3GPP2 X.S0013-005-B

Version 1.0

Date: December 2007

3rd Generation Partnership Project 2
"3GPP2"

All-IP Core Network Multimedia Domain

IP Multimedia Subsystem Cx Interface Signaling Flows and Message Contents

All-IP Core Network Multimedia Domain
IP Multimedia Subsystem Cx Interface
Signaling flows and Message Contents

Contents

Foreword

(This foreword is not part of this document).

This document was prepared by 3GPP2 TSG-X.

This document contains major modifications from the previous revision.

This document is part of the series of documents X.S0013.

This document contains portions of material copied from 3GPP document number TS 29.228 6.f.0. The copyright on the 3GPP document is owned by the Organizational Partners of 3GPP (ARIB - Association of Radio Industries and Businesses, Japan; CCSA – China Communications Standards Association, China; ETSI – European Telecommunications Standards Institute; ATIS, USA; TTA - Telecommunications Technology Association, Korea; and TTC – Telecommunication Technology Committee, Japan), which have granted license for reproduction and for use by 3GPP2 and its Organizational Partners.

Revision History

Revision	Changes	Date
0, v1.0	Initial Publication	December 2003
0, v2.0	Version Update	July 2005
A, v1.0	Release A	November 2005
B, v1.0	Initial Publication	December 2007

1 Scope

The present document specifies the interactions between the HSS (Home Subscriber Server) and the CSCFs (Call Session Control Function), referred to as the Cx interface.

This document addresses the signaling flows for the Cx interface.

2 References

2.1 Normative references

The following standards and documents contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP2 document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP2 X.S0013-002-B: “IP Multimedia (IM) Subsystem – Stage 2”.

[2] Void

[3] 3GPP2 S.R0086-A: “3GPP2 IMS Security Framework”.

[4] Void

[5] 3GPP2 X.S0013-006-B: “Cx Interface based on Diameter Protocol; Protocol details”

[6] 3GPP2 X.S0013-003-B: “IP Multimedia Subsystem – IP Multimedia Call Model; Stage 2”.

[7] Void

[8] 3GPP2 X.S0013-004-B: “IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3”.

[9] IETF RFC 3588, “Diameter Base Protocol”, September 2003.

[10] X.S0027-001-0 v1.0 “Presence Service Architecture and functional description”

[11] IETF RFC 3261, “SIP: Session Initiation Protocol”, June 2002.

[12] IETF RFC 4566, “SDP: Session Description Protocol”, April 1998.

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

[14] IETF RFC 2486 "The Network Access Identifier"

[15] IETF RFC 3966 "The tel URI for Telephone Numbers"

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

[17] 3GPP TS 23.003: "Numbering, addressing and identification"

[18] 3GPP TS 23.008: "Organization of subscriber data"

2.2 Informative references

[19] 3GPP2 S.R0037-0, “3GPP2 All-IP Network Architecture Model Version 2.0, May 14, 2002”.

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,or for unregistered Public Service 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.

Distinct Public Service Identity: An individual Public Service Identity that is stored in the HSS as such.

Authentication pending flag: A flag that indicates that the authentication of a Public User Identity - Private User Identity pair is pending and waiting for confirmation.

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: Public Identity is not Registered and has no S-CSCF assigned.

Private Identity: Either a Private User Identity or a Private Service Identity.

Public Identity: Either a Public User Identity or a Public Service Identity.

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 Public Identity is unregistered.

Registered State: Public User Identity 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 Identities in the S-CSCF. iFCs from the unregistered part need not be evaluated when the Public User Identity is registered.

Unregistered State: Public Identity 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
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IP	Internet Protocol
I-CSCF	Interrogating CSCF
IM	IP Multimedia
IMS	IP Multimedia Subsystem

LIA	Location Information Answer
LIR	Location Information Request
MAA	Multimedia Authentication Answer
MAR	Multimedia Authentication Request
MT	Mobile Terminating
P-CSCF	Proxy CSCF
PPA	Push Profile Answer
PPR	Push Profile Request
RTA	Registration Termination Answer
RTR	Registration Termination Request
SAA	Server Assignment Answer
SAR	Server Assignment Request
SIP	Session Initiation Protocol
S-CSCF	Serving CSCF
SLF	Server Locator Function
UAA	User Authorization Answer
UAR	User Authorization Request

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 and procedures are also included.

The IP Multimedia (IM) Subsystem stage 2 is specified in [1] and the protocol for the IP multimedia call control based on SIP and SDP are specified in [8].

5 General architecture

This clause further specifies the architectural assumptions associated with the Cx reference point, building on the IP Multimedia (IM) Subsystem stage 2 specified in [1] and also the Px reference point building upon [10].

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 [19].

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 [19].

5.1.4 Functional requirements of HSS

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

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.
3. User authentication procedures

NOTE: IMS restoration procedures are not defined in this version of the specification.

5.1.6 Functional Requirements of the Presentity Presence Proxy

The interaction between the Presentity Presence Proxy and the HSS, referred to as the Px interface, is handled using the mechanisms defined for the Cx interface.

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 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 [11] chapter 19.1.4 shall apply.

Unknown permanent failure error codes shall be treated in the same way as DIAMETER_UNABLE_TO_COMPLY. For unknown transient failure error codes the request may be repeated, or handled in the same way as DIAMETER_UNABLE_TO_COMPLY

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 [1]) and is used:

- To authorize the registration of the Public User Identity, checking multimedia subsystem access permissions and roaming agreements.

- To perform a first security check, determining whether the Public User Identity in the message is associated with the Private User Identity sent in the message.

- To obtain either the S-CSCF where 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), 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 [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	Public User 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, 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 S-CSCF currently assigned to the Public User Identity in the HSS, cannot be contacted and a new S-CSCF needs to be selected.
Private User Identity (See 7.3)	User-Name	M	Private User 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.

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 IMS Subscription.
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 [5]):

1. Check that the Private User Identity and the Public User Identity exists in the HSS. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check that the Public User Identity received in the request is associated with the Private User Identity received in the request. If not, Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. Check whether the Public User 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 User 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 Public User Identity is allowed to roam in the visited network (if not, Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED and processing should stop) and authorized to register (if not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED and processing should stop). 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 Public User Identity 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 all the requirements of all the service profiles associated with the IMS subscription. 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 User 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. In case the User-Authorization-Type is equal to REGISTRATION or is absent,   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, the

HSS shall return the stored S-CSCF name and the Result-Code shall be set to DIAMETER_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION or is absent, then 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.

+ 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 or is absent, then the HSS shall check if there is at least one Public User Identity within the IMS Subscription with an S-CSCF name assigned.

    – If there is at least one Public User Identity within the IMS Subscription that is registered the HSS shall return the S-CSCF name assigned for that Public User Identity and Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

    – If there is at least one Public User Identity within the IMS Subscription 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 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.

    – If there is no identity of the user within the same IMS Subscription that is registered or unregistered, the HSS shall check if there is an S-CSCF name stored for the user (e.g. the user is being authenticated by the S-CSCF). If it is, the HSS shall return the stored S-CSCF name and Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

    – If there is not any Public User Identity within the IMS Subscription 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 all the requirements of all the service profiles associated with the IMS subscription. 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 fulfill 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 [1]) and is used:

- To assign an S-CSCF to a Public Identity, or to clear the name of the S-CSCF assigned to one or more Public Identities.

- To download from HSS the relevant user profile information for the S-CSCF.

This procedure is mapped to the commands Server-Assignment-Request/Answer in the Diameter application specified in [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 / Public Service Identity (See 7.2 and 7.2a)	Public-Identity	C	Public Identity or list of Public Identities. One and only one Public Identity shall be present if the Server-Assignment-Type is any value other than TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA, TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME, USER_DEREGISTRATION_STORE_SERVER_NAME or ADMINISTRATIVE_DEREGISTRATION. If Server-Assignment-Type indicates deregistration of some type and Private Identity is not present in the request, at least one Public Identity shall be present.
S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity / Private Service Identity (See 7.3 and 7.3a)	User-Name	C	Private Identity. It shall be present if it is available when the S-CSCF issues the request. It may be absent during the initiation of a session to an unregistered Public Identity. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER. In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public Identity AVPs are present then the User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server-Assignment-Type	M	Type of update that the S-CSCF requests in the HSS (e.g: de-registration). See [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. In the case where Server-Assignment-Type is not equal to NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER, the HSS shall not use User Data Already Available when processing the request.
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 Public Identity. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node 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 / Private Service Identity (See 7.3 and 7.3a)	User-Name	C	Private 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 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 Private Identity with Server-Assignment-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 [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, either the Primary-Charging-Collection-Function-Name AVP or the Primary-Event-Charging-Function-Name AVP shall be included. All other elements shall be included if they are available.
Associated Private Identities	Associated-Identities	O	This AVP contains all Private Identities, which belong to the same IMS subscription as the Private Identity or Public Identity received in the SAR command. If the IMS subscription contains only single Private Identity this AVP shall not be present.

