ETSI TS 129 228 V5.12.0 (2005-06)

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 5.12.0 Release 5)**

Reference
RTS/TSGC-0429228v5c0

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

Intellectual Property Rights

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

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

Foreword

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

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

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

Contents

Foreword

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

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

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

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.

[8] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP" – stage 3

[9] IETF RFC 3588 "Diameter Base Protocol"

[10] IETF RFC 3261 "SIP: Session Initiation Protocol"

[11] IETF RFC 2327 "SDP: Session Description Protocol"

[12] IEEE 1003.1-2004, Part 1: Base Definitions

[13] IETF RFC 2617 "HTTP Authentication: Basic and Digest Access Authentication"

3 Definitions, symbols and abbreviations

3.1 Definitions

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

Common Part (of a user profile): Contains Initial Filter Criteria instances that should be evaluated both for registered and unregistered Public User Identities in the S-CSCF.

Complete user profile: Contains the Initial Filter Criteria instances of all three different user profile parts; registered part, unregistered part and common part.

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

Charging information: Data that is sent in the Charging-Information AVP.

Implicitly registered Public User identity set: A set of Public User Identities, which are registered and de-registered simultaneously when any of the Public User Identities belonging to that set is registered or de-registered.

Not Registered State: User is not Registered and has no S-CSCF assigned.

Registered Part (of a user profile): Contains Initial Filter Criteria instances that should be evaluated only for registered Public User Identities in the S-CSCF. iFCs from the registered part need not be evaluated when the user is unregistered.

Registered State: User is Registered at the request of the user and has an S-CSCF assigned.

Unregistered part (of a user profile): Contains Initial Filter Criteria instances that should be evaluated only for unregistered Public User Identities in the S-CSCF. iFCs from the unregistered part need not be evaluated when the user is registered.

Unregistered State: User is not Registered but has a serving S-CSCF assigned to execute Unregistered state services as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored.

User information: The user related data that the S-CSCF requests from the HSS or HSS pushes to the S-CSCF, e.g. user profile and charging information.

User profile: Data that is sent in the User-Data AVP.

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, (C) Conditional or (O) Optional.

- A mandatory Information Element (marked as (M) in the table) shall always be present in the command. If this Information Element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.
- A conditional Information Element (marked as (C) in the table) shall be present in the command if certain conditions are fulfilled.
  - If the receiver detects that those conditions are fulfilled and the Information Element is absent, an application error occurs and an answer message shall be sent back to the originator of the request with the Result-Code

set to DIAMETER_MISSING_AVP. This answer message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.

- If those conditions are not fulfilled, the Information Element shall be absent. If however this Information Element appears in the message, it shall not cause an application error and it may be ignored by the receiver if this is not explicitly defined as an error case. Otherwise, an application error occurs at the receiver and an answer message with the Result-Code set to DIAMETER_AVP_NOT_ALLOWED shall be sent back to the originator of the request. A Failed-AVP AVP containing a copy of the corresponding Diameter AVP shall be included in this message.

- An optional Information Element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this Information Element shall not cause an application error and may be ignored by the receiver.

When a procedure is required to determine whether two S-CSCF names are equal, the rules for SIP URI comparison specified in RFC 3261 chapter 19.1.4 shall apply.

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
Public 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 or expires parameter in Contact 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 or expires parameter in Contact field in the REGISTER method is not equal to zero then this AVP may be absent from the command. If present its value shall be set to REGISTRATION. If the request corresponds to an initial registration or a re-registration, and the I-CSCF explicitly queries the S-CSCF capabilities, then this AVP shall be present in the command and the value shall be set to REGISTRATION_AND_CAPABILITIES. The I-CSCF shall use this value when the user's current S-CSCF, which is stored in the HSS, cannot be contacted and a new S-CSCF needs to be selected.
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 / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
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 (if there is an error in any of the following 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 Experimental-Result-Code 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 Experimental-Result-Code shall be set to DIAMETER_ERROR _IDENTITIES_DONT_MATCH.

3. Check whether the public identity received in the request is barred for the establishment of multimedia sessions.

   - If it is, the HSS shall check whether there are other non-barred public identities to be implicitly registered with that one.

- If so, continue to step 4.
- If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

4. 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 Experimental-Result-Code 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 5.
- If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.
- If it is REGISTRATION_AND_CAPABILITIES, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code 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 Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy the most restrictive service profile of the user. The Server-Capabilities AVP may be absent, 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. Stop processing.

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

- If it is registered, the HSS shall return the stored S-CSCF name. No S-CSCF capabilities shall be present in the response. If User-Authorization-Type is equal to REGISTRATION, Experimental-Result-Code shall be set to DIAMETER_SUBSEQUENT_REGISTRATION. If User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER_SUCCESS.
- If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored) and User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION, then:
  - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
  - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to DIAMETER_SERVER_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
  - If the value of User-Authorization-Type is DE_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Experimental-Result-Code to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.
  - If the value of User-Authorization-Type is REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
    - If there is at least one identity of the user that is registered the HSS shall return the S-CSCF name assigned for the user and Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
    - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored), then:
      - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
      - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to

DIAMETER_SERVER_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.

- If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. The returned capabilities shall satisfy the most restrictive service profile of the user. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it may select any available S-CSCF. Experimental-Result-Code shall 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 User Identity, or to clear the name of the S-CSCF assigned to one or more Public User Identities.

- To download from HSS the relevant user 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
Public User Identity (See 7.2)	Public-Identity	C	Public User Identity or list of Public User Identities. One and only one Public User Identity shall be present if the Server-Assignment-Type is any value other than TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION. If Server-Assignment-Type indicates deregistration of some type and Private User Identityis not present in the request, at least one Public User Identity shall be present.
S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity (See 7.3)	User-Name	C	Private User 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 a 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 User Identity is present then the Private User Identity shall be present.
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 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 the HSS name, the 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 as a consequence of a session termination for an 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	C	Private User identity. It shall be present if it is available when the HSS sends the response. It may be absent in the following error case: when the Server-Assignment-Type of the request is UNREGISTERED_USER and the received Public User Identity is not known by the HSS.
Registration result (See 7.6)	Result-Code / Experimental-Result	M	Result of registration. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile (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, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER according to the rules defined in section 6.6. If the S-CSCF receives more data than it is prepared to accept, it shall perform the de-registration of the user with User-Authorization-Type set to DEREGISTRATION_TOO_MUCH_DATA and send back a SIP 3xx or 480 (Temporarily Unavailable) response, which shall trigger the selection of a new S-CSCF by the I-CSCF, as specified in 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging-Information	C	Addresses of the charging functions. It shall be present when the User-Data AVP is sent to the S-CSCF. When this parameter is included, the Primary Charging Collection Function name shall be included. All other elements shall be included if they are available.

6.1.2.1 Detailed behaviour

On registering/deregistering a Public User 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 sections 6.5.1 and 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 states. For implicitly registered identities, the rules defined in Section 6.5.1 shall apply.. 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 Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS may check whether the private and Public User Identities received in the request belong to the same user. If not Experimental-Result-Code 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 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 and the HSS shall set the registration state of the Public User Identity as registered (if not already registered).

     Only one Public User Identity shall 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 User Identity as unregistered, i.e. registered as a consequence of a terminating call and download the relevant user information. The Result-Code shall be set to DIAMETER_SUCCESS.

