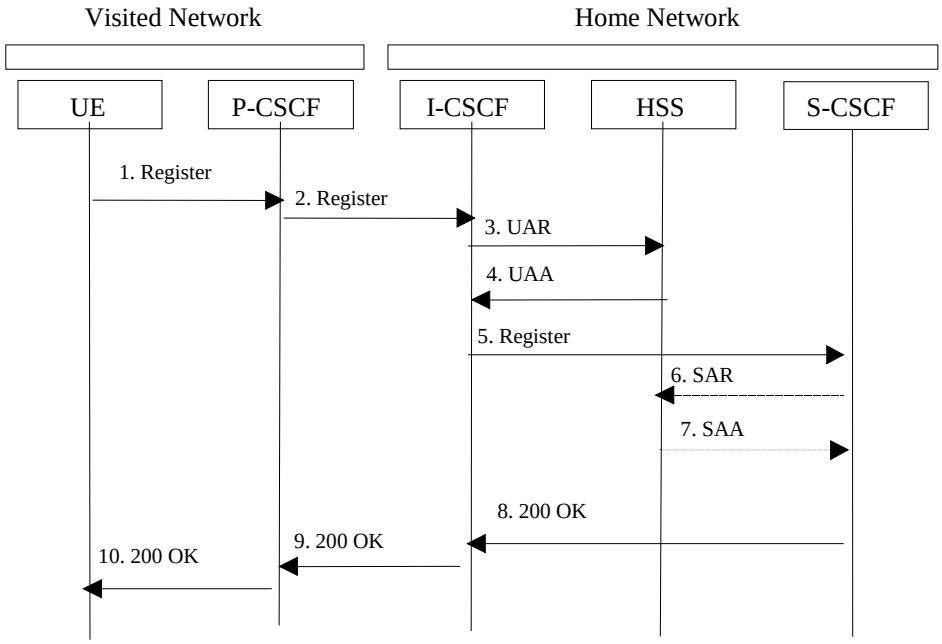


Figure A.4.2.1: Re-registration

A.4.3 Mobile initiated de-registration

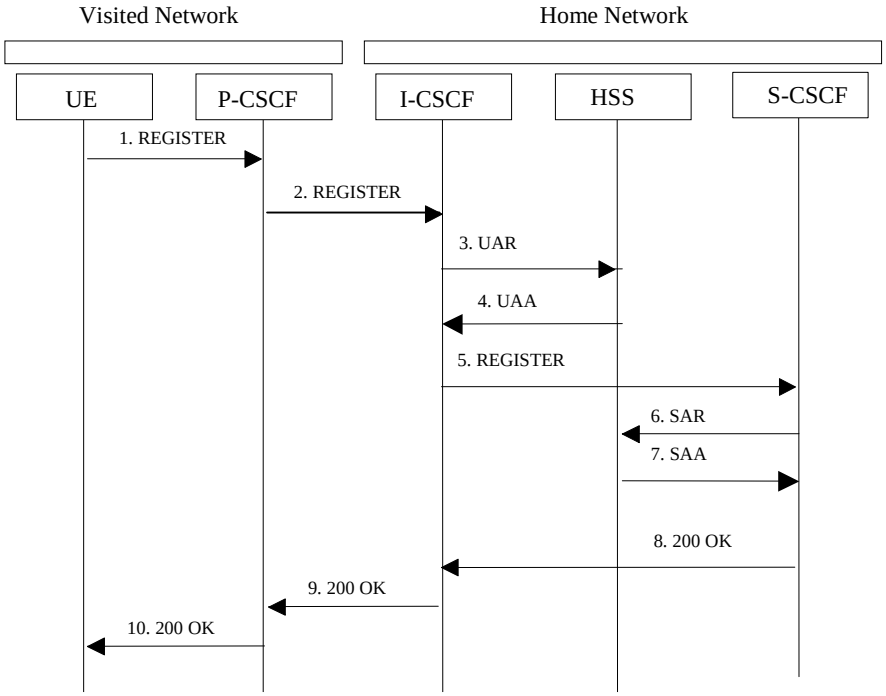


Figure A.4.3.1: Mobile initiated de-registration

A.4.4 Network initiated de-registration

A.4.4.1 Registration timeout

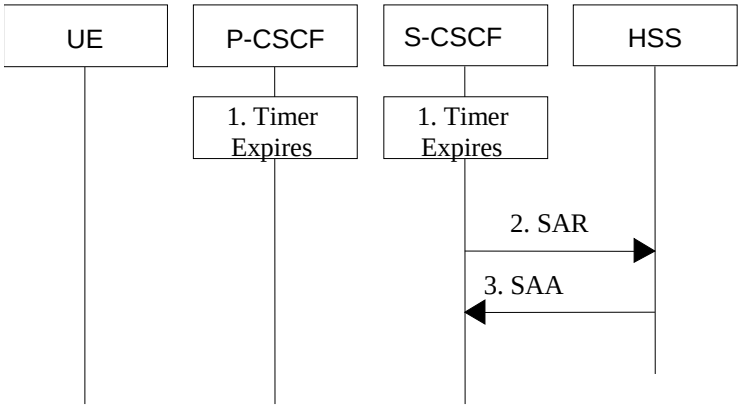


Figure A.4.4.1.1: Network initiated de-registration – registration timeout