6.1.2.1 Detailed behaviour

On registering/deregistering a Public Identity, the S-CSCF shall inform the HSS. The same procedure is used by the S-CSCF to get the user information which contains the user profile and the charging information. The relevant user profile downloaded is described in more detailed in sections 6.5.1 and 6.6. The Public-Identity AVP and User-Data AVPs in this command pair shall contain only one type of identities i.e. either only Public User Identities, or only Public Service Identities. The HSS holds information about the state of registration of all the identities related to an IMS Subscription. The S-CSCF uses this procedure to update such states. For Shared Public User Identities, the S-CSCF shall initiate this procedure towards the HSS for each Private User Identity undergoing a Registration or Deregistration related to the Shared Public User Identity. 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 [5]):

1. Check that the Public Identity and Private Identity exist in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS may check whether the Private and Public Identities received in the request are associated in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. If more than one Public-Identity AVP is present and the Server-Assignment-Type is one of the values defined in Table 6.1.2.1 as applying for only one identity, then the Result Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and no user information shall be returned.

4. If the identity in the request is a Public Service Identity, then check if the PSI Activation State for that identity is active. If not, then the response shall contain Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN.

5. 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 the Public User Identity’s authentication pending flag which is specific for the Private User Identity is set, the HSS shall clear it. 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). If there are multiple Private User Identities, which belong to the served IMS subscription the Associated-Identities AVP should be added to the answer message and it shall contain all Private User Identities associated to the IMS subscription.

   + If it indicates UNREGISTERED_USER, the HSS shall store the S-CSCF name, set the registration state of the Public Identity as unregistered, i.e. registered as a consequence of a terminating call and download the relevant user information. If there are multiple Private User Identities associated to the Public User Identity in the HSS, the HSS shall arbitrarily select one of the Private User Identities and put it into the response message. The Result-Code shall be set to DIAMETER_SUCCESS. If there are multiple Private User Identities, which belong to the served IMS subscription the Associated-Identities AVP should be added to the answer message and it shall contain all Private User Identities associated to the IMS subscription.

     If the HSS sends a Wildcarded PSI in the response, the S-CSCF may do the wildcard matching using the wildcarded PSI received in this first Server-Assignment-Answer and omit the Server-Assignment-Request for subsequent requests matching the same wildcarded PSI.

   + If it indicates TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA or ADMINISTRATIVE_DEREGISTRATION, the HSS shall check the registration state for all the Public Identities in the request. If the request did not contain Public Identities the HSS shall check the registration state of the Public Identities associated with the Private Identity identified in the request. For each Public Identity;

     - if the registration state of the Public User Identity is Registered, the HSS shall check if the Public User Identity is currently registered with one or more Private User Identities.

- If the Public User Identity is currently registered with only one Private User Identity, the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name associated with the Public User Identity.

- If the Public User Identity is currently registered with more than one Private User Identity, the HSS shall keep the registration state of the Public User Identity as Registered and retain the S-CSCF name associated with the Public User Identity.

- if the registration state of the Public Identity is Unregistered, the HSS shall set the registration state of the Public Identity to Not Registered and clear the S-CSCF name associated with the Public Identity.

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 associated to the Private User Identity 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 decides to keep the S-CSCF name stored, the HSS shall keep the S-CSCF name stored for all the Public User Identities associated to the Private User Identity. The Result-Code shall be set to DIAMETER_SUCCESS.

  The HSS shall check if each Public User Identity in the request is currently registered with one or more Private User Identities. If the request did not contain Public User Identities the HSS shall check if each Public User Identity associated with the Private User Identity in the request is currently registered with one or more Private User Identities. For each Public User Identity;

  - If only one Private User Identity associated with the Public User Identity is currently registered with the Public User Identity, the HSS shall set the registration state of the Public User Identity to Unregistered.

  - If more than one Private User Identity that shares that Public User Identity is currently registered with the Public User Identity the HSS shall keep the registration state of the Public User Identity as Registered.

- 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.

  The HSS shall check if each Public User Identity in the request is currently registered with one or more Private User Identities. If the request did not contain Public User Identities the HSS shall check if each Public User Identity associated with the Private User Identity in the request is currently registered with one or more Private User Identities. For each Public User Identity;

  - If only one Private User Identity associated with the Public User Identity is currently registered with the Public User Identity, the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name associated with Public User Identity.

  - If more than one Private User Identity that shares that Public User Identity is currently registered with the Public User Identity the HSS shall keep the registration state of the Public User Identity as Registered.

+ If it indicates NO_ASSIGNMENT, the HSS checks whether the Public Identity 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. If there are multiple Private User Identities, which belong to the served IMS subscription the Associated-Identities AVP should be added to the answer message and it shall contain all Private User Identities associated to the IMS subscription.

+ If it indicates AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the HSS shall keep the registration state of the Public User Identity. The HSS shall check the registration state for the Public User Identity in the request and only if the registration state of the Public User Identity is Not Registered, the HSS shall clear the S-CSCF name associated with the Public User Identity.

If the Public User Identity's authentication pending flag which is specific for the Private User Identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER_SUCCESS.

If the HSS cannot fulfill 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 registration state nor download any Public Identity information to the S-CSCF.

See section 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 Public Identity.

6.1.3 Network initiated de-registration by the HSS, administrative

In case of network initiated de-registration by the HSS, the HSS shall change the state of the Public Identities to Not Registered and send a notification to the S-CSCF indicating the identities that shall be de-registered. The procedure is invoked by the HSS and corresponds to the functional level operation Cx-Deregister (see [1]).

This procedure is mapped to the commands Registration-Termination-Request/Answer in the Diameter application specified in [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 / Public Service Identity (See 7.2 and 7.2a)	Public-Identity	C	It contains the list of Public Identities that are de-registered, in the form of SIP URL or TEL URL. Public-Identity AVP shall be present if the de-registration reason code is NEW_SERVER_ASSIGNED. It may be present with the other reason codes.
Private User Identity / Private Service Identity (See 7.3 and 7.3a)	User-Name	M	It contains the Private Identity in the form of a NAI. The HSS shall always send a Private Identity that is known to the S-CSCF based on an earlier SAR/SAA procedure.
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 [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 IMS Subscription. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.
Associated Private Identities	Associated-Identities	O	This AVP contains Private Identities, which belong to the same IMS subscription as the Private Identity in the User-Name AVP and should be de-registered together with that one. If the IMS subscription contains only a single Private Identity, this AVP shall not be present.

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.
Associated Private Identities	Associated-Identities	C	This AVP shall be present if the S-CSCF de-registered more than one Private Identity with the request. It contains all Private Identities that have been deregistered together with the one in the User-Name AVP of the request.

6.1.3.1 Detailed behaviour

The HSS shall de-register the affected identities and invoke this procedure to inform the S-CSCF. The S-CSCF shall remove all the information stored in the S-CSCF for the affected identities.

The HSS may de-register:

- One Public Identity or a list of Public Identities. HSS may include all Public User Identities associated with the User-Name AVP to the request. This option is applicable with all reason codes.
- One or more Private Identities of the IMS Subscription with all associated Public Identities. No Public-Identity AVPs shall be present in this case. This option is applicable with reason codes PERMANENT_TERMINATION, SERVER_CHANGE, and REMOVE_S-CSCF.
- All Public Service Identities that match a Wildcarded Public Service Identity. In this case the HSS may send one of the Public Service Identities that was received in the Server Assignment Request for that Wildcarded Public Service Identity and the associated Private Service Identity.

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 HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to the Public Identity and associated implicitly registered Public Identities for the Private Identity(ies) indicated in the request (e.g. due to an IMS subscription modification).

  The HSS shall check the registration state of the Public Identities. If no Public Identities are involved, the HSS shall check the registration state of the Public Identities associated with the Private User Identity identified. For each Public Identity;

  - If the registration state of the Public Identity is Registered, the HSS shall check if the Public User Identity is currently registered with one or more Private User Identities.
    - If the Public User Identity is currently registered with only one Private User Identity, the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name associated with the Public User Identity. The S-CSCF initiates the de-registration of the Public User Identity.
    - If the Public User Identity is currently registered with more than one Private User Identity, the HSS shall keep the registration state of the Public User Identity as Registered and retain the S-CSCF name associated with the Public User Identity. The S-CSCF initiates the de-registration of the Public User Identity.
  - If the registration state of the Public Identity is Unregistered, the HSS shall set the registration state of the Public Identity to Not Registered and clear the S-CSCF name associated with the Public Identity.
- NEW_SERVER_ASSIGNED: The HSS indicates to the S-CSCF that a new S-CSCF has been allocated to the IMS Subscription (e.g., because the previous assigned S-CSCF was unavailable during a registration procedure). The S-CSCF shall remove all information for all of the Public Identities indicated in the request.
- SERVER_CHANGE: The HSS indicates to the S-CSCF that the de-registration is requested to force the selection of new S-CSCF to assign to the IMS Subscription (e.g., when the 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 HSS shall set the registration state to "Not Registered" and clear the S-CSCF name for all of the Public Identities affected by the request . If the S-CSCF does not indicate in the response all the Private Identities that were in the request the HSS shall repeat this request for each of the remaining Private Identities in the IMS Subscription that are known to the S-CSCF. The S-CSCF should start the network initiated de-registration towards the user, i.e.

all registrations within the IMS Subscription 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 will no longer be assigned to an unregistered Public Identity(ies) (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored) for a given IMS Subscription. For each Public Identity contained within the request the HSS shall set the registration state of the Public Identity to Not Registered and clear the S-CSCF name associated with the Public Identity. The S-CSCF shall remove all information related to the Public User Identity contained within the request.