     Only one Public User Identity shall 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, DEREGISTRATION_TOO_MUCH_DATA or ADMINISTRATIVE_DEREGISTRATION, the HSS shall clear the S-CSCF name for all the Public User 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 User Identity shall be present; in this case 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 User Identities that the S-CSCF indicated in the request. If no Public User Identity is present in the request, the Private User Identity shall be present. If the HSS decided to keep the S-CSCF name stored, the HSS shall keep the S-CSCF name stored for all the identities of the user and set their registration state to unregistered.

     The Result-Code shall be set to DIAMETER_SUCCESS.

     If the HSS decides not to keep the S-CSCF name the Experimental-Result-Code shall be set to DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED. If the HSS received Public User Identities in the request, the HSS shall set the registration state to not registered for the Public User Identity(ies) that the S-CSCF indicated in the request. If the HSS received a Private User Identity in the request, the HSS shall set the registration state of all Public User Identities related to the Private User Identity to not registered.

   - If it indicates NO_ASSIGNMENT, the HSS checks whether the user is assigned for the S-CSCF requesting the data and download the relevant user Information. 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.

     Only one Public User Identity shall be present in the request. If more than one Public User 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 AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the HSS shall clear the S-CSCF name for the Public User 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 confirmation of the authentication shall be cleared. The Result-Code shall be set to DIAMETER_SUCCESS.

     Only one Public User Identity shall 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 the HSS cannot fulfil the received request, e.g. due to database error, it shall set the Result-Code to DIAMETER_UNABLE_TO_COMPLY. The HSS shall not modify any user state nor download any user information to the S-CSCF.

See chapter 8.1.2 and 8.1.3 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
Public 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 / Experimental-Result	M	This information element indicates the result of de-registration. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

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: 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 when the user's S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for the updated User Profile. 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	Mapping to	Cat.	Description

element name	Diameter AVP		
Result (See 7.6)	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
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 Experimental-Result-Code 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 there is at least one identity of 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 Experimental-Result-Code shall be set to DIAMETER_UNREGISTERED_SERVICE.

   - If it is not registered and has no unregistered services related data the response shall contain Experimental-Result-Code 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 and/or charging 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	Private User Identity.
User profile (See 7.7)	User-Data	C	Updated user profile (see section s 6.5.2.1 and 6.6.1), with the format defined in chapter 7.7. It shall be present if the user profile is changed in the HSS. If the User-Data AVP is not present, the Charging-Information AVP shall be present.
Charging Information (See 7.12)	Charging-Information	C	Addresses of the charging functions. It shall be present if the charging information is changed in the HSS. If the Charging-Information AVP is not present, the User-Data AVP shall be present. When this parameter is included, the Primary-Charging-Collection-Function-Name AVP shall be included. All other charging information shall be included if they are available.
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 element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Experimental-Result	M	This information element indicates the result of the update of User Profile in the S-CSCF. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

6.2.2.1 Detailed behaviour

The HSS shall make use of this procedure to update relevant user information and/or the charging information in the S-CSCF. The user information contains the user profile. See chapter s 6.5.2.1 and 6.6.1 for the rules of user profile updating.

If the User-Data AVP is present in the request, the S-CSCF shall overwrite, for the Public User Identities indicated in the request, current information with the information received from the HSS, except in the error situations detailed in table 6.2.2.1.1.

If the S-CSCF receives more data than it can accept, it shall return the corresponding error code to the HSS as indicated in table 6.2.2.1.1. The S-CSCF shall not overwrite the data that it already has to give service to the user. The HSS shall initiate a network-initiated de-registration procedure towards the S-CSCF with Deregistration-Reason set to SERVER_CHANGE, which will trigger the assignment of a new S-CSCF. If the Charging-Information AVP is present in the request, the S-CSCF shall replace the existing charging address information with the information received from the HSS.

The Charging-Information AVP and/or the User-Data AVP shall be present in the request.

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_ERROR_NOT SUPPORTED_USER_DATA	The request failed.The S-CSCF informs the HSS that the received user information contained data, which was not recognised or supported, i.e. user profile which is not correctly encoded according to the XML schema or standardised profile information which cannot be interpreted by the S-CSCF due to unsupported S-CSCF capabilities.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in S-CSCF.
DIAMETER_ERROR_TOO_MUCH_DATA	The request failed. The S-CSCF informs to the HSS that it tried to push too much data into the S-CSCF.
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
Public 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”.
Authentication Context (See 7.9.7)	SIP-Authentication-Context	C	It shall contain authentication-related information relevant for performing the authentication. When Authentication Scheme contains "Digest-AKAv1-MD5", this AVP is not used and shall be missing.

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, as sent to the terminal, and auts, as received from the terminal. Nonce and auts shall both be binary encoded.

Table 6.3.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description

User Identity (See 7.2)	Public-Identity	C	User public identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity (See 7.3)	User-Name	C	User private identity. It shall be present when the result is DIAMETER_SUCCESS.
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	C	This AVP indicates the number of authentication vectors delivered in the Authentication Data information element. It shall be present when the result is DIAMETER_SUCCESS.
Authentication Data (See 7.9)	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero or it is not present, then this AVP shall not be present. See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 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 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, binary 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.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain, binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentiality Key (See 7.9.5)	Confidentiality-Key	O	This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	This information element shall contain the integrity key. It shall be binary encoded.

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 Experimental-Result-Code 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 Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

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

4. If the request indicates there is a synchronization failure, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

   - If they are identical 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 compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

     - If they are different, the HSS shall store the S-CSCF name. 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. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

     - If they are identical, 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 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) or not registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

     - If they are different or if there is no S-CSCF name stored in the HSS for any identity of the IMS subscription, the HSS shall store the S-CSCF name. 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. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

     - If they are identical, 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. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

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

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 User 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 User Identities that are configured in the HSS to be in the same implicitly registered Public User Identity set with the targeted individual Public User Identity. Where the S-CSCF initiated procedure affects the Registration state of the targeted Public User Identity, the Registration states of the Public User Identities in the associated implicitly registered Public User Identity set are affected in the same way..

6.5.1.1 Registration

The notification of a registration of a Public User Identity implies the registration of the corresponding implicitly registered Public User Identity set.. The user information downloaded in the response contains the Public User Identities of the implicitly registered Public User Identity set with the associated service profiles. This allows the S-CSCF to know which Public User Identities belong to the implicitly registered Public User identity set. The S-CSCF shall take from the set of implicitly registered Public User Identities the first identity which has the syntax of a SIP URI and which is not barred, and use this as the default Public User Identity.

6.5.1.2 De-registration

The de-registration of a Public User Identity implies the de-registration of the corresponding implicitly registered Public User Identity set, both in the HSS and in the S-CSCF. The S-CSCF shall include in the request a single Public User Identity to deregister all the Public User Identities that belong to the corresponding implicitly registered Public User Identity set.

The de-registration of a private identity implies the de-registration of all the corresponding Public User Identities, both in the HSS and in the S-CSCF.

6.5.1.3 Authentication

Setting the flag for a Public User Identity that indicates a pending authentication implies setting the "authentication pending" flag for each corresponding implicitly registered Public User Identity in the HSS.

6.5.1.4 Downloading the user profile

If the S-CSCF requests to download a user profile from HSS, the user profile in the response shall contain the Public User Identities of the corresponding implicitly registered Public User Identity set with the associated service profiles.

