

1 3GPP2 X.S0013-005-0
2 *Version 1.0*
3 *Version Date: December, 2003*



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

All-IP Core Network Multimedia Domain

IP Multimedia Subsystem Cx Interface Signaling flows and Message Contents

COPYRIGHT NOTICE

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

20
21

- 1 No text.
- 2

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

Contents

1			
2			
3			
4			
5			
6			
7	1	Scope	1
8	2	References	1
9	3	Definitions, symbols and abbreviations	1
10	3.1	Definitions	1
11	3.2	Abbreviations	1
12	4	Main Concept	2
13	5	General Architecture	2
14	5.1	Functional requirements of network entities	2
15	5.1.1	Functional requirements of P-CSCF	2
16	5.1.2	Functional requirements of I-CSCF	2
17	5.1.3	Functional requirements of S-CSCF	2
18	5.1.4	Functional requirements of HSS	2
19	5.1.5	Functional classification of Cx interface procedures	3
20	6	Procedure Descriptions	3
21	6.1	Location management procedures	3
22	6.1.1	User registration status query	3
23	6.1.1.1	Detailed behaviour	4
24	6.1.2	S-CSCF registration/deregistration notification	6
25	6.1.2.1	Detailed behaviour	8
26	6.1.3	Network initiated de-registration by the HSS, administrative	9
27	6.1.3.1	Detailed behaviour	10
28	6.1.4	User location query	11
29	6.1.4.1	Detailed behaviour	12
30	6.2	User data handling procedures	12
31	6.2.1	User Profile download	12
32	6.2.2	HSS initiated update of User Profile	12
33	6.2.2.1	Detailed behaviour	13
34	6.3	Authentication procedures	14
35	6.3.1	Detailed behaviour	16
36	6.4	void	17
37	6.5	Implicit registration	17

1 6.5.1 S-CSCF initiated procedures 17

2 6.5.1.1 Registration..... 18

3 6.5.1.2 De-registration 18

4 6.5.1.3 Authentication 18

5 6.5.1.4 Downloading the user profile 18

6 6.5.2 HSS initiated procedures 18

7 6.5.2.1 Update of User Profile..... 18

8 6.5.2.2 De-registration 18

9 6.6 Download of relevant user data 18

10 6.6.1 HSS initiated update of User Profile..... 19

11 6.6.2 S-CSCF operation..... 19

12 6.7 S-CSCF Assignment 19

13 7 Information element contents 19

14 7.1 Visited Network Identifier 19

15 7.2 Public User Identity 20

16 7.3 Private User Identity 20

17 7.4 S-CSCF Name 20

18 7.5 S-CSCF Capabilities 20

19 7.6 Result 20

20 7.7 User Profile 20

21 7.8 Server Assignment Type..... 20

22 7.9 Authentication Data 20

23 7.9.1 Item Number..... 20

24 7.9.2 Authentication Scheme..... 20

25 7.9.3 Authentication Information 20

26 7.9.4 Authorization Information 20

27 7.9.5 Confidentiality Key 21

28 7.9.6 Integrity Key..... 21

29 7.10 Number Authentication Items 21

30 7.11 Reason for de-registration 21

31 7.12 Charging information 21

32 7.13 Routing information 21

33 7.14 Type of authorization 21

34 7.15 User Data Request Type 21

35 7.16 User Data Already Available 21

36 8 Error handling procedures..... 21

37 8.1 Registration error cases 21

1	8.1.1	Cancellation of the old S-CSCF	21
2	8.1.2	Error in S-CSCF name.....	22
3	9	Protocol version identification.....	22
4	10	Operational Aspects	22
5		Annex A (normative): Mapping of Cx operations and terminology to Diameter	23
6	A.1	Introduction	23
7	A.2	Cx message to Diameter command mapping	23
8	A.3	Cx message parameters to Diameter AVP mapping.....	23
9	A.4	Message flows	24
10	A.4.1	Registration– user not registered	25
11	A.4.2	Registration – user currently registered	26
12	A.4.3	Mobile initiated de-registration	26
13	A.4.4	Network initiated de-registration.....	27
14	A.4.4.1	Registration timeout	27
15	A.4.4.2	Administrative de-registration.....	27
16	A.4.4.3	De-registration initiated by service platform	28
17	A.4.5	MT SIP session set-up	28
18	A.4.6	Initiation of a session to a non-registered user	29
19	A.4.7	User Profile update.....	29
20		Annex B (informative): User Profile UML model.....	30
21	B.1	General description.....	30
22	B.2	Service profile	30
23	B.2.1	Public Identification.....	31
24	B.2.2	Initial Filter Criteria.....	32
25	B.2.3	Service Point Trigger.....	33
26		Annex C (informative): Conjunctive and Disjunctive Normal Form	35
27		Annex D (informative): High-level format for the User Profile	40
28		Annex E (normative): XML schema for the Cx interface user profile	41
29		Annex F (CxDataType.xsd):	45
30			
31			

1 **Foreword**

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

8

9 **Revision History**

10

Revision	Changes	Date
0	Initial Publication	December 2003

11

12

1 Scope

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

This document addresses the signalling flows for the Cx interface.