The detailed de-registration procedures performed by the S-CSCF for each reason code are described in [8].

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 assigned to a Public Identity. The procedure invoked by the I-CSCF is performed per Public Identity, and corresponds to the functional level operation Cx-Location-Query (see [1]).

This procedure is mapped to the commands Location-Info-Request/Answer in the Diameter application specified in [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 / Public Service Identity (See 7.2 and 7.2a)	Public-Identity	M	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 based on the Diameter routing table in the I-CSCF.

Table 6.1.4.2 : User Location response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / 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, AS Name (See 7.4 and 7.4a)	Server-Name	C	Name of the assigned S-CSCF for basic IMS routing or the name of the AS for direct routing.

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 (if an error occurs in any of the steps the HSS shall stop processing and return the corresponding error code, see [5]):

1. Check that the Public Identity is known. If not the Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. If the identity in the request is a Public Service Identity, then check if the PSI Activation State for that identity is active. If not, then the response shall contain Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN.

3. Check the state of the Public Identity received in the request, and where necessary, check if the Public Identity has services related to the unregistered state.

   + If it is registered, or 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 has services related to the unregistered state, 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 Public Identity within the IMS Subscription with an S-CSCF name assigned:

     - If this is the case the HSS shall return the S-CSCF name assigned for that Public Identity. 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 to a Public Identity within the IMS Subscription , 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 for the IMS Subscription.. The Server-Name AVP shall not be present. The Experimental-Result-Code shall be set to DIAMETER_UNREGISTERED_SERVICE.

   + If it is not registered or unregistered and if it has no services related to the unregistered state, 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 ([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 [1]).

This procedure is mapped to the commands Push-Profile-Request/Answer in the Diameter application specified in [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 / Private Service Identity (See 7.3 and 7.3a)	User-Name	M	Private Identity. The HSS shall always send a Private Identity that is known to the S-CSCF based on an earlier SAR/SAA procedure.
User Profile (See 7.7)	User-Data	C	Updated user profile (see sections 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 addresses are changed in the HSS. If the Charging-Information AVP is not present, the User-Data AVP shall be present. When this parameter is included, either the Primary-Charging-Collection-Function-Name AVP or the Primary-Event-Charging-Function-Name AVP shall be included. All other charging information shall be included if it is 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 IMS Subscription. 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 the relevant user information to the S-CSCF. The user information contains the user profile. See sections 6.5.2.1 and 6.6.1 for the rules of user profile updating. If there are multiple registered Private User Identities associated to the Public User Identity in the HSS, the HSS shall send only single request and select arbitrarily one of the Private User Identities and put it into the request. For updates of the profile of a Wildcarded Public Service Identity, the HSS shall send only one single request. That request shall contain the Wildcarded Public Service Identity (content within the Identity tag in the XML data shall be ignored by the S-CSCF)

The Charging-Information AVP and/or the User-Data AVP shall be present in the request. If the User-Data AVP is present in the request, the S-CSCF shall overwrite, for the Public Identities indicated in the User profile included 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 Charging-Information AVP is present in the request, the S-CSCF shall replace the existing charging information with the information received from the HSS.

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 IMS Subscription. 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.

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/Experimental-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 information, which was not recognized or supported by the S-CSCF due to unsupported S-CSCF capabilities.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the Private Identity or one of the Public Identities 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-AV-Req-Resp (see [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 [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 User Identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the Private User 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 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. If the authentication scheme is Digest-AKA, this information element 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. If the authentication scheme is Digest-AKA, this information element shall contain "Digest-AKAv1-MD5".
Authorization Information (See 7.9.4)	SIP-Authorization	M	If the authentication scheme is Digest-AKA, it shall contain the concatenation of RAND, as sent to the terminal, and AUTS, as received from the terminal. RAND and AUTS shall both be binary encoded. See [3] for further details about RAND and AUTS.

Table 6.3.4: Authentication Request Response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	C	Public User Identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity (See 7.3)	User-Name	C	Private User 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. If the authentication scheme is Digest-AKA, this information element 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 [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 [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. The use of this key for algorithms other than “Digest-AKAv1-MD5” is not specified in this document.

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 [5]):

1. Check that the Private User Identity and the Public User Identity exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check whether the Private and Public User Identities in the request are associated in the HSS. 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_NOT_SUPPORTED.

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 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

5. Check the registration status of the Public User 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. The HSS shall set the Public User

Identity's authentication pending flag which is specific to the Private User Identity received in the request. 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 an unregistered Public User Identity 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 Public User 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. The HSS shall set the Public User Identity's authentication pending flag which is specific to the Private User Identity which was received in the request. 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 HSS shall set the Public User Identity's authentication pending flag which is specific to the Private User Identity that was received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

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

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 Public 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 [1] is based on the Subscription Locator Function (SLF). The SLF shall act as either an enhanced Diameter redirect agent [9] or as a Diameter proxy [9] but not as both.

As an enhanced Diameter redirect agent the SLF 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 Public Identity 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 [1]. Further requests associated to the same user shall make use of the stored HSS address.

As a Diameter Proxy the SLF receives Cx requests from the I-CSCF and the S-CSCF, and proxies it to the HSS. The SLF using the extracted Public User Identity from the received requests determines the HSS address. The SLF based on the HSS address modifies the Destination-Realm AVP of the Cx_request as needed. Based on the HSS address, the SLF then adds the Destination-Host AVP to the Cx_request. The SLF appends a Route-Record AVP to the request and sends it to the HSS. The HSS resolves the Cx request and sends a Cx response. The Cx response contains the Origin-Realm AVP set to the HSS Realm value and Origin-Host AVP set to the HSS name. The Cx_response is routed back to the SLF. The SLF shall not modify the Origin-Realm and Origin-Host in the Cx_response. The SLF sends the Cx response back to the I-CSCF or S-CSCF. The I-CSCF and S-CSCF extract the HSS address/name from the Cx response. While the I-CSCF is stateless, the S-CSCF shall store the HSS address/name (i.e., the Origin-Realm AVP and the Origin-Host AVP in the Cx_Request), as specified in [1]. Further requests associated to the same user shall make use of the stored HSS address.

In networks where the use of the user identity to HSS resolution mechanism is required only one of the two SLF mechanisms shall be used. 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 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 User 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 authentication pending flag for a Public User Identity 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.

6.5.1.5 Initiation of a session to a non-registered user

The change of a Public Identity to the Unregistered state due to the initiation of a session to a Public User Identity that was in Not Registered state and the opposite change from Unregistered state to Not Registered state implies the same change for all the Public User Identities in the same Implicit Registration Set.

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.

This procedure shall be used by the HSS to add a newly provisioned or Not Registered Public User Identity or Identities to an existing implicitly registered Public User Identity set that is in the state Registered or Unregistered. The added Public User Identity gets the registration state of the set it is added to.

The HSS shall use this procedure if a Public User Identity or Identities are removed from the implicitly registered Public User Identity set that is in a state Registered or Unregistered. In practise, this is done by sending a PPR for the set without the removed identities. The S-CSCF shall remove all information stored in the S-CSCF for the removed identities.

The HSS shall not use this procedure if there is no Public User Identities left in the implicitly registered Public User Identity set after the removal. In that case the HSS shall use the RTR command instead.

The HSS shall not use this procedure to change the default Public User Identity of the implicitly registered Public User Identity set that is in a state Registered. In that case the HSS shall use the RTR command to de-register the Public User Identity set.

Moving of a Public User Identity or Identities from one implicitly registered Public User Identity set to another set shall be done in two steps: First the identity or identities are removed from the "old" set as described above, then the identity or identities are added to the "new" set as described above.

6.5.2.2 De-registration

A request sent by the HSS to de-register any of the identities included in an implicitly registered Public User Identity set shall affect 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 relevant user profile

The download of the relevant user profile from the HSS to the S-CSCF depends on whether the user profile is already stored in the S-CSCF. If the SiFC feature is supported by the HSS and S-CSCF, the HSS shall download the identifiers of the shared iFC sets. If either the HSS or the S-CSCF does not support the SiFC feature, the HSS shall download the complete iFCs, and SiFC identifiers shall not be downloaded by the HSS. The SiFC feature is defined in [5].

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 the user profile 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 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, the 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 the “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.

The following table is a guideline for operators that records S-CSCF capabilities that need to be supported by an S-CSCF in order to serve a user or a service (identified by a Public User Identity or Public Service Identity), that cannot be served by an S-CSCF which is only compliant to a previous 3GPP release.

Table 6.7 Guidelines for S-CSCF Capabilities

Capability	Mandatory or Optional (note 1)	
Support of "Wildcarded PSI"	M	This capability indicates that the assigned S-CSCF shall support the handling of Wildcarded PSIs.