6.5.2 HSS initiated procedures

6.5.2.1 Update of User Profile

A request sent by the HSS to update the user profile shall include only the Public User Identities of the implicitly registered Public User Identity set, with the associated service profiles (even if not updated). If other Public User Identities not associated with the implicitly registered Public User Identity set are affected, they shall be downloaded in separate commands.

6.5.2.2 De-registration

A request sent by the HSS to de-register an implicitly registered Public User Identity set shall contain all the Public User identities of the deregistered set.

The de-registration of a Private User Identity implies the de-registration of all the corresponding Public User Identities, both in the HSS and in the S-CSCF.

6.5.2.3 Update of the Charging information

A request sent by the HSS to update the charging information shall include the private user identity for whom the charging information changed.

6.6 Download of the Relevant User Profile

The download of the relevant profile data from the HSS to the S-CSCF depends on whether the user profile is already stored in the S-CSCF.

If User-Data-Already-Available is set to USER_DATA_NOT_AVAILABLE the HSS shall download the requested user profile. If the Public User Identity in the request is included in an implicitly registered Public User Identity set, the HSS shall include in the response the service profiles associated with all Public User Identities within the implicitly registered Public User Identity set to which the received Public User Identity belongs.

If User-Data-Already-Available is set to USER_DATA_ALREADY_AVAILABLE, the HSS shall not return any user profile data.

6.6.1 HSS initiated update of User Profile

The request to update of the user information in the S-CSCF includes only the Public User Identities of the implicitly registered Public User identity set with the associated service profiles. See 6.5.2.1.

If the Public User Identity 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) and there are changes in the user profile, the HSS shall immediately push the complete user profile to the S-CSCF.

6.6.2 S-CSCF operation

At deregistration of a Public User Identity, the S-CSCF shall store the user information 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 information.

6.7 S-CSCF Assignment

The list of mandatory and optional capabilities received by an I-CSCF from the HSS allows operators to distribute users between S-CSCFs, 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.

As a first choice, t-he I-CSCF shall select an S-CSCF that has all the mandatory and optional capabilities for the user. 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.

It is the responsibility of the operator to ensure that there are S-CSCFs which have mandatory 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 capabilities indicated by the HSS, the I-CSCF shall inform the HSS via the O&M subsystem.

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. To do this, the operator may include one or more S-CSCF names as part of the capabilities of the user profile. The 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].

7.9.7 Authentication Context

This information element contains authentication-related information relevant for performing the authentication but that is not part of the SIP authentication headers. Some mechanisms (e.g. PGP, digest with quality of protection set to authint defined in IETF RFC 2617 [13], digest with predictive nonces or sip access digest) request that part or the whole SIP request (e.g. the SIP method) is passed to the entity performing the authentication. In such cases the SIPAuthentication-Context AVP shall be carrying such information.

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, secondary 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 Void

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 error cases, which can occur during the registration process. If the new and previously assigned S-CSCF names sent in the Multimedia-Auth-Request command are different, and the Multimedia-Auth-Request is not indicating synchronisation failure (i.e.the request does not contain auts parameter) then the HSS shall overwrite the S-CSCF name.

If the new and previously assigned S-CSCF names sent in a command other than the Multimedia-Auth-Request command are different, then the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF indicating an error.

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 shall 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 HSS shall first check whether the deregistration is really required by comparing the Diameter client address of the newly assigned S-CSCF received in the MAR command to the Diameter client address stored in the HSS. If the Diameter client addresses match, the deregistration shall not be initiated. Otherwise the deregistration may be initiated and it 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 S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different, then, the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF with Experimental-Result-Code value set to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

8.1.3 Error in S-CSCF assignment type

If the Server-Assignment-Type in the Server-Assignment-Request command sent by the S-CSCF to the HSS is not allowed, e.g. Server-Assignment-Type set to UNREGISTERED_USER for a user already registered, the HSS shall send a response to the S-CSCF with the Experimental-Result-Code value set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE.

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 / Experimental-Result-Code
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	Confidentiality-Key
Integrity Key	Integrity-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