A.4.4.2 Administrative de-registration

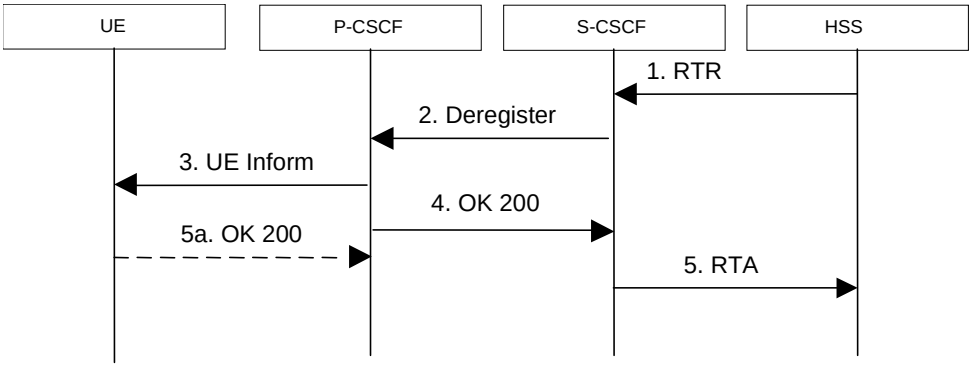


Figure A.4.4.2.1: Network initiated de-registration – administrative de-registration

A.4.4.3 De-registration initiated by service platform

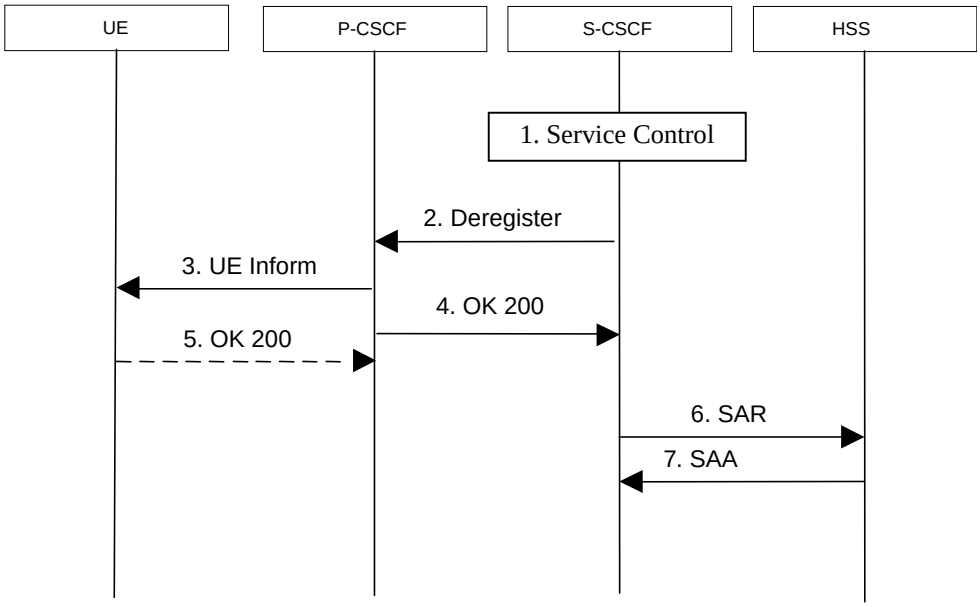


Figure A.4.4.3.1: Network initiated de-registration – initiated by service platform