Support of "Shared iFC sets"	O	This capability indicates that the assigned S-CSCF may support the "SiFC" feature defined in the [5].
Note 1: Mandatory (M) corresponds to Mandatory Capability that shall be supported by the assigned S-CSCF for a given user. The I-CSCF shall not select an S-CSCF that does not meet a mandatory capability. The selection of a S-CSCF not supporting this capability would lead to an unspecified network behaviour. Optional (O) corresponds to an Optional Capability that may be supported by the assigned S-CSCF for a given user. The selection of a S-CSCF that would not support this capability will not significantly affect the network behaviour.		

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 User Identity. For definition of a Public User Identity, see [17].

7.2a Public Service Identity

This information element contains a Public Service Identity (PSI) that is hosted by an application server. For definition of a PSI, see [17].

7.3 Private User Identity

This information element contains the Private User Identity. For definition of a Private User Identity, see [17].

7.3a Private Service Identity

This information element contains the Private Service Identity. For definition of a Private Service Identity, see [17].

7.4 S-CSCF Name

This information element contains the S-CSCF Name of the S-CSCF assigned to an IMS Subscription. For definition of a S-CSCF Name, see [18].

7.4a AS Name

This information element contains the AS Name of the AS hosting a Public Service Identity. For definition of AS Name, see [18].

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 IMS Subscription.

7.6 Result

This information element contains result of an operation. See [5] for a list of values.

7.7 User Profile

This information element contains the user profile in XML format. The user profile XML shall be validated against the user profile XML schema defined in Annex E.

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

Annex D contains an informative, high level representation, of the wire representation of user profile data.

7.8 Server Assignment Type

Indicates the type of server assignment. See [5] for a list of 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.

If the authentication scheme is Digest-AKA, the scheme is “Digest-AKAv1-MD5”.

7.9.3 Authentication Information

This information element is used to convey the challenge and authentication token used during the authentication procedure. See [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 [3].

7.9.5 Confidentiality Key

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

7.9.6 Integrity Key

This information element contains the integrity key. See [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 [16], 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. See [5] for a list of values.

7.12 Charging information

Addresses of the charging functions. See [5].

7.13 Routing information

Information to route requests.

7.14 Type of Authorization

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

7.15 Void

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 [5] for a list of values.

7.17 Associated Private Identities

This information element indicates to the S-CSCF the Private Identities, which belong to the same IMS Subscription as the Private Identity received in the request command. See [5].

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 User Identity, which is registered in the new S-CSCF.

2. Deregistration-Reason AVP value set to SERVER_CHANGE, for the Public User 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 the 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 Public User Identity 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 [5].

10 Operational aspects

See [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 [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
Location Query + Cx-LocQuery	I-CSCF	HSS	Location-Info-Request	LIR
Cx-LocQueryResp+Response	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

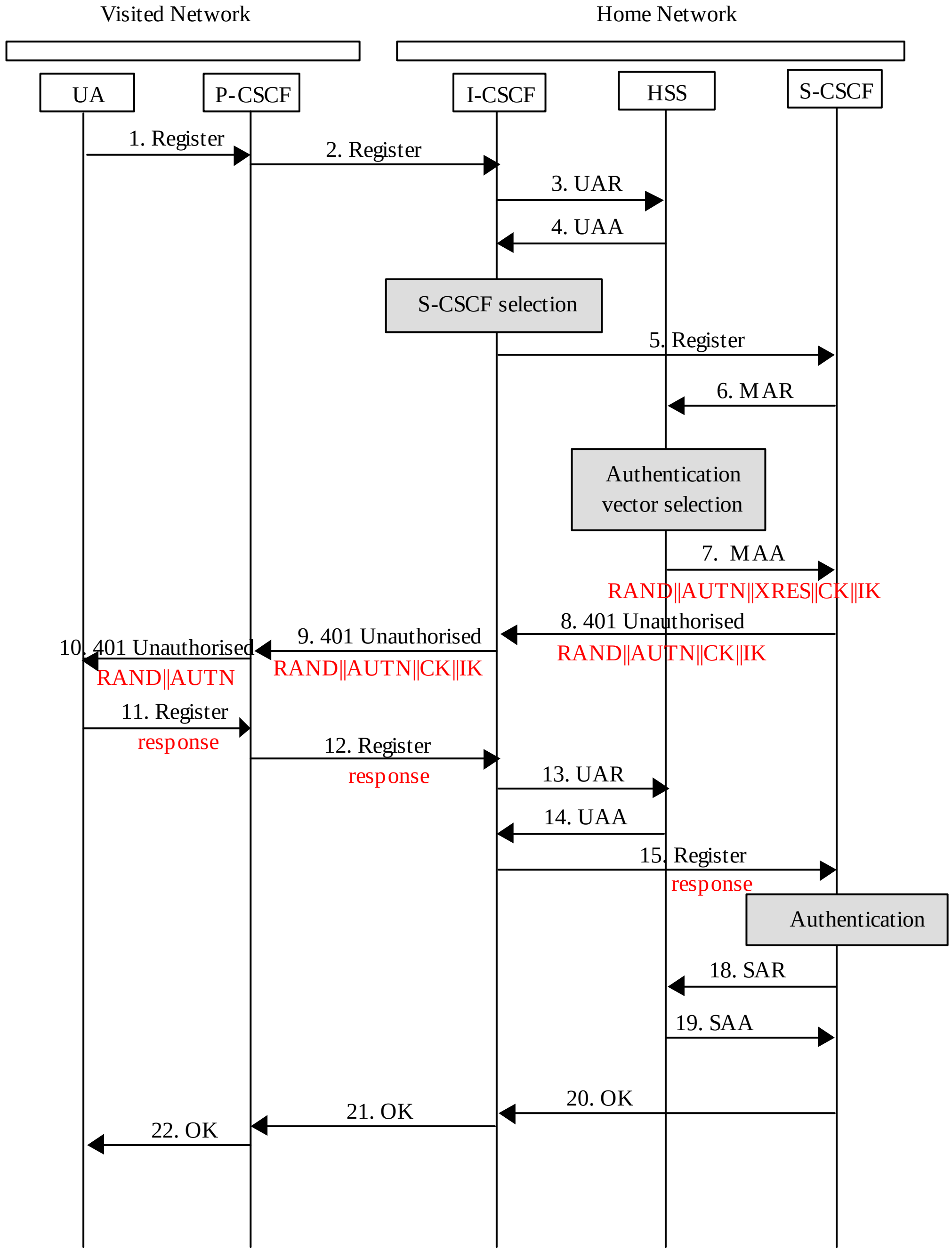
Cx parameter	AVP Name
Visited Network Identifier	Visited-Network-Identifier
Public User Identity	Public-Identity
Private User Identity	User-Name
S-CSCF Name	Server-Name
AS Name	
S-CSCF Capabilities	Server-Capabilities
Result	Result-Code
	Experimental-Result-Code
User Profile	User-Data
Server Assignment 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
Associated Private Identities	Associated-Identities