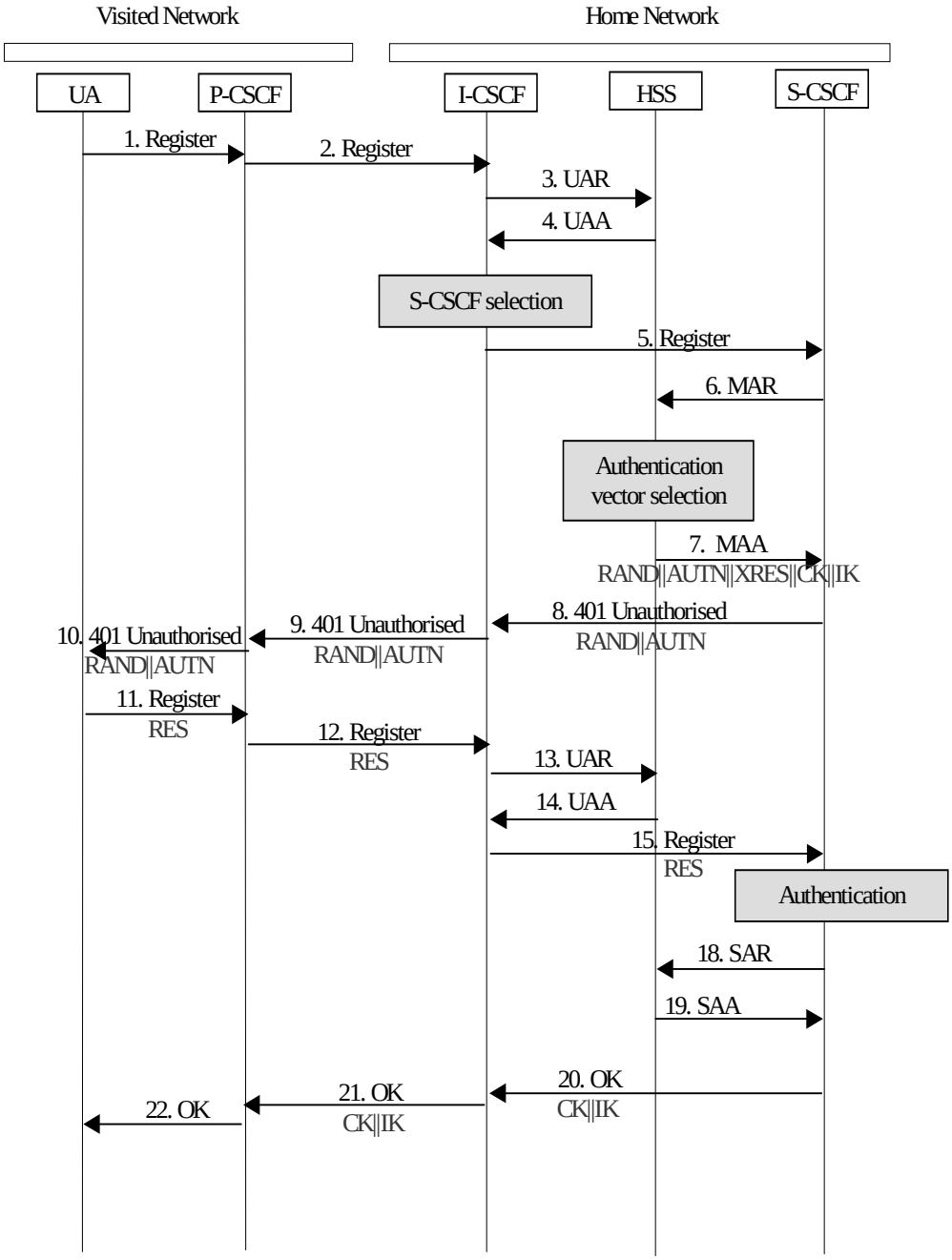

Figure A.4.1.1: Registration – user not registered

A.4.2 Registration – user currently registered

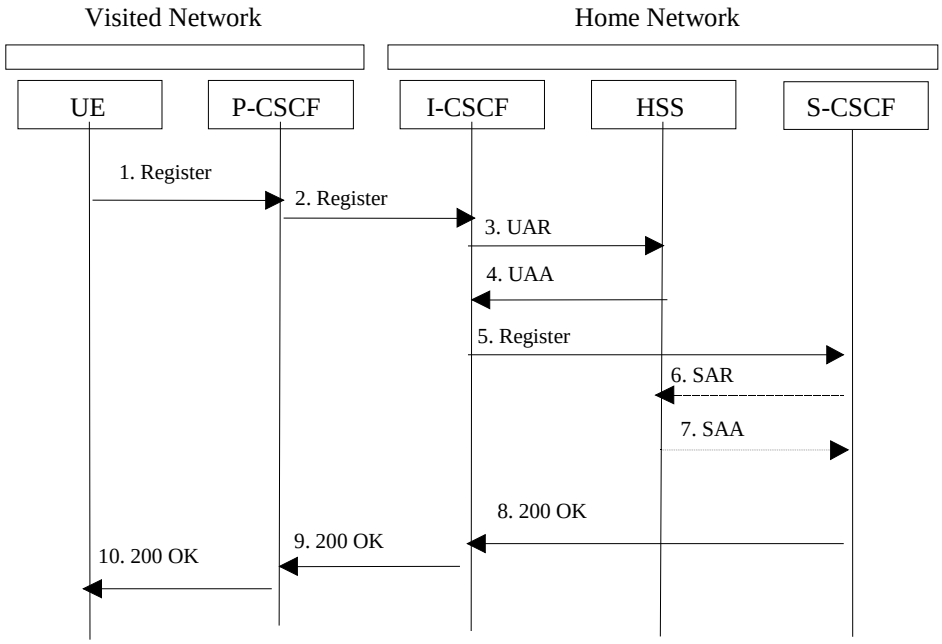

Figure A.4.2.1: Re-registration

A.4.3 Mobile initiated de-registration

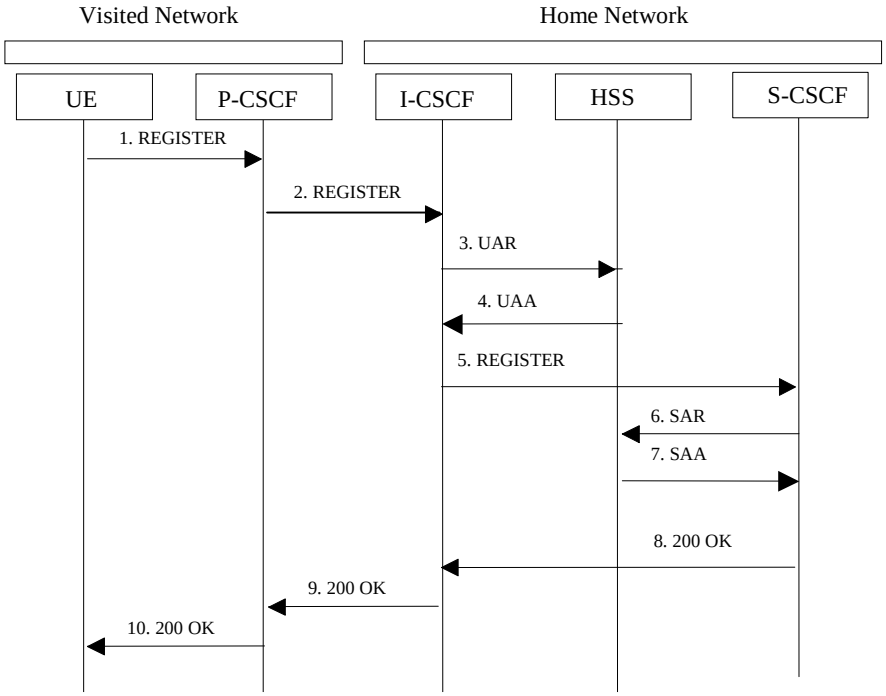

Figure A.4.3.1: Mobile initiated de-registration

A.4.4 Network initiated de-registration

A.4.4.1 Registration timeout

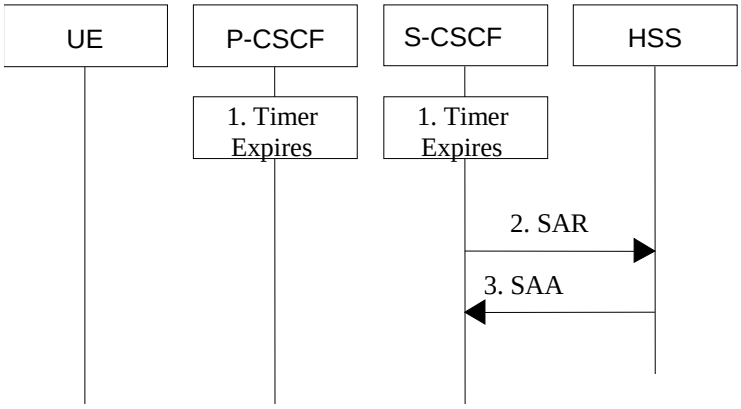

Figure A.4.4.1.1: Network initiated de-registration – registration timeout

A.4.4.2 Administrative de-registration

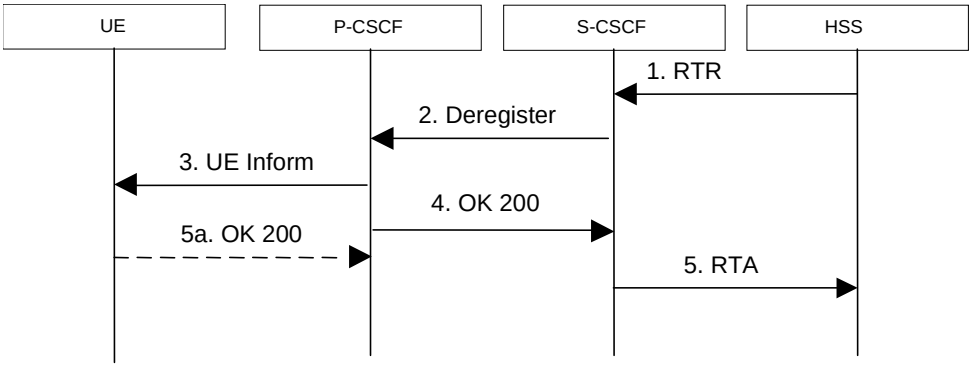

Figure A.4.4.2.1: Network initiated de-registration – administrative de-registration