A.4.5 MT SIP session set-up

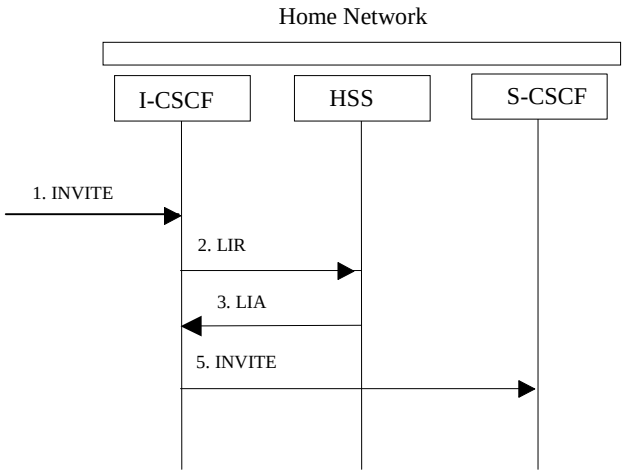


Figure A.4.5.1: MT SIP session set-up

A.4.6 Initiation of a session to a non-registered user

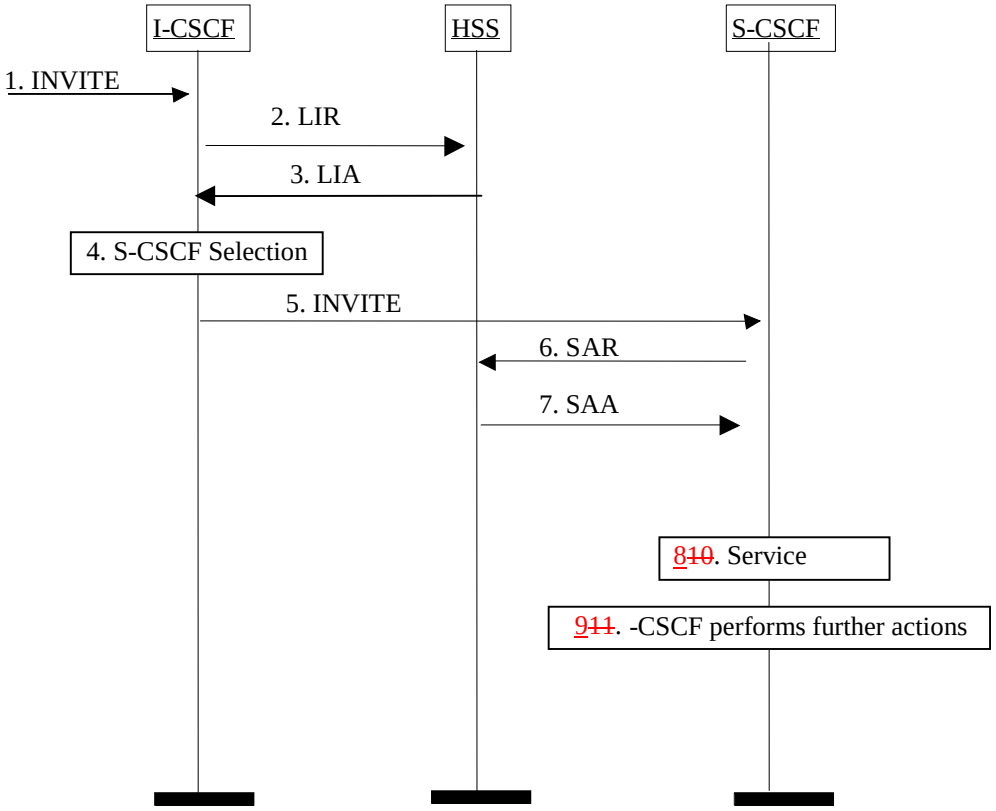


Figure A.4.6.1: Initiation of a session to a non-registered user

A.4.7 User Profile update

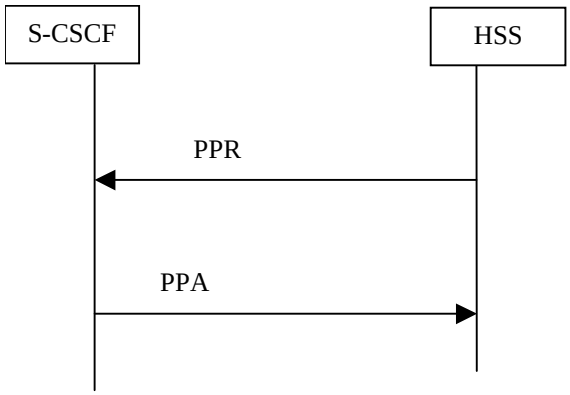


Figure A.4.7.1: User profile update

Annex B (informative): User profile UML model

The purpose of this UML model is to define in an abstract level the structure of the user profile downloaded over the Cx interface and describe the purpose of the different information classes included in the user profile.