A.4 Message flows

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

1 ### A.4.1 Registration– user not registered

2



3

4 **Figure A.4.1.1: Registration – user not registered**

5

A.4.2 Registration – user currently registered

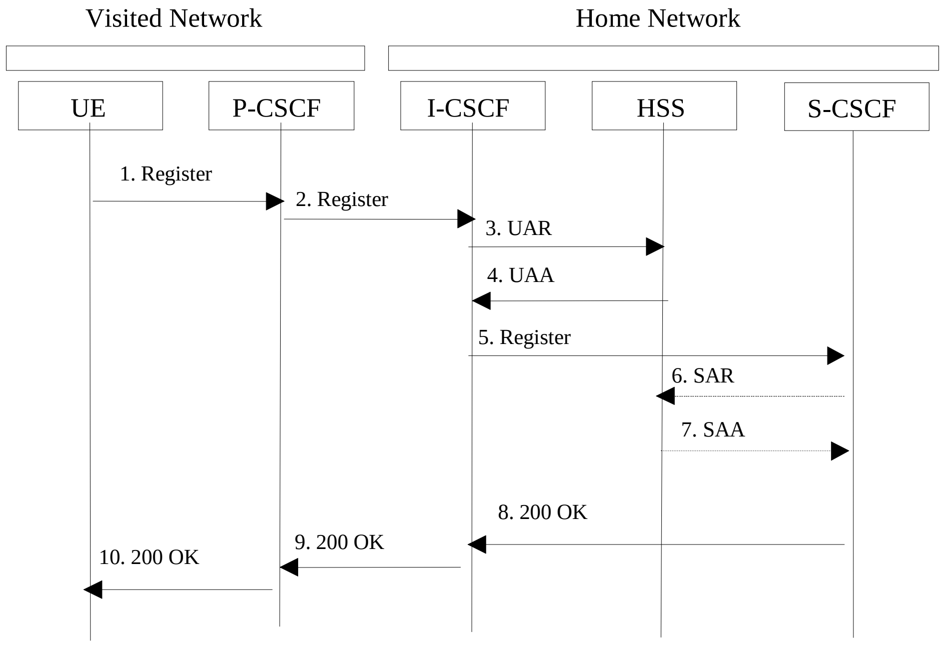


Figure A.4.2.1: Re-registration

A.4.3 Mobile initiated de-registration

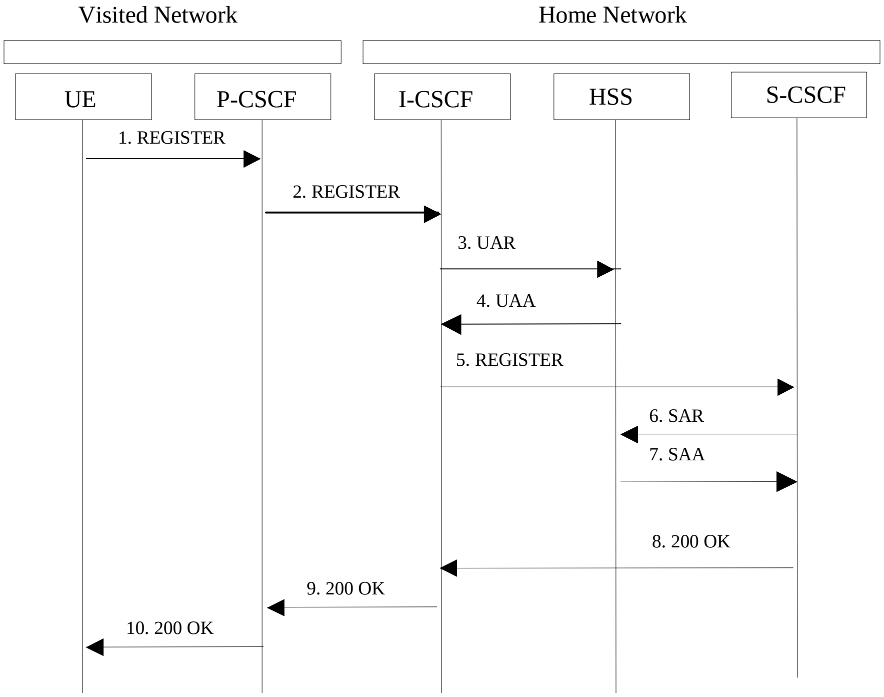


Figure A.4.3.1: Mobile initiated de-registration

A.4.4 Network initiated de-registration

A.4.4.1 Registration timeout

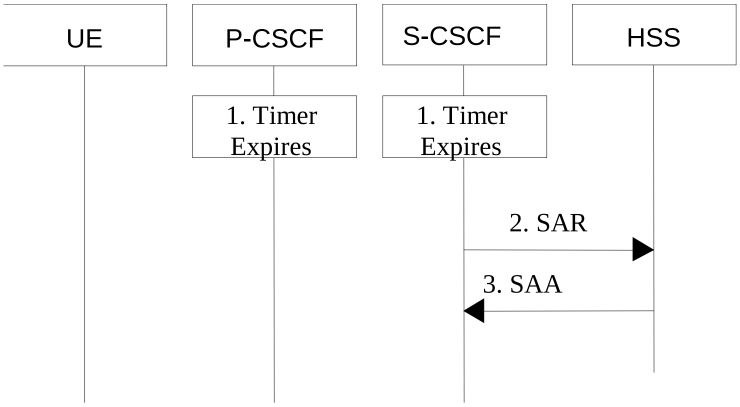


Figure A.4.4.1.1: Network initiated de-registration – registration timeout

A.4.4.2 Administrative de-registration

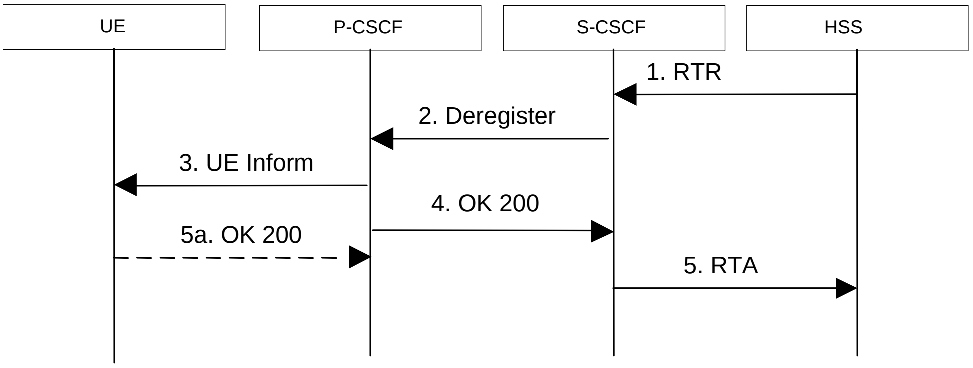


Figure A.4.4.2.1: Network initiated de-registration – administrative de-registration

A.4.4.3 De-registration initiated by service platform

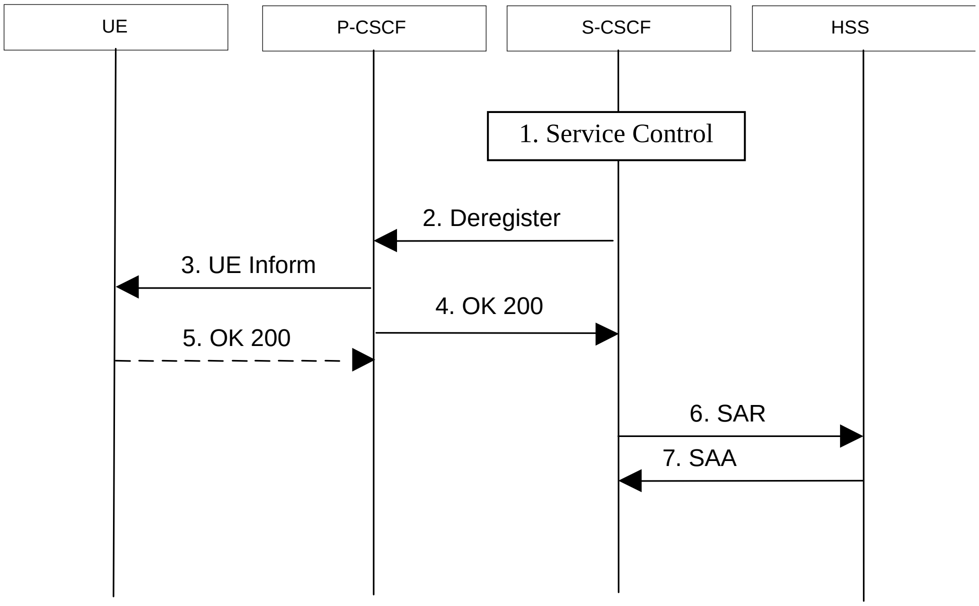


Figure A.4.4.3.1: Network initiated de-registration – initiated by service platform