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].

2 References

- [1] TIA-873-002: "IP Multimedia (IM) Subsystem – Stage 2".
3GPP2 X.S0013-002: "IP Multimedia (IM) Subsystem – Stage 2".
- [2] Void
- [3] 3GPP2 S.S0086-0: "3GPP2 IMS Security Framework".
- [4] TIA/TSB-151: IP Network Reference Model (NRM) for cdma2000 Spread Spectrum Systems, December 2003.
3GPP2 S.R0037-0, "3GPP2 All-IP Network Architecture Model Version 2.0, May 14, 2002".
- [5] TIA-873-006: "Cx Interface based on Diameter Protocol; Protocol details"
3GPP2 X.S0013-006: "Cx Interface based on Diameter Protocol; Protocol details"
- [6] TIA-873-003: "IP Multimedia Subsystem – IP Multimedia Call Model; Stage 2".
3GPP2 X.S0013-003: "IP Multimedia Subsystem – IP Multimedia Call Model; Stage 2".
- [7] Internet Engineering Task Force (IETF) RFC 2045, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", November 1996.
- [8] TIA-873-004: "IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3".
3GPP2 X.S0013-004: "IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3".
- [9] IETF RFC 3588, "Diameter Base Protocol", September 2003.

3 Definitions, symbols and abbreviations

3.1 Definitions

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

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

3.2 Abbreviations

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

AVP	Attribute Value Pair
CSCF	Call Session Control Function
HSS	Home Subscriber Server
IE	Information Element

1	IP	Internet Protocol
2	I-CSCF	Interrogating CSCF
3	IM	IP Multimedia
4	IMS	IP Multimedia Subsystem
5	LIA	Location Information Answer
6	LIR	Location Information Request
7	MAA	Multimedia Authentication Answer
8	MAR	Multimedia Authentication Request
9	MO	Mobile Originating
10	MT	Mobile Terminating
11	P-CSCF	Proxy CSCF
12	PPA	Push Profile Answer
13	PPR	Push Profile Request
14	RTA	Registration Termination Answer
15	RTR	Registration Termination Request
16	SAA	Server Assignment Answer
17	SAR	Server Assignment Request
18	SIP	Session Initiation Protocol
19	S-CSCF	Serving CSCF
20	UAA	User Authorization Answer
21	UAR	User Authorization Request

22 **4 Main Concept**

23 This document presents the Cx interface related functional requirements of the communicating entities.
 24 It gives a functional classification of the procedures and describes the procedures and message parameters.
 25 Error handling flows, protocol version identification and procedures are also included.

26 **5 General Architecture**

27 This clause further specifies the architectural assumptions associated with the Cx reference point, building
 28 on [1].

29 **5.1 Functional requirements of network entities**

30 **5.1.1 Functional requirements of P-CSCF**

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

32 **5.1.2 Functional requirements of I-CSCF**

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

34 For functionality of the I-CSCF refer to [4].

35 **5.1.3 Functional requirements of S-CSCF**

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

37 For functionality of the S-CSCF refer to [4].

38 **5.1.4 Functional requirements of HSS**

39 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.
3. User authentication procedures

6 Procedure Descriptions

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

6.1 Location management procedures

6.1.1 User registration status query

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

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

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

Table 6.1.1.1 : User registration status query

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	M	User public identity to be registered

Visited Network Identifier (See 7.1)	Visited-Network-Identifier	M	Identifier that allows the home network to identify the visited network
Type of Authorization (See 7.14)	User-Authorization-Type	C	Type of authorization requested by the I-CSCF. If the request corresponds to a de-registration, i.e. Expires field in the REGISTER method is equal to zero, this AVP shall be present in the command and the value shall be set to DE_REGISTRATION. If the request corresponds to an initial registration or a re-registration, i.e. Expires field in the REGISTER method is not equal to zero then this AVP may be absent from the command. If present its value shall be set to REGISTRATION. If the request corresponds to an initial registration or a re-registration, and the I-CSCF explicitly queries the S-CSCF capabilities, then this AVP shall be present in the command and the value shall be set to REGISTRATION_AND_CAPABILITIES. The I-CSCF shall use this value when the user's current S-CSCF, which is stored in the HSS, cannot be contacted and a new S-CSCF needs to be selected.
Private User Identity (See 7.3)	User-Name	M	User private identity
Routing Information (See 7.13)	Destination-Host, Destination-Realm	C	If the I-CSCF knows HSS name Destination-Host AVP shall be present in the command. Otherwise, only Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node.