B.1 General description

The following picture gives an outline of the UML model of the user profile, which is downloaded from HSS to S-CSCF:

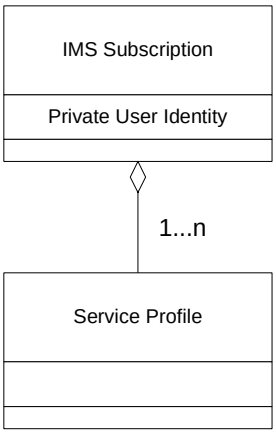


Figure B.1.1: User Profile

IMS Subscription class contains as a parameter the private user identity of the user in NAI format.

Each instance of the IMS Subscription class contains one or several instances of the class Service Profile. Service Profile class contains the meaningful data in the user profile: Public Identification, Core Network Service Authorization and Initial Filter Criteria.

B.2 Service profile

The following picture gives an outline of the UML model of the Service Profile class:

:

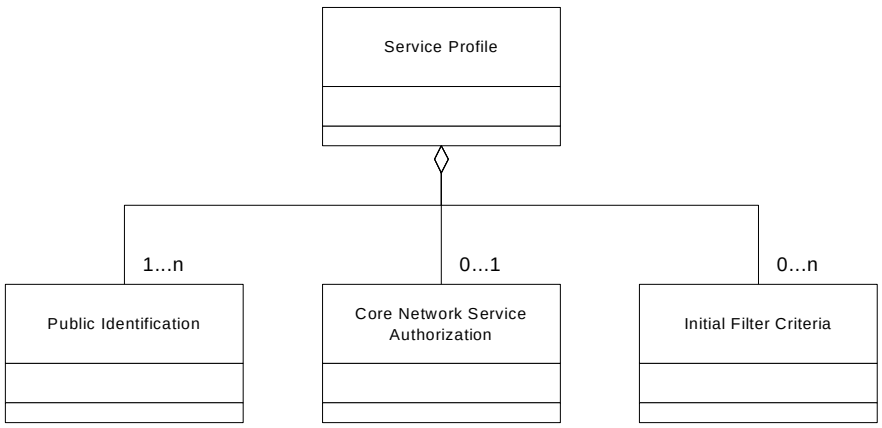


Figure B.2.1: Service Profile

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

Each instance of the Service Profile class contains zero or one instance of the class Core Network Service Authorization.

Editor's Note: The content of this information element is FFS. The intention is that it can be used to carry information that can be forced at CN level like, e.g. the maximum number or simultaneous multimedia sessions of a user.

Each instance of the class Service Profile contains zero or several instances of the class Initial Filter Criteria.

B.2.1 Public Identification

The following picture gives an outline of the UML model of Public Identification class:

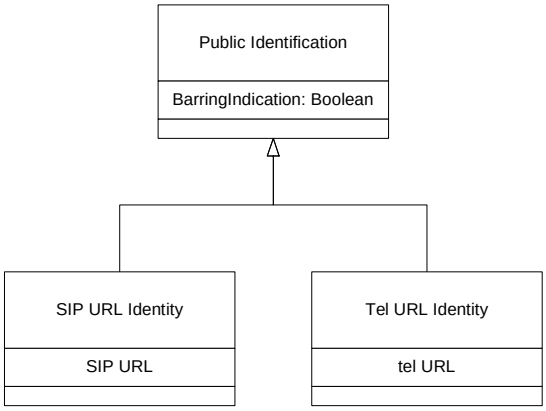


Figure B.2.1.1: Public Identification

Public Identification class can contain either SIP URL Identity, i.e. SIP URL, or Tel URL Identity class, i.e. tel URL.

The attribute BarringIndication is of type Boolean. If it is set to TRUE, the S-CSCF shall prevent that public identity from being used to establish multimedia sessions (both originating and terminating sessions are barred).

B.2.2 Initial Filter Criteria

The following picture gives an outline of the UML model of Initial Filter Criteria class:

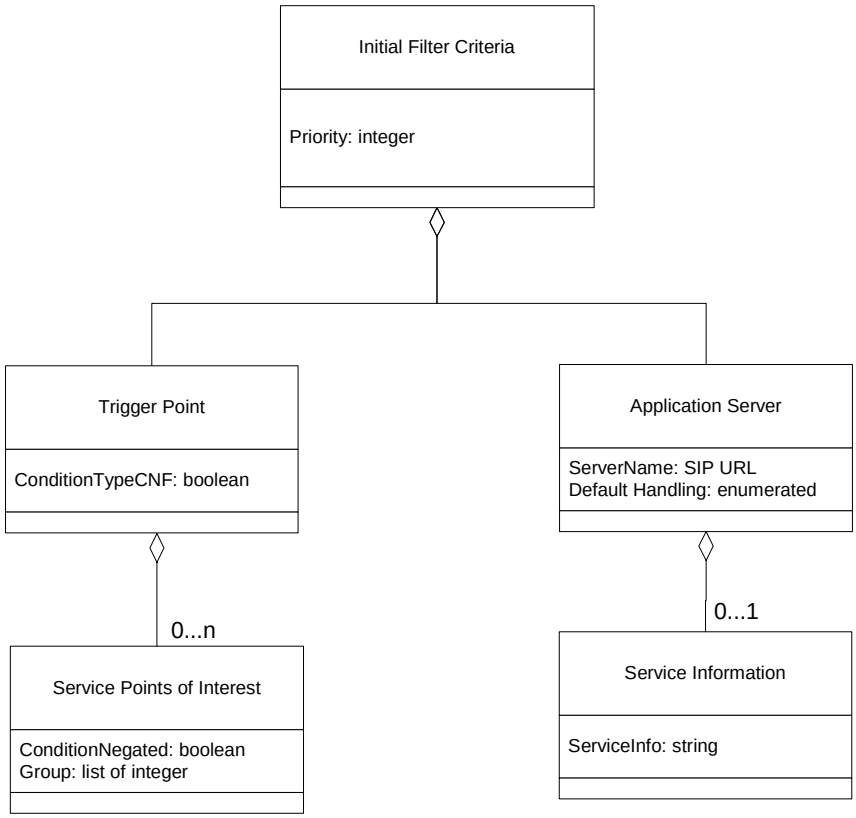


Figure B.2.2.1.1: Initial Filter Criteria

Each instance of the Initial Filter Criteria class is composed of one instance of a Trigger Point class and one instance of an Application Server class. FilterID identifies the particular instance of the Filter Criteria class. Priority indicates the priority of the Filter Criteria. The higher the Priority Number the lower the priority of the Filter Criteria is; i.e., a Filter Criteria with a higher value of Priority Number shall be assessed after the Filter Criteria with a smaller Priority Number have been assessed. The same priority shall not be assigned to more than one AS. ConditionTypeCNF is a boolean that is TRUE when the Trigger Point associated with the FilterCriteria is a boolean expresion in Conjuctive Normal Form (CNF) and FALSE if the Trigger Point is expressed in Disjunctive Normal Form (DNF) (see Annex C).

Trigger Point class describes the trigger points that should be checked in order to find out if the indicated Application Server should be contacted or not. Each TriggerPoint is a boolean expression in Conjuctive or Disjunctive Normal form (CNF of DNF).

The attribute ConditionTypeCNF attribute defines how the set of SPIs are expressed, i.e. either an Ored set of ANDed sets of SPI statements or an ANDed set of Ored sets of statements. Individual SPI statements can also be negated. These combinations are termed, respectively, Disjunctive Normal Form (DNF) and Conjunctive Normal Form (CNF) for the SPI (see Annex C). Both DNF and CNF forms can be used.

Each Trigger Point is composed by 0 to n instances of the class Service Points of Interest.

Application Server class defines the application server, which is contacted, if the trigger points are met. Server Name is the SIP URL of the application server to contact. Default Handling determines whether the dialog should 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. Service Information class allows to download to S-CSCF information that is to be transferred transparently to an Application Server when the trigger points of a filter criterion are satisfied. ServiceInformation is a string conveying that information. See 3GPP TS 23.218 [7] for a description of the use of this information element.

B.2.3 Trigger Point

The following picture gives an outline of the UML model of Filter Criteria class:

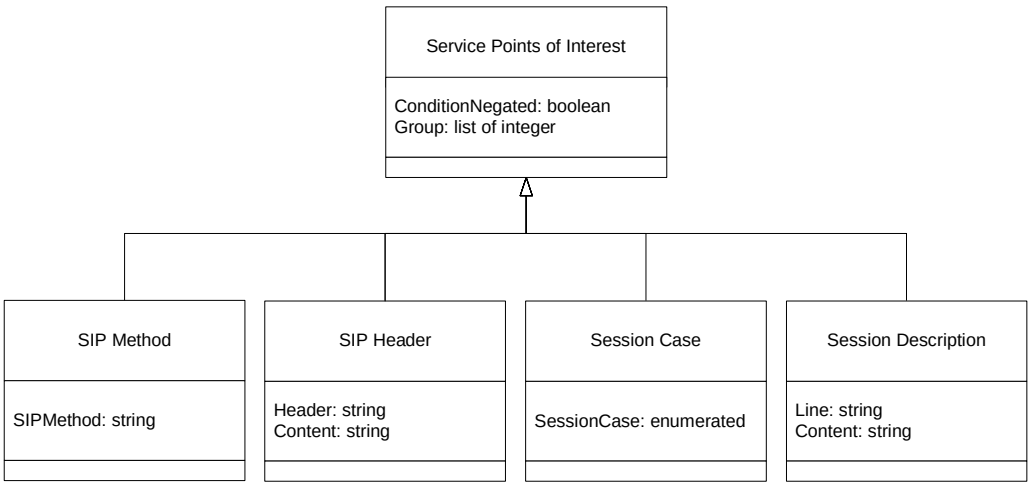


Figure B.2.3.1: Trigger Point

The attribute Group of the class Service Points of Interest allows the grouping of SPIs that will configure the sub-expressions inside a CNF or DNF expression. For instance, in the following CNF expression (A+B).(C+D), A+B and C+D would correspond to different groups.

In CNF, the attribute Group identifies the Ored sets of SPI instances. If the SPI belongs to different Ored sets, SPI can have more than one Group values assigned. At least one Group must be assigned for each SPI.

In DNF, the attribute Group identifies the ANDed sets of SPI instances. If the SPI belongs to different ANDed sets, SPI can have more than one Group values assigned. At least one Group must be assigned for each SPI.

The attribute ConditionNegated of the class Service Points of Interest defines whether the individual SPI instance is negated (i.e. NOT logical expression).

SIP Method class defines SPI for the SIP method. SIP Method contains attribute SIPMethod which can evaluate to any existent SIP method.

SIP Header class defines SPI for the presence or absence of any SIP header or for the content of any SIP header. SIP Header contains attribute SIP Header which identifies the SIP Header, which is the SPI, and the Content attribute defines the value of the SIP Header if required. The value of the Content attribute is a string that shall be interpreted as a regular expression. Perl-like regular expressions shall be taken as a model for legal regular expressions for this function. A regular expression would be as simple as a literal (e.g. “john”) or a more elaborated one, allowing to match a string “containing” a substring, beginning with a substring, etc. Examples of regular expressions valid for the “Match” attribute could be:

(1 “Joe”: meaning that a given header matches exactly with the string “Joe”.

(1 “^(Jo).*”: meaning that a given header contains a value that begins with “Jo”.

(1 “.*Jo.*”: meaning that a given header contais the substring “Jo” at any possition.

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

Session Case class represents an enumerated type, with possible values “Originating”, “Terminating”, “Terminating_Unregistered” indicating if the filter should be used by the S-CSCF handling the Originating, Terminating or Terminating for an unregistered end user services.

Session Description Information class defines SPI for the content of any SDP field within the body of a SIP Method. The Line attribute identifies the line inside the session description. Content is a string defining the content of the line

identified by Line. Perl-like regular expressions shall be taken as a model for regular expressions for this function (as described above).

Annex C (informative): Conjunctive and Disjunctive Normal Form

A Trigger Point expression is constructed out of atomic expressions (i.e. Service Points of Interest) linked by Boolean operators AND, OR and NOT. Any logical expression constructed in that way can be transformed to forms called Conjunctive Normal Form (CNF) and Disjunctive Normal Form (DNF).

A Boolean expression is said to be in Conjunctive Normal Form if it is expressed as a conjunction of disjunctions of literals (positive or negative atoms), i.e. as an AND of clauses, each of which is the OR of one of more atomic expressions.

Taking as an example the following trigger:

Method = “INVITE” OR Method = “MESSAGE” OR (Method=”SUBSCRIBE” AND NOT Header = “from” Match = “joe”)

The trigger can be split into the following atomic expressions:

- Method=”INVITE”
- Method=”MESSAGE”
- Method=”SUBSCRIBE”
- NOT header=”from” Match=”joe”

Grouping the atomic expressions, the CNF expression equivalent to the previous example looks like:

(Method=”INVITE” OR Method = “MESSAGE” OR Method=”SUBSCRIBE”) AND (Method=”INVITE” OR Method = “MESSAGE” OR (NOT Header = “from” Match = “joe”))

This result in two “OR” groups linked by “AND” (CNF):

- (Method=”INVITE” OR Method = “MESSAGE” OR Method=”SUBSCRIBE”)
- (Method=”INVITE” OR Method = “MESSAGE” OR (NOT Header = “from” Content = “joe”))