A.4.5 MT SIP session set-up

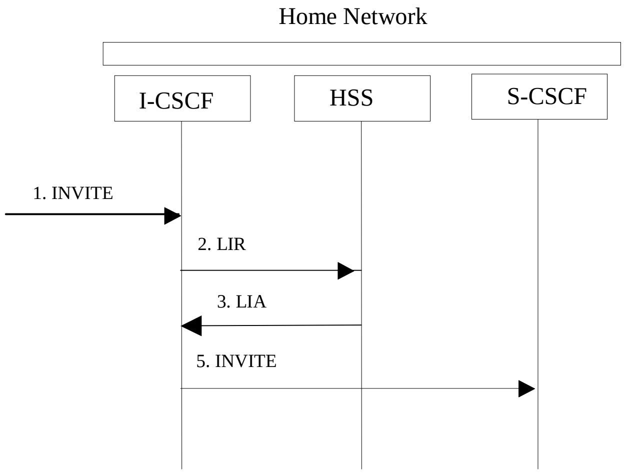


Figure A.4.5.1: MT SIP session set-up

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

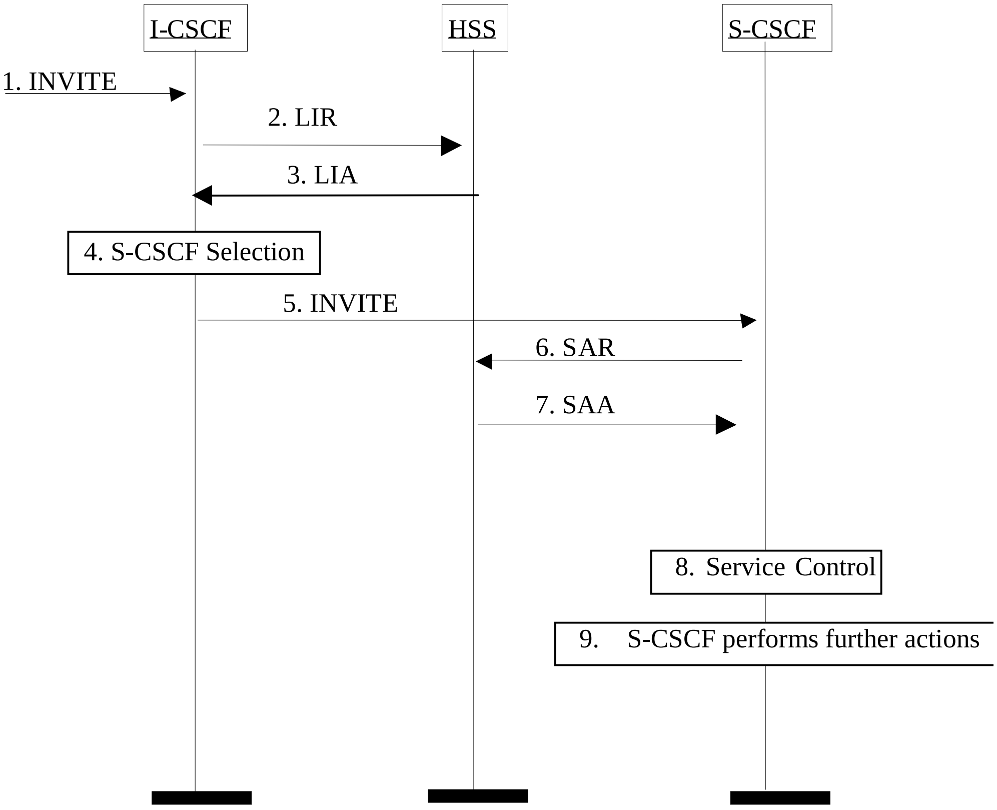


Figure A.4.6.1: Initiation of a session to a non-registered user

A.4.7 User Profile update

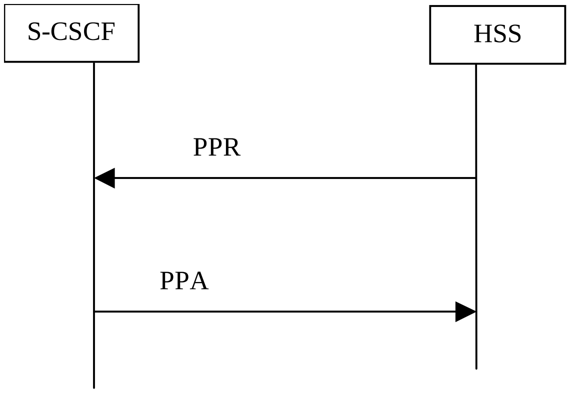


Figure A.4.7.1: User Profile update

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:

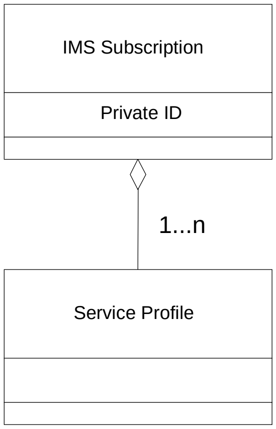


Figure B.1.1: User Profile

IMS Subscription class contains as a parameter the Private User Identity in NAI format.

Each instance of the IMS Subscription class contains one or several instances of the class Service Profile.

B.2 Service profile

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

:

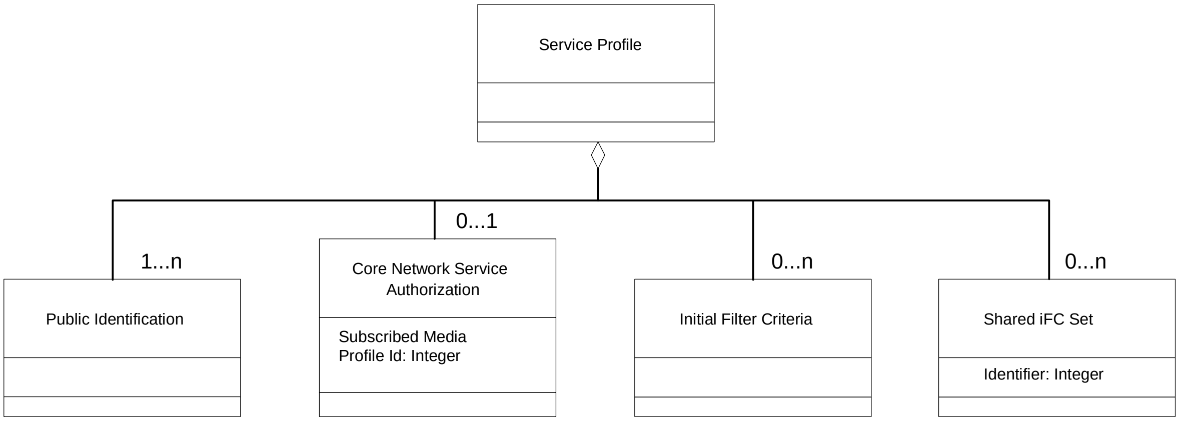


Figure B.2.1: Service Profile

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 associated with that service profile. The information in the Core Network Service Authorization Initial Filter Criteria, and Shared iFC Set classes apply to all Public Identification instances, which are included in one Service profile class.

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

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

B.2.1 Public Identification

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

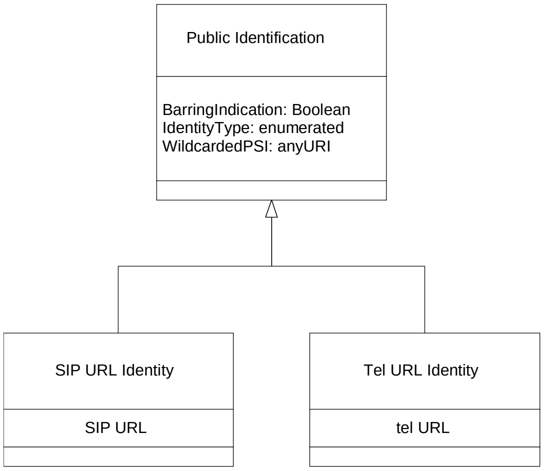


Figure B.2.1.1: Public Identification

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 absent, or if it is present and set to FALSE, the S-CSCF shall not restrict the use of that public user identity in any IMS communications. If it is present and set to TRUE, the S-CSCF shall prevent that public user identity from being used in any IMS communication except registrations and re-registrations, as specified in [8].

The attribute IdentityType indicates if the identity is a Public User Identity, a distinct Public Service Identity or a Public Service Identity matching a Wildcarded Public Service Identity. If the identity type is not present, it is assumed to be Public User Identity.

The attribute WildcardedPSI shall be present and contain the Wildcarded Public Service Identity that matched the Public Service Identity if the identity is a Public Service Identity matching a Wildcarded Public Service Identity. This Wildcarded Public Service identity shall be sent as stored in the HSS, that is including the delimiter described in [17].

B.2.2 Initial Filter Criteria

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

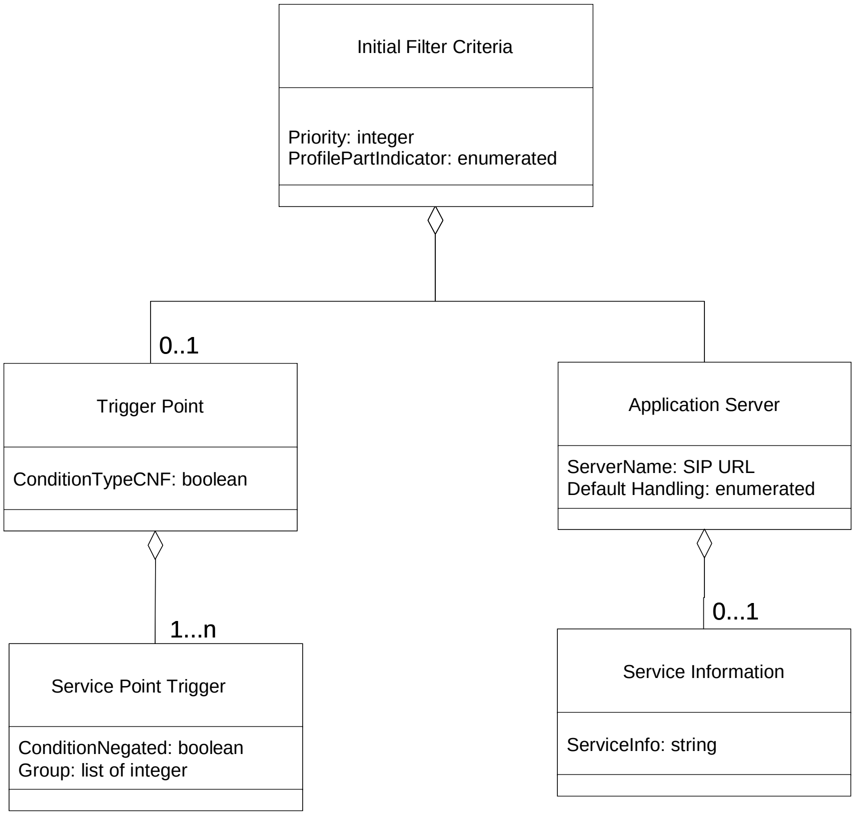


Figure B.2.2.1: Initial Filter Criteria

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 Conjunctive or Disjunctive Normal form (CNF or 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 SPT statements 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. Default Handling determines whether the dialog should be released if the Application Server could not be reached or not; it is of type enumerated and can take the values: SESSION_CONTINUED or SESSION_TERMINATED.