A.4.4.3 De-registration initiated by service platform

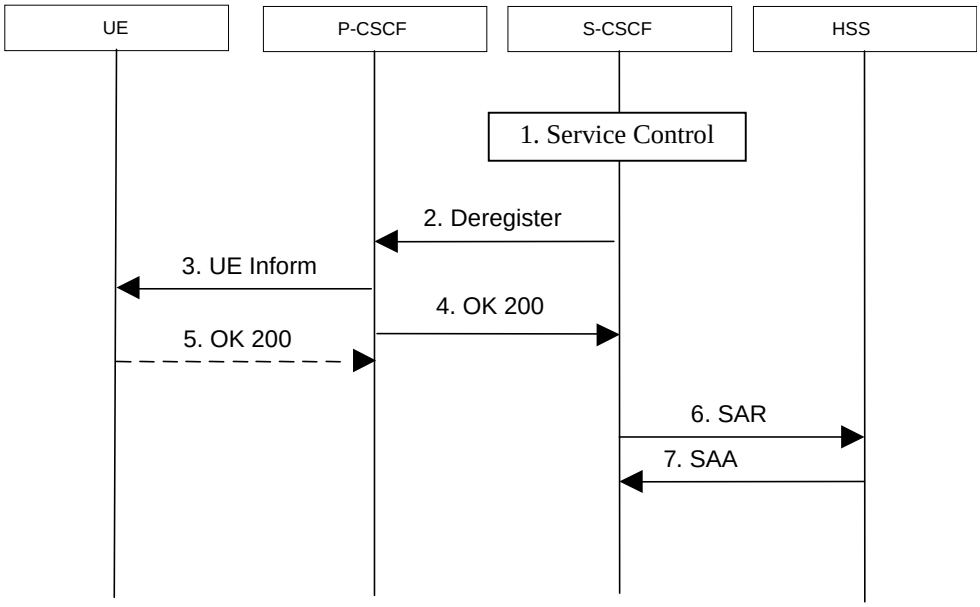

Figure A.4.4.3.1: Network initiated de-registration – initiated by service platform

A.4.5 MT SIP session set-up

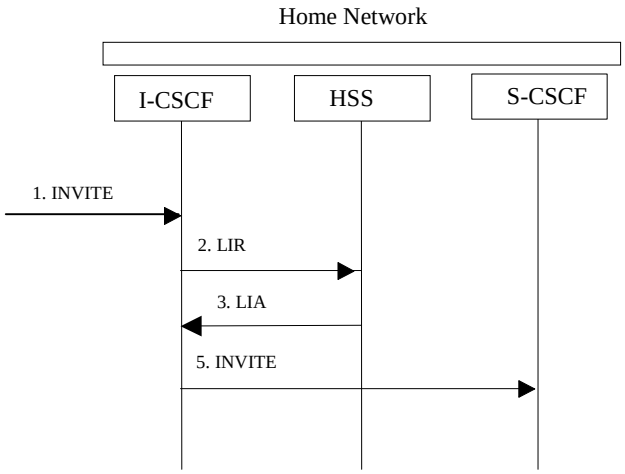

Figure A.4.5.1: MT SIP session set-up

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

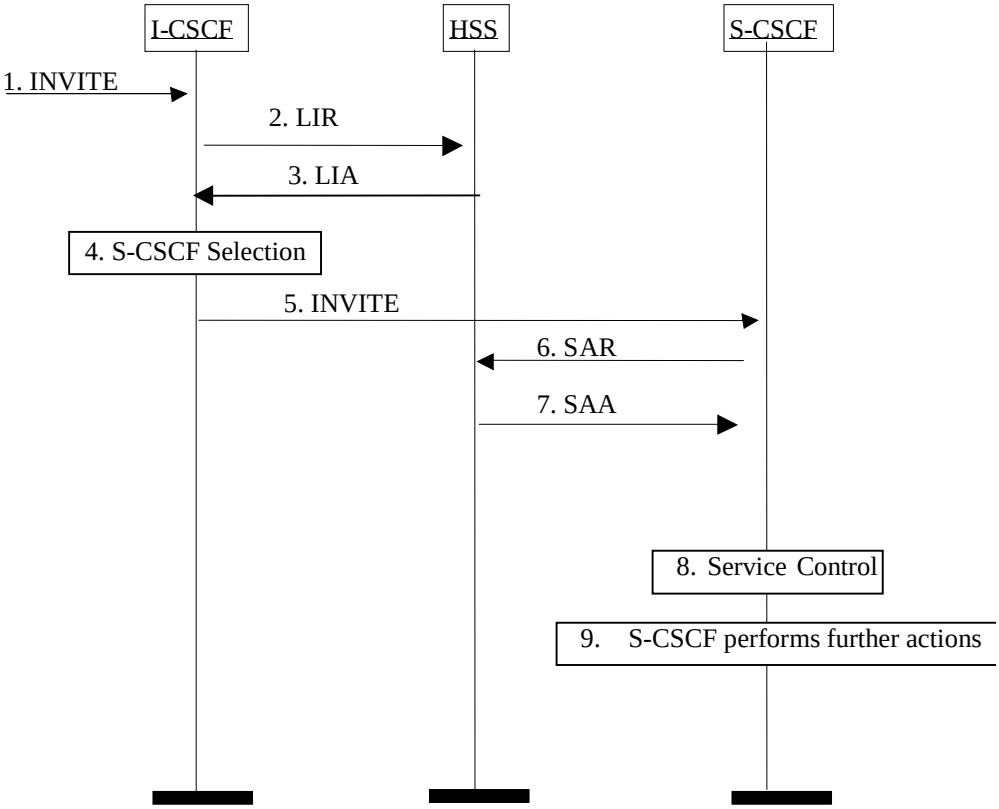

Figure A.4.6.1: Initiation of a session to a non-registered user

A.4.7 User Profile update

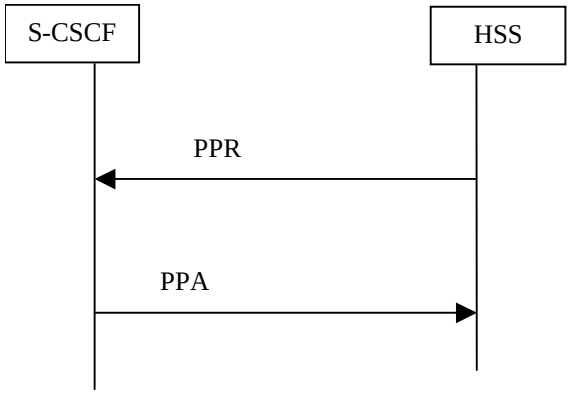

Figure A.4.7.1: User profile update

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:

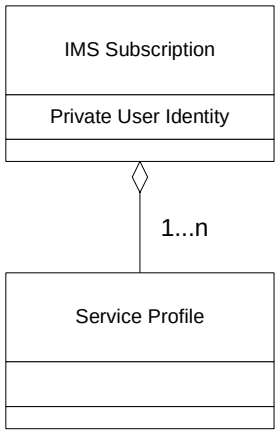

Figure B.1.1: User Profile

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:

:

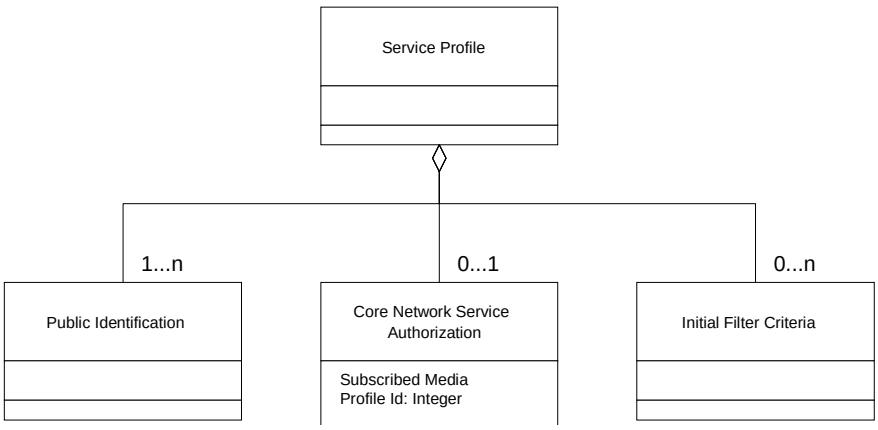

Figure B.2.1: Service Profile

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. If no instance of the class Core Network Service Authorization is present, no filtering related to subscribed media applies in S-CSCF.