1

2

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 errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the user.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

3

6.1.1.1 Detailed behaviour

4 The HSS shall, in the following order (if there is an error in any of the following steps the HSS shall stop
5 processing and return the corresponding error code, see [5]):
6

- 1 1. Check that the user exists in the HSS. If not, Experimental-Result-Code shall be set to
2 DIAMETER_ERROR_USER_UNKNOWN.
- 3 2. Check that the private and public identities received in the request belong to the same user. If not,
4 Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.
- 5 3. Check whether the public identity received in the request is barred for the establishment of multimedia
6 sessions.
- 7 + If it is, the HSS shall check whether there are other non-barred public identities to be implicitly
8 registered with that one.
- 9 -- If so, continue to step 4.
- 10 -- If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.
- 11 4. Check the User-Authorization-Type received in the request:
- 12 + If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall
13 check that the user is allowed to roam in the visited network (if not, Experimental-Result-Code shall
14 be set to DIAMETER_ERROR_ROAMING_NOT_ALLOWED and processing should stop) and
15 authorized to register (if not, Result-Code shall be set to
16 DIAMETER_AUTHORIZATION_REJECTED and processing should stop). Continue to step 5.
- 17 + If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to
18 step 5.
- 19 + If it is REGISTRATION_AND_CAPABILITIES, the HSS shall check that the user is allowed to
20 roam in the visited network (if not, Experimental-Result-Code shall be set to DIAMETER_ERROR
21 _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to
22 DIAMETER_AUTHORIZATION_REJECTED). The HSS shall return the list of S-CSCF
23 capabilities, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy
24 the most restrictive service profile of the user. The list of capabilities may be empty, to indicate to
25 the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to
26 DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name. Stop processing.
- 27 5. Check the state of the public identity received in the request:
- 28 + If it is registered, the HSS shall return the stored S-CSCF name. No S-CSCF capabilities shall be
29 present in the response. In case the User-Authorization-Type is equal to REGISTRATION,
30 Experimental-Result-Code shall be set to DIAMETER_SUBSEQUENT_REGISTRATION. If User-
31 Authorization-Type is equal to DE_REGISTRATION, Result-Code shall be set to
32 DIAMETER_SUCCESS.
- 33 +If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping
34 the user profile stored) and User-Authorization-Type is equal to DE_REGISTRATION, Result-Code
35 shall be set to DIAMETER_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION,
36 then:
- 37 ○ If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF
38 name and the Experimental-Result-Code set to
39 DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF
40 capabilities.
- 41 ○ Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the
42 S-CSCF capabilities and the Experimental-Result-Code set to
43 DIAMETER_SERVER_SELECTION. Considering the information received from the HSS,
44 the I-CSCF shall determine whether or not it has to select a new S-CSCF.
- 45

- 1 + If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the
- 2 request:
- 3 -- If the value of User-Authorization-Type is DE_REGISTRATION, then the HSS shall not return
- 4 any S-CSCF name or S-CSCF capabilities. The HSS shall set the Experimental-Result-Code to
- 5 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.
- 6 -- If the value of User-Authorization-Type is REGISTRATION, then the HSS shall check if there is
- 7 at least one identity of the user with an S-CSCF name assigned.
- 8 --- If there is at least one identity of the user that is registered the HSS shall return the S-CSCF
- 9 name assigned for the user and Experimental-Result-Code set to
- 10 DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF
- 11 capabilities.
- 12 --- If there is at least one identity of the user that is unregistered (i.e registered as a consequence
- 13 of a terminating call or there is an S-CSCF keeping the user profile stored), then:
- 14 ▪ If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-
- 15 CSCF name and the Experimental-Result-Code set to
- 16 DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-
- 17 CSCF capabilities.
- 18 ▪ Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered
- 19 user, the S-CSCF capabilities and the Experimental-Result-Code set to
- 20 DIAMETER_SERVER_SELECTION. Considering the information received from
- 21 the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
- 22
- 23 --- If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall
- 24 return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The list of
- 25 S-CSCF capabilities may be empty, to indicate to the I-CSCF that it may select any available S-
- 26 CSCF. Experimental-Result-Code shall be set to DIAMETER_FIRST_REGISTRATION. The
- 27 HSS shall not return any S-CSCF name..
- 28 If the HSS cannot fulfill received request, e.g. due to database error, it shall set Result-Code to
- 29 DIAMETER_UNABLE_TO_COMPLY. No S-CSCF name or S-CSCF capabilities shall be present in the
- 30 response.