The Application Server class contains zero or one instance of the Service Information class. Service Information class allows to download to S-CSCF information that is to be transferred transparently to an Application Server when the trigger points of a filter criterion are satisfied. ServiceInformation is a string conveying that information. See [6] 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:

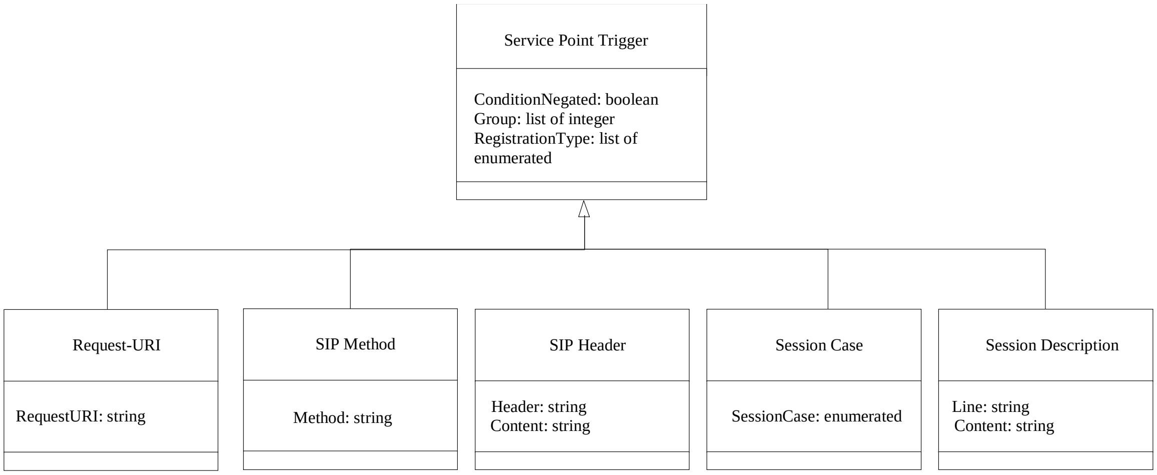


Figure B.2.3.1: Service Point Trigger

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 SPT belongs to different ORed sets, SPT can 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 SPT belongs to different ANDed sets, SPT can have more than one Group values assigned. At least one Group must be assigned for each SPT.

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

The attribute RegistrationType of the class Service Point Trigger is relevant only to the SIP Method SPT with a value of "REGISTER" and its' support is optional in the HSS and in the S-CSCF. The RegistrationType may contain a list of values that define whether the SPT matches to REGISTER messages that are related to initial registrations, re-registrations, and/or de-registrations. If RegistrationTypes are given, the SIP Method SPT with a value of "REGISTER" shall match if any of the RegistrationTypes match and the S-CSCF supports the RegistrationType attribute. If the SIP Method SPT contains value “REGISTER”, and no RegistrationType is given, or if the S-CSCF does not support the RegistrationType attribute, the SIP Method SPT matches to all REGISTER messages. The attribute RegistrationType may be discarded if it is present in an SPT other than SIP Method with value "REGISTER".

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 Method which holds the name of to any 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 SPT is 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 SPT for the content of any SDP field within the body of a SIP Method. The Line attribute identifies the line inside the session description. Content is a string defining the content of the line identified by Line.

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”?>

<IMSSubscription xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xsi:noNamespaceSchemaLocation=”D:\ \CxDataType.xsd”>

        <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>
                <DefaultHandling >0</DefaultHandling>
            </ApplicationServer>
        </InitialFilterCriteria>
    </ServiceProfile>
</IMSSubscription>
```

A Boolean expression is said to be in Disjunctive Normal Form if it is expressed as a disjunction of conjunctions 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”?>
<IMSSubscription xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance”
xsi:noNamespaceSchemaLocation=”D:\ CxDataType.xsd”>
    <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>
```

```
                <DefaultHandling >0</DefaultHandling>
            </ApplicationServer>
        </InitialFilterCriteria>
    </ServiceProfile>
</IMSSubscription>
```

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

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

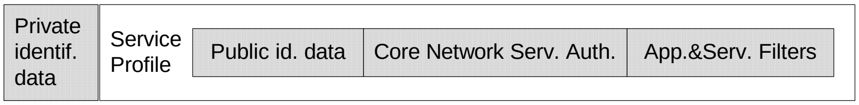


Figure D.1: Example of in-line format of user profile

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

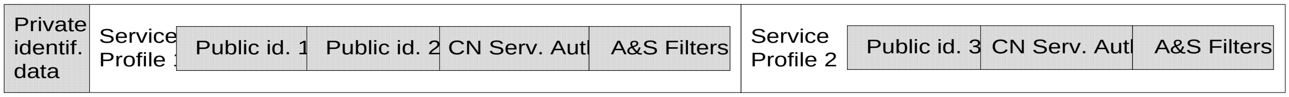


Figure D.2: Example of in-line format of user profile

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

The file CxDataType_Rel6.xsd, attached to this specification, contains the XML schema for the user profile that is sent over the Cx interface. The user profile XML schema defines the data types that are used in the user profile XML. The data that is allowed to be sent in the user profile may vary depending on the features supported by the Diameter end points, see 3GPP TS 29.229 [5]. The user profile XML schema file is intended to be used by an XML parser. The version of the Cx application sending the user profile XML shall be the same as the version of the sent user profile XML and thus it implies the version of the user profile XML schema to be used to validate it.

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

1 **Table E.1: XML schema for the Cx interface user profile: simple data types**

Data type	Tag	Base type	Comments
tPriority	Priority	integer	>= 0
tProfilePartIndicator	ProfilePartIndicator	enumerated	Possible values: 0 (REGISTERED) 1 (UNREGISTERED)
tSharedIFCSetID	SharedIFCSetID	integer	>= 0
tGroupID	Group	integer	>= 0
tRegistrationType	RegistrationType	enumerated	Possible values: 0 (INITIAL_REGISTRATION) 1 (RE-REGISTRATION) 2 (DE-REGISTRATION)
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 [14]
tSIP_URL	Identity	anyURI	Syntax described in [11]
tTEL_URL	Identity	anyURI	Syntax described in [15]
tIdentity	Identity	(union)	Union of tSIP_URL and tTEL_URL
tIdentityType	IdentityType	enumerated	Possible values: 0 (PUBLIC_USER_IDENTITY) 1 (DISTINCT_PSI)

			2 (WILDCARDED_PSI)
tWildcardedPSI	WildcardedPSI	anyURI	Syntax described in [17].
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

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

Data type	Tag	Compound of		
		Tag	Type	Cardinality
tIMSSubscription	IMSSubscription	PrivateID	tPrivateID	1
		ServiceProfile	tServiceProfile	(1 to n)
tServiceProfile	ServiceProfile	PublicIdentity	tPublicIdentity	(1 to n)
		InitialFilterCriteria	tInitialFilterCriteria	(0 to n)
		CoreNetworkServicesAuthorization	tCoreNetworkServicesAuthorization	(0 to 1)
		Extension	tServiceProfileExtension	(0 to 1)
tServiceProfileExtension	Extension	SharedIFCSetID	tSharedIFCSetID	(0 to n)
tCoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	SubscribedMediaProfileId	tSubscribedMediaProfileId	(0 to 1)
tPublicIdentity	PublicIdentity	BarringIndication	tBool	(0 to 1)
		Identity	tIdentity	1
		Extension	tPublicIdentityExtension	(0 to 1)

<table>
<tr><td rowspan="4">tInitialFilterCriteria</td><td rowspan="4">InitialFilterCriteria</td><td colspan="2">Priority</td><td>tPriority</td><td>1</td></tr>
<tr><td colspan="2">TriggerPoint</td><td>tTrigger</td><td>(0 to 1)</td></tr>
<tr><td colspan="2">ApplicationServer</td><td>tApplicationServer</td><td>1</td></tr>
<tr><td colspan="2">ProfilePartIndicator</td><td>tProfilePartIndicator</td><td>(0 to 1)</td></tr>
<tr><td rowspan="2">tTrigger</td><td rowspan="2">TriggerPoint</td><td colspan="2">ConditionTypeCNF</td><td>tBool</td><td>1</td></tr>
<tr><td colspan="2">SPT</td><td>tSePoTri</td><td>(1 to n)</td></tr>
<tr><td rowspan="8">tSePoTri</td><td rowspan="8">SPT</td><td colspan="2">ConditionNegated</td><td>tBool</td><td>(0 to 1)</td></tr>
<tr><td colspan="2">Group</td><td>tGroupID</td><td>(1 to n)</td></tr>
<tr><td rowspan="5">Choice of</td><td>RequestURI</td><td>tString</td><td>1</td></tr>
<tr><td>Method</td><td>tString</td><td>1</td></tr>
<tr><td>SIPHeader</td><td>tHeader</td><td>1</td></tr>
<tr><td>SessionCase</td><td>tDirectionOfRequest</td><td>1</td></tr>
<tr><td>SessionDescription</td><td>tSessionDescription</td><td>1</td></tr>
<tr><td colspan="2">Extension</td><td>tSePoTriExtension</td><td>(0 to 1)</td></tr>
<tr><td>tSePoTriExtension</td><td>Extension</td><td colspan="2">RegistrationType</td><td>tRegistrationType</td><td>(0 to 2)</td></tr>
<tr><td rowspan="2">tHeader</td><td rowspan="2">SIPHeader</td><td colspan="2">Header</td><td>tString</td><td>1</td></tr>
<tr><td colspan="2">Content</td><td>tString</td><td>(0 to 1)</td></tr>
<tr><td rowspan="2">tSessionDescription</td><td rowspan="2">SessionDescription</td><td colspan="2">Line</td><td>tString</td><td>1</td></tr>
<tr><td colspan="2">Content</td><td>tString</td><td>(0 to 1)</td></tr>
<tr><td rowspan="3">tApplicationServer</td><td rowspan="3">ApplicationServer</td><td colspan="2">ServerName</td><td>tSIP_URL</td><td>1</td></tr>
<tr><td colspan="2">DefaultHandling</td><td>tDefaultHandling</td><td>(0 to 1)</td></tr>
<tr><td colspan="2">ServiceInfo</td><td>tServiceInfo</td><td>(0 to 1)</td></tr>
<tr><td rowspan="2">tPublicIdentityExtension</td><td rowspan="2">Extension</td><td colspan="2">IdentityType</td><td>tIdentityType</td><td>(0 to 1)</td></tr>
<tr><td colspan="2">WildcardedPSI</td><td>tWildcardedPSI</td><td>(0 to 1)</td></tr>
</table>

NOTE: “n” shall be interpreted as non-bounded.