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:

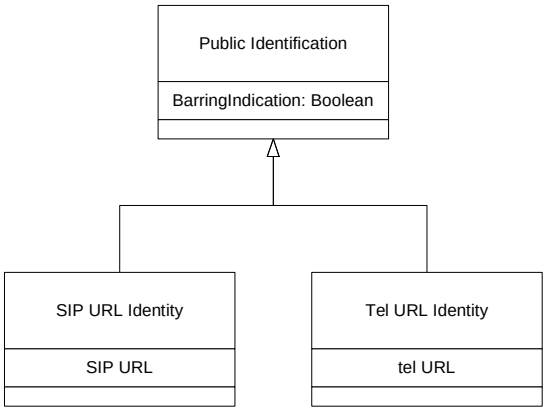

Figure B.2.1.1: Public Identification

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 in any IMS communication except registrations and re-registrations, as specified in 3GPP TS 24.229 [8]..

B.2.2 Initial Filter Criteria

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

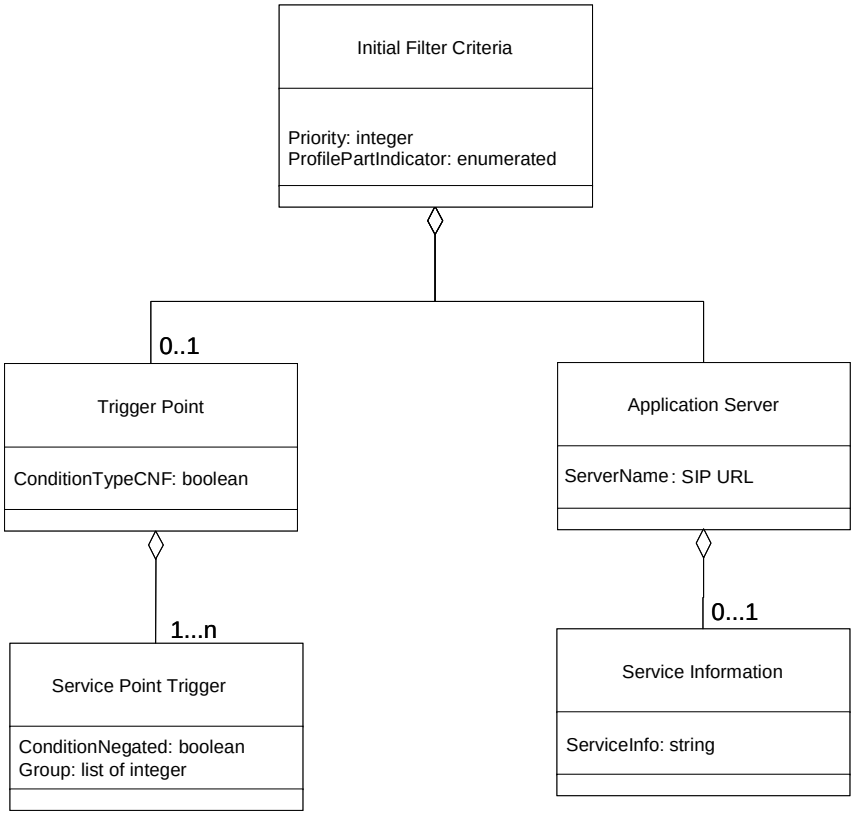

Figure B.2.2.1.1: Initial Filter Criteria

Each instance of the Initial Filter Criteria class is composed of 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. 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 initial Filter Criterion.

ProfilePartIndicator attribute is an enumerated type, with possible values “REGISTERED and UNREGISTERED, indicating if the iFC is a part of the registered or unregistered user profile. If ProfilePartIndicator is missing from the iFC, the iFC is considered to be relevant to both the registered and unregistered parts of the user profile, i.e. belongs to the common part of the user profile.

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 absence of Trigger Point instance will indicate an unconditional triggering to Application Server.

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

Each Trigger Point is composed by 1 to n instances of the class Service Point Trigger.

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.

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 Service Point Trigger

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

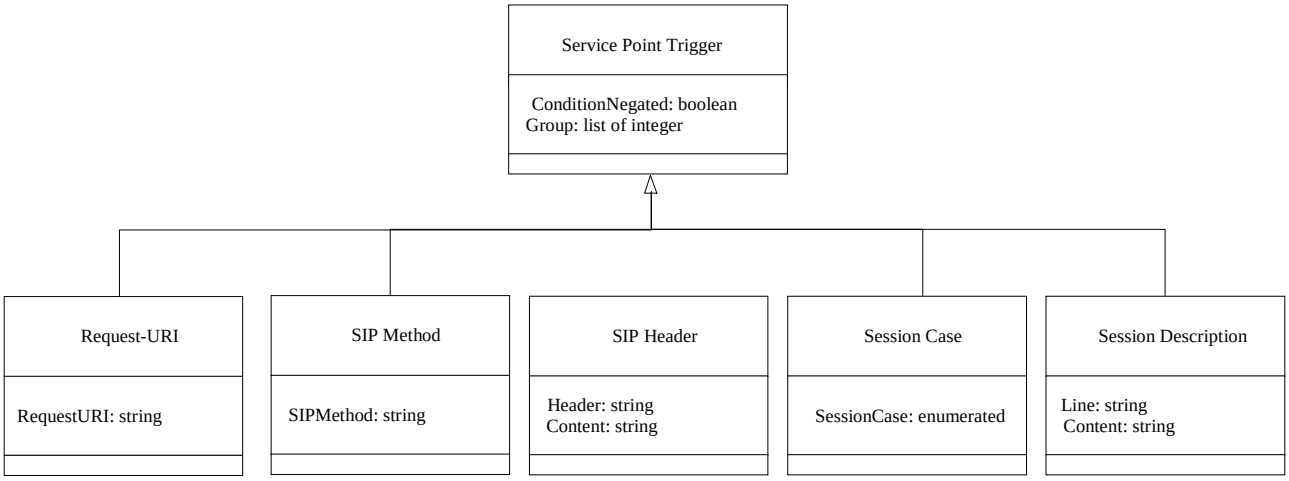

Figure B.2.3.1: Service Point Trigger

The attribute Group of the class Service Point Trigger allows the grouping of SPTs 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 SPT instances. If the SPTbelongs to different ORed sets, SPTcan have more than one Group values assigned. At least one Group must be assigned for each SPT.