The XML representation of the trigger is:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<testDatatype xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xsi:noNamespaceSchemaLocation=”D:\
\CxDataType.xsd”>
        <IMSSubscription>
        <PrivateID index=”0”>IMPI1@homedomain.com</PrivateID>
        <ServiceProfile index=”0”>
                <PublicIdentity index=”0”>
                        <BarringIndication index=”0”>1</BarringIndication>
                        <Identity index=”0”> sip:IMPU1@homedomain.com </Identity>
                </PublicIdentity>
                <PublicIdentity index=”0”>
                        <Identity index=”0”> sip:IMPU2@homedomain.com </Identity>
                </PublicIdentity>
”””””           <InitialFilterCriteria index=”0”>
””                      <Priority index=”0”>0</Priority>
                        <TriggerPoint index=”0”>
                                <ConditionTypeCNF index=”0”>1</ConditionTypeCNF>
                                <SPI index=”0”>
                                        <ConditionNegated index=”0”>0</ConditionNegated>
                                        <Group index=”0”>0</Group>
                                        <Method index=”0”>INVITE</Method>
                                </SPI>
                                <SPI index=”0”>
                                        <ConditionNegated index=”0”>0</ConditionNegated>
                                        <Group index=”0”>0</Group>
                                        <Method index=”0”>MESSAGE</Method>
```

```
                                    </SPI>
                                    <SPI index=”0”>
                                            <ConditionNegated index=”0”>0</ConditionNegated>
                                            <Group index=”0”>0</Group>
                                            <Method index=”0”>SUBSCRIBE</Method>
                                    </SPI>
                                    <SPI index=”0”>
                                            <ConditionNegated index=”0”>0</ConditionNegated>
                                            <Group index=”0”>1</Group>
                                            <Method index=”0”>INVITE</Method>
                                    </SPI>
                                    <SPI index=”0”>
                                            <ConditionNegated index=”0”>0</ConditionNegated>
                                            <Group index=”0”>1</Group>
                                            <Method index=”0”>MESSAGE</Method>
                                    </SPI>

                                    <SPI index=”0”>
                                            <ConditionNegated index=”0”>1</ConditionNegated>
                                            <Group index=”0”>1</Group>
                                            <SIPHeader index=”0”>
                                                    <Header index=”0”>From</Header>
                                                    <Content index=”0”>”joe”</Content>
                                            </SIPHeader>
                                    </SPI>
                            </TriggerPoint>
                            <ApplicationServer index=”0”>
                                    <ServerName index=”0”>sip:AS1@homedomain.com</ServerName>
                                    <DefaultHandling index=”0”>0</DefaultHandling>
                            </ApplicationServer>
                    </InitialFilterCriteria>
            </ServiceProfile>
            </IMSSubscription>
</testDatatype>
```

A Boolean expression is said to be in Disjunctive Normal Form if it is expressed as a disjunction of conjuctions of literals (positive or negative atoms), i.e. as an OR of clauses, each of which is the AND of one of more atomic expressions.

The previous example is already in DNF, composed by the following groups:

- Method=”INVITE”
- Method=”MESSAGE”
- Method=”SUBSCRIBE” AND (NOT header=”from” Match=”joe”)

The XML representation of the trigger is:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<testDatatype xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xsi:noNamespaceSchemaLocation=”D:\
CxDataType.xsd”>
        <IMSSubscription>
        <PrivateID index=”0”>IMPI1@homedomain.com</PrivateID>
        <ServiceProfile index=”0”>
                <PublicIdentity index=”0”>
                        <BarringIndication index=”0”>1</BarringIndication>
                        <Identity index=”0”> sip:IMPU1@homedomain.com </Identity>
                </PublicIdentity>
                <PublicIdentity index=”0”>
                        <Identity index=”0”> sip:IMPU2@homedomain.com </Identity>
                </PublicIdentity>””””””
                <InitialFilterCriteria index=”0”>
””                      <Priority index=”0”>0</Priority>
                        <TriggerPoint index=”0”>
```

```
                        <ConditionTypeCNF index=”0”>0</ConditionTypeCNF>
                        <SPI index=”0”>
                                <ConditionNegated index=”0”>0</ConditionNegated>
                                <Group index=”0”>0</Group>
                                <Method index=”0”>INVITE</Method>
                        </SPI>
                        <SPI index=”0”>
                                <ConditionNegated index=”0”>0</ConditionNegated>
                                <Group index=”0”>1</Group>
                                <Method index=”0”>MESSAGE</Method>
                        </SPI>
                        <SPI index=”0”>
                                <ConditionNegated index=”0”>0</ConditionNegated>
                                <Group index=”0”>2</Group>
                                <Method index=”0”>SUBSCRIBE</Method>
                        </SPI>
                        <SPI index=”0”>
                                <ConditionNegated index=”0”>1</ConditionNegated>
                                <Group index=”0”>2</Group>
                                <SIPHeader index=”0”>
                                        <Header index=”0”>From</Header>
                                        <Content index=”0”>”joe”</Content>
                                </SIPHeader>
                        </SPI>
                </TriggerPoint>
                <ApplicationServer index=”0”>
                        <ServerName index=”0”>sip:AS1@homedomain.com</ServerName>
                        <DefaultHandling index=”0"">0</DefaultHandling>
                </ApplicationServer>
        </InitialFilterCriteria>
</ServiceProfile>
</IMSSubscription>
</testDatatype>
```