31 **6.1.2 S-CSCF registration/deregistration notification**

32 This procedure is used between the S-CSCF and the HSS. The procedure is invoked by the S-CSCF,

33 corresponds to the combination of the operations Cx-Put and Cx-Pull (see [1]) and is used:

- 34 - To assign an S-CSCF to a public identity, or to clear the name of the S-CSCF assigned to one or
- 35 more public identities.
- 36 - To download from HSS the relevant user profile information that the S-CSCF needs to serve the
- 37 user.

38 This procedure is mapped to the commands Server-Assignment-Request/Answer in the Diameter

39 application specified in [5]. Tables 6.1.2.1 and 6.1.2.2 describe the involved information elements.

40 **Table 6.1.2.1: S-CSCF registration/deregistration notification request**

Information element name	Mapping to Diameter AVP	Cat.	Description
--------------------------	-------------------------	------	-------------

Public User Identity (See 7.2)	Public-Identity	C	User public identity or list of user public identities. At least one public identity shall be present if User-Name is not present in the request.
S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity (See 7.3)	User-Name	C	User private identity. It shall be present if it is available when the S-CSCF issues the request. It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER. In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server-Assignment-Type	M	Type of update the S-CSCF requests in the HSS (e.g: de-registration). See [5] for all the possible values.
User Data Request Type (See 7.15)	User-Data-Request-Type	M	Part of the user profile the S-CSCF requests from the HSS (e.g: complete profile). See [5] for all the possible values.
User Data Already Available (See 7.16)	User-Data-Already-Available	M	This indicates if the user profile is already available in the S-CSCF.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command. This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent in as a consequence of a session termination for an unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node based on the Diameter routing table in the S-CSCF.

1

2

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	C	User 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 user identity is not known by the HSS.

Registration result (See 7.6)	Result-Code / Experimental- -Result	M	Result of registration. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx 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. If the Server-Assignment-Type in the request is equal to REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER the User-Data AVP shall be present according to the rules defined in the section 6.6. If the S-CSCF receives more data than it is prepared to accept, it shall perform the de-registration of the user with User-Authorization-Type set to DEREGISTRATION_TOO_MUCH_DATA and send back a SIP 3xx or 480 (Temporarily Unavailable) response, which will trigger the selection of a new S-CSCF by the I-CSCF, as specified in [8].
Charging Information (See 7.12)	Charging- Information	O	Addresses of the charging functions.

1

2 6.1.2.1 Detailed behaviour

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

9 1. Check that the user is known. If not Experimental-Result-Code shall be set to
10 DIAMETER_ERROR_USER_UNKNOWN.

11 2. Check that the private and public identities received in the request belong to the same user. If not
12 Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

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

14 + If it indicates REGISTRATION or RE_REGISTRATION, the HSS shall download the relevant user
15 public identity information based on the description in section 6.6. If set, the flag that indicates that
16 the identity is pending of the confirmation of the authentication shall be cleared. The Result-Code
17 shall be set to DIAMETER_SUCCESS.