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

The attribute ConditionNegated of the class Service Point Trigger defines whether the individual SPT instance is negated (i.e. NOT logical expression).

Request-URI class defines SPT for the Request-URI. Request-URI contains attribute RequestURI.

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

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

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

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

Session Description Information class defines SPTfor 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.

Annex C (informative): Conjunctive and Disjunctive Normal Form

A Trigger Point expression is constructed out of atomic expressions (i.e. Service Point Trigger) 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” Content = “joe”)

The trigger can be split into the following atomic expressions:

Method=”INVITE”

Method=”MESSAGE”

Method=”SUBSCRIBE”

NOT header=”from” Content =”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” Content = “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>IMPI1@homedomain.com</PrivateID>
        <ServiceProfile>
                <PublicIdentity>
                        <BarringIndication>1</BarringIndication>
                        <Identity> sip:IMPU1@homedomain.com </Identity>
                </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>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>MESSAGE</Method>
                    </SPT>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>SUBSCRIBE</Method>
                    </SPT>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>1</Group>
                        <Method>INVITE</Method>
                    </SPT>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>1</Group>
                        <Method>MESSAGE</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>
                </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” 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>IMPI1@homedomain.com</PrivateID>
        <ServiceProfile>
            <PublicIdentity>
                <BarringIndication>1</BarringIndication>
```