Annex D (informative): High-level format for the User Profile

The way the information will be transferred through the Cx interface can be seen from a high-level point of view in the following picture:

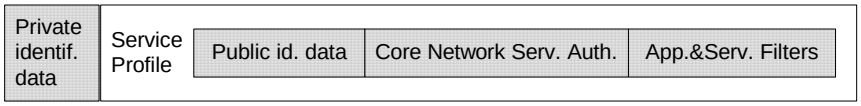


Figure C.1: Example of in-line format of user profile

If more than one service profile is created, for example to assign a different set of filters to public identifiers 1 and 2 and public identity 3, the information will be packaged in the following way:

Figure C.2: Example of in-line format of user profile

Annex E (normative): XML schema for the Cx interface user profile

The file CxDataType.xsd, attached to this specification, contains the XML schema for the Cx interface user profile. Such XML schema details all the data types on which XML documents containing Cx profile information shall be based. The XML schema file is intended to be used by an XML parser.

Table E.1 describes the data types and the dependencies among them that configure the XML schema.

Table E.1: XML schema for Cx interface: simple data types

Data type	Tag	Base type	Comments
tPriority	Priority	integer	>= 0
tGroupID	Group	integer	>= 0
tDefaultHandling	DefaultHandling	enumerated	Possible values: 0 (SESSION_CONTINUED) 1 (SESSION_TERMINATED)
tDirectionOfRequest	SessionCase	enumerated	Possible values: 0 (ORIGINATING_SESSION) 1 TERMINATING_SESSION 2 (TERMINATING_UNREGISTERED)
tPrivateID	PrivateID	anyURI	Syntax described in RFC 2486
tSIP_URL	PublicIdentity	anyURI	Syntax described in RFC 3261
tTEL_URL	PublicIdentity	anyURI	Syntax described in RFC 2806
tPublicIdentity	PublicIdentity	(union)	Union of tSIP_URL and tTEL_URL
tServiceInfo	ServiceInfo	string	
tString	Method, Header, Content, Line	string	
tBool	ConditionTypeCNF, ConditionNegated	enumerated	Possible values: 0 (FALSE) 1 (TRUE)

Table E.2: XML schema for Cx interface: complex data types

Data type	Tag	Compound of		
		Tag	Type	Cardinality
tIMSSubscription	IMSSubscription	PrivateID	tPrivateID	1
		ServiceProfile	tServiceProfile	(1 to 20)
tServiceProfile	ServiceProfile	PublicIdentity	tPublicIdentity	(1 to 20)
		InitialFilterCriteria	tInitialFilterCriteria	(1 to 10)
tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1
		TriggerPoint	tTrigger	(0 to 1)
		ApplicationServer	tApplicationServer	1
tTrigger	Trigger	SPI	tSiPoInt	(0 to 25)
		ConditionTypeCNF	tBool	1
tSiPoInt	SPI	ConditionNegated	tBool	(0 to 1)
		Group	tGroupID	(1 to 25)
		Choice of: Method	tString	1
		Choice of: SIPHeader	tHeader	1
		Choice of: SessionCase	tDirectionOfRequest	1
		Choice of: SessionDescription	tSessionDescription	1
tHeader	SIPHeader	Header	tString	1
		Content	tString	(0 to 1)
tSessionDescription	SessionDescription	Line	tString	1
		Content	tString	(0 to 1)
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	(0 to 1)
		ServiceInfo	tServiceInfo	(0 to 1)

Annex F (informative): XML document for the Cx interface user profile

The file CxDataTypes.xml, attached to this specification, contains the XML document with the data description for Cx interface, compliant with the Data Description Framework.

Annex G (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Jun 2002	CN#16	NP-020264			Version 2.0.0 approved at CN#16	2.0.0	5.0.0

History

Document history		
V5.0.0	June 2002	Publication