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 [13]. The regular expression shall be matched against the header-name of the SIP header. For definition of header and header-name, see [11]. 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 [11].
Content (of SIPHeader)	Content tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in [13]. The regular expression shall be matched against the header-value of the SIP header. For definition of header and header-value, see [11]. 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 [11].
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 [13]. The regular expression shall be matched against the type of the field inside the session description. For definition of type, see chapter 6 in [12].
Content (of SessionDescription)	Content tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in [13]. The regular expression shall be matched against the value of the field inside the session description. For definition of value, see chapter 6 in [12].

Annex G (Informative): CxDataType_Rel6.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xs:simpleType name="tPriority" final="list restriction">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tProfilePartIndicator" final="list restriction">
        <xs:restriction base="xs:unsignedByte">
            <xs:maxInclusive value="1"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">REGISTERED</label>
                        <definition xml:lang="en">iFC is part of the registered profile</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">UNREGISTERED</label>
                        <definition xml:lang="en">iFC is part of the unregistered profile</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tSharedIFCSetID" final="list restriction">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tGroupID" final="list restriction">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tRegistrationType" final="list restriction">
        <xs:restriction base="xs:unsignedByte">
            <xs:maxInclusive value="2"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">INITIAL_REGISTRATION</label>
                        <definition xml:lang="en">Matches to REGISTER messages that are related to initial registration</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">RE-REGISTRATION</label>
                        <definition xml:lang="en">Matches to REGISTER messages that are related to re-registration</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="2">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">DE-REGISTRATION</label>
                        <definition xml:lang="en">Matches to REGISTER messages that are related to de-registration</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tDefaultHandling" final="list restriction">
        <xs:restriction base="xs:unsignedByte">
            <xs:maxInclusive value="1"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label
xml:lang="en">SESSION_CONTINUED</label>
                        <definition xml:lang="en">Session
Continued</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:documentation>
                        <label
xml:lang="en">SESSION_TERMINATED</label>
                        <definition xml:lang="en">Session
Terminated</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tDirectionOfRequest" final="list restriction">
        <xs:restriction base="xs:unsignedByte">
            <xs:maxInclusive value="3"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label
xml:lang="en">ORIGINATING_SESSION</label>
                        <definition xml:lang="en">Originating
Session</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">TERMINATING_REGISTERED</label>
                        <definition xml:lang="en">Terminating Session for registered user</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="2">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">TERMINATING_UNREGISTERED</label>
                        <definition xml:lang="en">Terminating Session for unregistered user</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tPrivateID" final="list restriction">
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="tSIP_URL" final="list restriction">
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="tTEL_URL" final="list restriction">
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="tIdentity" final="list restriction">
        <xs:union memberTypes="tSIP_URL tTEL_URL"/>
    </xs:simpleType>
    <xs:simpleType name="tIdentityType" final="list restriction">
        <xs:restriction base="xs:unsignedByte">
            <xs:minInclusive value="0"/>
            <xs:maxInclusive value="2"/>
            <xs:enumeration value="0">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">PUBLIC_USER_IDENTITY</label>
                        <definition xml:lang="en">Identity is a Public User Identity.</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="1">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">DISTINCT_PSI</label>
                        <definition xml:lang="en">Identity is a distinct Public Service Identity.</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
            <xs:enumeration value="2">
                <xs:annotation>
                    <xs:documentation>
                        <label xml:lang="en">WILDCARDED_PSI</label>
                        <definition xml:lang="en">Identity matches a wildcarded Public Service Identity.</definition>
                    </xs:documentation>
                </xs:annotation>
            </xs:enumeration>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tPublicIdentityExtension">
        <xs:sequence>
            <xs:element name="IdentityType" type="tIdentityType" minOccurs="0"/>
            <xs:element name="WildcardedPSI" type="xs:anyURI" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:simpleType name="tServiceInfo" final="list restriction">
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tString" final="list restriction">
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tBool">
        <xs:restriction base="xs:boolean"/>
    </xs:simpleType>
    <xs:simpleType name="tSubscribedMediaProfileId" final="list restriction">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tExtension">
        <xs:sequence>
            <xs:any processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tServiceProfileExtension">
        <xs:sequence>
            <xs:element name="SharedIFCSetID" type="tSharedIFCSetID" minOccurs="0"
maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tSePoTriExtension">
        <xs:sequence>
            <xs:element name="RegistrationType" type="tRegistrationType"
minOccurs="0" maxOccurs="2"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tIMSSubscription">
```

```
        <xs:sequence>
            <xs:element name="PrivateID" type="tPrivateID"/>
            <xs:element name="ServiceProfile" type="tServiceProfile"
maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tServiceProfile">
        <xs:sequence>
            <xs:element name="PublicIdentity" type="tPublicIdentity"
maxOccurs="unbounded"/>
            <xs:element name="CoreNetworkServicesAuthorization"
type="tCoreNetworkServicesAuthorization" minOccurs="0"/>
            <xs:element name="InitialFilterCriteria" type="tInitialFilterCriteria"
minOccurs="0" maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tServiceProfileExtension"
minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tCoreNetworkServicesAuthorization">
        <xs:sequence>
            <xs:element name="SubscribedMediaProfileId"
type="tSubscribedMediaProfileId" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tInitialFilterCriteria">
        <xs:sequence>
            <xs:element name="Priority" type="tPriority"/>
            <xs:element name="TriggerPoint" type="tTrigger" minOccurs="0"/>
            <xs:element name="ApplicationServer" type="tApplicationServer"/>
            <xs:element name="ProfilePartIndicator" type="tProfilePartIndicator"
minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tTrigger">
        <xs:sequence>
            <xs:element name="ConditionTypeCNF" type="tBool"/>
            <xs:element name="SPT" type="tSePoTri" maxOccurs="unbounded"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tSePoTri">
        <xs:sequence>
            <xs:element name="ConditionNegated" type="tBool" default="0" minOccurs="0"/>
            <xs:element name="Group" type="tGroupID" maxOccurs="unbounded"/>
            <xs:choice>
                <xs:element name="RequestURI" type="tString"/>
                <xs:element name="Method" type="tString"/>
                <xs:element name="SIPHeader" type="tHeader"/>
                <xs:element name="SessionCase" type="tDirectionOfRequest"/>
                <xs:element name="SessionDescription" type="tSessionDescription"/>
            </xs:choice>
            <xs:element name="Extension" type="tSePoTriExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tHeader">
        <xs:sequence>
            <xs:element name="Header" type="tString"/>
            <xs:element name="Content" type="tString" minOccurs="0"/>
            <xs:element name="Extension" type="tExtension" minOccurs="0"/>
            <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
```

```
	<xs:complexType name="tSessionDescription">
		<xs:sequence>
			<xs:element name="Line" type="tString"/>
			<xs:element name="Content" type="tString" minOccurs="0"/>
			<xs:element name="Extension" type="tExtension" minOccurs="0"/>
			<xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
		</xs:sequence>
	</xs:complexType>
	<xs:complexType name="tApplicationServer">
		<xs:sequence>
			<xs:element name="ServerName" type="tSIP_URL"/>
			<xs:element name="DefaultHandling" type="tDefaultHandling"
minOccurs="0"/>
			<xs:element name="ServiceInfo" type="tServiceInfo" minOccurs="0"/>
			<xs:element name="Extension" type="tExtension" minOccurs="0"/>
			<xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
		</xs:sequence>
	</xs:complexType>
	<xs:complexType name="tPublicIdentity">
		<xs:sequence>
			<xs:element name="BarringIndication" type="tBool" default="0"
minOccurs="0"/>
			<xs:element name="Identity" type="tIdentity"/>
			<xs:element name="Extension" type="tPublicIdentityExtension"
minOccurs="0"/
			<xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
		</xs:sequence>
	</xs:complexType>
	<xs:element name="IMSSubscription" type="tIMSSubscription"/>
</xs:schema>
```