```
                <Identity> sip:IMPU1@homedomain.com </Identity>
            </PublicIdentity>
            <PublicIdentity>
                <Identity> sip:IMPU2@homedomain.com </Identity>
            </PublicIdentity>
            <InitialFilterCriteria>
                <Priority>0</Priority>
                <TriggerPoint>
                    <ConditionTypeCNF>0</ConditionTypeCNF>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>INVITE</Method>
                    </SPT>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>1</Group>
                        <Method>MESSAGE</Method>
                    </SPT>
                    <SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>2</Group>
                        <Method>SUBSCRIBE</Method>
                    </SPT>
                    <SPT>
                        <ConditionNegated>1</ConditionNegated>
                        <Group>2</Group>
                        <SIPHeader>
                            <Header>From</Header>
                            <Content>”joe”</Content>
                        </SIPHeader>
                    </SPT>
                </TriggerPoint>
                <ApplicationServer>
                    <ServerName>sip:AS1@homedomain.com</ServerName>
                </ApplicationServer>
            </InitialFilterCriteria>
        </ServiceProfile>
        </IMSSubscription>
</testDatatype>
```

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

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

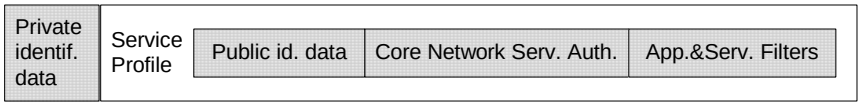

Figure C.1: Example of in-line format of user profile

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 shall 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
tProfilePartIndicator	ProfilePartIndicator	enumerated	Possible values: 0 (REGISTERED) 1 (UNREGISTERED)
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_ REGISTERED 2 (TERMINATING_UNREGISTERED)
tPrivateID	PrivateID	anyURI	Syntax described in RFC 2486
tSIP_URL	Identity	anyURI	Syntax described in RFC 3261
tTEL_URL	Identity	anyURI	Syntax described in RFC 2806
tIdentity	Identity	(union)	Union of tSIP_URL and tTEL_URL
tServiceInfo	ServiceInfo	string	
tString	RequestURI, Method, Header, Content, Line	string	
tBool	ConditionTypeCNF, ConditionNegated, BarringIndication	boolean	Possible values: 0 (false) 1 (true)
tSubscribedMediaProfileId	SubscribedMediaProfileId	integer	>=0
(*) the tDefaultHandling is not used in Release 5			

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 n)
tServiceProfile	ServiceProfile	PublicIdentity	tPublicIdentity	(1 to n)
		InitialFilterCriteria	tInitialFilterCriteria	(0 to n)
		CoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	(0 to 1)
tCoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	SubscribedMediaProfileId	tSubscribedMediaProfileId	(0 to 1)
tPublicIdentity	PublicIdentity	BarringIndication	tBool	1
		Identity	tIdentity	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	1
		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)
NOTE: “n” shall be interpreted as non-bounded. (*): the DefaultHandling should not be sent by a Rel-5 HSS				

Annex F (normative): Definition of parameters for service point trigger matching

Table F.1 defines the parameters that are transported in the user profile XML.

Table F.1: Definition of parameters in the user profile XML

Tag	Description
SIPHeader	A SIP Header SPT shall be evaluated separately against each header instance within the SIP message. The SIP Header SPT matches if at least one header occurrence matches the SPT.
Header (of SIPHeader)	Header tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [12]. The regular expression shall be matched against the header-name of the SIP header. For definition of header and header-name, see IETF RFC 3261 [10]. Before matching the header-name to the pattern, all SWSs shall be removed from the header-name and all LWSs in the header-name shall be reduced to a single white space character (SP). For definition of SWS and LWS, see IETF RFC 3261 [10].
Content (of SIPHeader)	Content tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [12]. The regular expression shall be matched against the header-value of the SIP header. For definition of header and header-value, see IETF RFC 3261 [10]. If the SIP header contains several header-values in a comma-separated list, each of the header-value shall be matched against the pattern for the Content separately. Before matching the header-value to the pattern, all SWSs shall be removed from the header-value and all LWSs in the header-value shall be reduced to a single white space character (SP). For definition of SWS and LWS, see IETF RFC 3261 [10].
SessionDescription	A Session Description SPT shall be evaluated separately against each SDP field instance within the SIP message. The Session Description SPT matches if at least one field occurrence matches the SPT.
Line (of SessionDescription)	Line tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [12]. The regular expression shall be matched against the type of the field inside the session description. For definition of type, see chapter 6 in IETF RFC 2327 [11].
Content (of SessionDescription)	Content tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [12]. The regular expression shall be matched against the value of the field inside the session description. For definition of value, see chapter 6 in IETF RFC 2327 [11].

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
Sep 2002	CN#17	NP-020449	001	2	Clarification of implicit registration	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	002	1	Clarification of user registration status query	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	003	1	Clarification of HSS initiated update of user profile	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	004	2	Clarification of MAR command	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	005	1	Conditionality of the SIP-Auth-Data-Item in MAA command	5.0.0	5.1.0
Dec 2002	CN#18	NP-020587	008	2	Rejection of registration of a Temporary Public Identity without active implicit registration	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	010	-	Removal of upper bounds in Cx i/f user profile	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	011	-	S-CSCF Assignment	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	012	-	NAS-Session-Key AVPs in MAA command	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	013	1	Correction to detailed behaviour of user registration status query	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	014	1	Removing the DDF dependencies from Cx interface	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	015	1	Clarification of SERVER_CHANGE de-registration reason code	5.1.0	5.2.0
Dec 2002	CN#18	NP-020589	016	1	Clarification of User-Authorization-Type AVP usage within the UAR	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	017	1	Correction to HSS initiated update of user profile	5.1.0	5.2.0
Dec 2002	CN#18	NP-020588	019	-	Correction in charging information	5.1.0	5.2.0
Dec 2002	CN#18	NP-020590	020	1	Error handling in S-CSCF when receiving too much data	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	021	1	Re-allocation of S-CSCF	5.1.0	5.2.0
Dec 2002	CN#18	NP-020591	022	-	Correction of the SPI	5.1.0	5.2.0
March 2003	CN#19	NP-030238	025	1	Clarification of service profile download at service profile modification	5.2.0	5.3.0
March 2003	CN#19	NP-030016	028	-	Filter ID field removal in InitialFilterCriteria class	5.2.0	5.3.0
March 2003	CN#19	NP-030242	030	1	Clarification of IMPU barring handling	5.2.0	5.3.0
March 2003	CN#19	NP-030245	032	1	The default public user identity in the Server-Assignment-Answer	5.2.0	5.3.0
March 2003	CN#19	NP-030247	034	2	Corrections to service profile	5.2.0	5.3.0
March 2003	CN#19	NP-030314	037	3	Handling of non supported data in the S-CSCF when the profile is being updated	5.2.0	5.3.0
March 2003	CN#19	NP-030240	024	1	Clarification of the HSS behaviour in REGISTRATION and DE_REGISTRATION procedures at IMPU checking time.	5.2.0	5.3.0
March 2003	CN#19	NP-030015	027	-	Deletion of Annex F	5.2.0	5.3.0
March 2003	CN#19	NP-030017	029	-	Clarification of User-Authorization-Type AVP usage within UAR	5.2.0	5.3.0

March 2003	CN#19	NP-030243	031	1	Update TS 29.228 after Diameter has become RFC	5.2.0	5.3.0
March 2003	CN#19	NP-030246	033	1	Replacement of the NAS-Session-Key AVP	5.2.0	5.3.0
March 2003	CN#19	NP-030312	035	1	Clarification on Re-allocation of S-CSCF	5.2.0	5.3.0
March 2003	CN#19	NP-030261	038	1	Change of SPI to SPT	5.2.0	5.3.0
March 2003	CN#19	NP-030252	040	1	Definition of the Subscribed Media Profile Identifier	5.2.0	5.3.0
March 2003	CN#19	NP-030014	026	-	Error in definition of Service Point of Interest class	5.2.0	5.3.0
June 2003	CN#20	NP-030215	043	-	Correct use of the Result-Code AVP	5.3.0	5.4.0
June 2003	CN#20	NP-030215	044	1	Conditionality of User-Name AVP in Server-Assignment-Answer	5.3.0	5.4.0
June 2003	CN#20	NP-030215	045	2	Corrections to the base 64 encoding examples	5.3.0	5.4.0
June 2003	CN#20	NP-030215	046	1	Deregistration of implicitly registered public user identities	5.3.0	5.4.0
June 2003	CN#20	NP-030215	047	-	Clarification on the Server-Assignment-Type NO_ASSIGNMENT	5.3.0	5.4.0
June 2003	CN#20	NP-030215	048	1	Incorrect use of result-code	5.3.0	5.4.0
June 2003	CN#20	NP-030215	049	1	Misalignment in the Public-User-Identity IE	5.3.0	5.4.0
June 2003	CN#20	NP-030215	050	1	Duplicated Destination-Host AVP within MAR command code	5.3.0	5.4.0
September 2003	CN#21	NP-030383	042	3	Error in S-CSCF Assignment Type	5.4.0	5.5.0
September 2003	CN#21	NP-030383	051	2	Mistakes in the XML schema of 29.228-540	5.4.0	5.5.0
September 2003	CN#21	NP-030383	055	1	Extensibility of the public identity structure in the XML schema	5.4.0	5.5.0
December 2003	CN#22	NP-030500	054	3	The S-CSCF name needs to be checked always in MAR	5.5.0	5.6.0
December 2003	CN#22	NP-030585	056	3	Conditions for inclusion of Charging Information	5.5.0	5.6.0
December 2003	CN#22	NP-030500	059	1	MAR in synchronisation failure case	5.5.0	5.6.0
December 2003	CN#22	NP-030500	062	-	Conditional AVPs in answer commands	5.5.0	5.6.0
December 2003	CN#22	NP-030500	064	1	Server-Assignment-Request	5.5.0	5.6.0
December 2003	CN#22	NP-030500	066	-	Determination of User-Authorization-Type AVP based on registration expiration	5.5.0	5.6.0
December 2003	CN#22	NP-030500	068	2	Not registered state after deregistration with S-CSCF deleted at the HSS	5.5.0	5.6.0
December 2003	CN#22	NP-030500	070	-	The extensibility of the XML schema	5.5.0	5.6.0
December 2003	CN#22				Application ID reference updated	5.5.0	5.6.0
March 2004	CN#23	NP-040046	076	1	Clarification on S-CSCF-Name comparison	5.6.0	5.7.0
March 2004	CN#23	NP-040046	084	1	Conditions for inclusion of Public Identity in SAR	5.6.0	5.7.0
March 2004	CN#23	NP-040046	086	1	Correction to sending the Charging-Information AVP	5.6.0	5.7.0
March 2004	CN#23	NP-040046	088		Correction to User-Authorization-Answer	5.6.0	5.7.0
March 2004	CN#23	NP-040046	090		Default handling of error cases during IMS registration	5.6.0	5.7.0

June 2004	CN#24	NP-040215	096	2	Update of the charging addresses from HSS	5.7.0	5.8.0
June 2004	CN#24	NP-040215	094	1	Content of the User Profile	5.7.0	5.8.0
June 2004	CN#24	NP-040215	098		Correction of SessionCase attribute ambiguity	5.7.0	5.8.0
Sept 2004	CN#25	NP-040416	108	1	LIR and services related to unregistered state	5.8.0	5.9.0
Sept 2004	CN#25	NP-040396	123	2	Simplification of the User Profile Split concept	5.8.0	5.9.0
Sept 2004	CN#25	NP-040416	119	3	Use of regular expressions	5.8.0	5.9.0
Dec 2004	CN#26	NP-040523	137	1	HSS initiated deregistration with “not registered” registration state	5.9.0	5.10.0
Dec 2004	CN#26	NP-040523	141	2	HSS initiated deregistration using the network initiated de-registration procedure	5.9.0	5.10.0
Dec 2004	CN#26	NP-040523	149		Regular expressions	5.9.0	5.10.0
Dec 2004	CN#26	NP-040523	160	2	Handling of Information Element marked as (M), (C) or (O)	5.9.0	5.10.0
Mar 2005	CN#27	NP-050030	165		Avoiding undesired deregistration	5.10.0	5.11.0
Mar 2005	CN#27	NP-050030	167	1	Correction to authentication procedures in not registered case	5.10.0	5.11.0
Mar 2005	CN#27	NP-050030	177		HSS initiated deregistration using the network initiated de-registration procedure	5.10.0	5.11.0
Jun 2005	CN#28	CP-050081	189	1	Clarification of the content of SIP-Authentication-Context	5.11.0	5.12.0
Jun 2005	CN#28	CP-050081	190	1	Removal of the default handling in the service profile	5.11.0	5.12.0

History

Document history		
V5.0.0	June 2002	Publication
V5.1.0	September 2002	Publication
V5.2.0	December 2002	Publication
V5.3.0	March 2003	Publication
V5.4.0	June 2003	Publication
V5.5.0	September 2003	Publication
V5.6.0	December 2003	Publication
V5.7.0	March 2004	Publication
V5.8.0	June 2004	Publication
V5.9.0	September 2004	Publication
V5.10.0	December 2004	Publication
V5.11.0	March 2005	Publication
V5.12.0	June 2005	Publication