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

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

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

- 1 + If it indicates TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION,
 2 DEREGISTRATION_TOO_MUCH_DATA or ADMINISTRATIVE_DEREGISTRATION, the
 3 HSS shall clear the S-CSCF name for all the public identities that the S-CSCF indicated in the
 4 request and set the registration state of the identities as not registered. If no public identity is present
 5 in the request, the private identity shall be present; the HSS shall clear the S-CSCF name for all the
 6 identities of the user and set their registration state to not registered. The Result-Code shall be set to
 7 DIAMETER_SUCCESS.
- 8 + If it indicates TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME or
 9 USER_DEREGISTRATION_STORE_SERVER_NAME the HSS decides whether to keep the S-
 10 CSCF name stored or not for all the public identities that the S-CSCF indicated in the request and
 11 set the registration state of the identities as unregistered. If no public identity is present in the
 12 request, the private identity shall be present. If the HSS decided to keep the S-CSCF name stored the
 13 HSS keeps the S-CSCF name stored for all the identities of the user and set their registration state to
 14 unregistered.
- 15 If the HSS decides to keep the S-CSCF name the Result-Code shall be set to
 16 DIAMETER_SUCCESS.
- 17 If the HSS decides not to keep the S-CSCF name the Experimental-Result-Code shall be set to
 18 DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED.
- 19 + If it indicates NO_ASSIGNMENT, the HSS checks whether the user is assigned for the S-CSCF
 20 requesting the data and download the user public identity information requested in the User-Data-
 21 Request-Type AVP. The Result-Code shall be set to DIAMETER_SUCCESS. If the requesting S-
 22 CSCF is not the same as the assigned S-CSCF, the Result-Code shall be set to
 23 DIAMETER_UNABLE_TO_COMPLY.
- 24 Only one public identity shall be present in the request. If more than one public identity is present
 25 the Result-Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and no user
 26 information shall be returned.
- 27 + If it indicates AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the HSS shall
 28 clear the S-CSCF name for the public identity that the S-CSCF indicated in the request and set the
 29 registration state of the identity as not registered. The flag that indicates that the identity is pending
 30 of the confirmation of the authentication shall be cleared. The Result-Code shall be set to
 31 DIAMETER_SUCCESS.
- 32 Only one public identity shall be present in the request. If more than one identity is present the
 33 Result-Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and the
 34 modifications specified in the previous paragraph shall not be performed.
- 35 See chapter 8.1.2 for the description of the handling of the error situations: reception of an S-CSCF name
 36 different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible
 37 with the registration state of the user.

38 **6.1.3 Network initiated de-registration by the HSS, administrative**

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

42 HSS may decide to de-register:

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

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

1

Table 6.1.3.1 : Network Initiated Deregistration by HSS request

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

2

3

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 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.

4

6.1.3.1 Detailed behaviour

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

9 The HSS may de-register:

- 10 - Only one public identity or a list of public identities. In this case the S-CSCF shall remove all the
11 information stored in the S-CSCF for those public identities.
- 12 - The user with all his/her public identities (no public identity sent in the Cx-Deregister request). In
13 this case the S-CSCF shall remove all the information stored for that user.

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

- 1 - PERMANENT_TERMINATION: The IMS subscription or service profile(s) has been
 2 permanently terminated. The S-CSCF should start the network initiated de-registration towards the
 3 user.
- 4 - NEW_SERVER_ASSIGNED: A new S-CSCF has been allocated to the user due to some reason,
 5 e.g. an error case, where the SIP registration is terminated in a new S-CSCF. The S-CSCF shall
 6 not start the network initiated de-registration towards the user but only clears its registration state
 7 and information regarding the user, i.e. all service profiles are cleared.
- 8 - SERVER_CHANGE: A new S-CSCF shall be allocated to the user when the user's S-CSCF
 9 capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory
 10 for the updated User Profile. The S-CSCF should start the network initiated de-registration
 11 towards the user, i.e. all registrations are de-registered and the user is asked to re-register to all
 12 existing registrations.
- 13 - REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF should no longer be used
 14 for a given user. The S-CSCF shall not start the network initiated de-registration towards the user
 15 when the user is not currently registered but clears all information regarding the user and responds
 16 to the HSS. The HSS then removes the S-CSCF for that user.

17 6.1.4 User location query

18 This procedure is used between the I-CSCF and the HSS to obtain the name of the S-CSCF where a public
 19 identity is registered. The procedure is invoked by the I-CSCF per public identity.

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

22 **Table 6.1.4.1 : User Location query**

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

23

24 **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 errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

S-CSCF capabilities (See 7.5)	Server-Capabilities	O	It contains the information to help the I-CSCF in the selection of the S-CSCF.
----------------------------------	---------------------	---	--

1

2 **6.1.4.1 Detailed behaviour**

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

- 5 1. Check that the user is known. If not the Experimental-Result-Code shall be set to
6 DIAMETER_ERROR_USER_UNKNOWN.
- 7 2. Check the state of the public identity received in the request.
 - 8 + If it is registered or unregistered (i.e. registered as a consequence of a terminating call or there is a
9 S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name. The
10 Server-Name AVP shall contain the SIP URL of the server. The Server-Capabilities AVP shall not
11 be present. The Result-Code AVP shall be set to DIAMETER_SUCCESS.
 - 12 + If it is not registered, but has services related to unregistered state, the HSS shall check if there is
13 at least one identity of the user with an S-CSCF name assigned:
 - 14 -- If this is the case the HSS shall return the S-CSCF name assigned for that user. The
15 Server-Name AVP shall contain the SIP URL of the server. The Server-Capabilities AVP
16 shall not be present. The Result-Code shall be set to DIAMETER_SUCCESS.
 - 17 -- If there is not any S-CSCF name assigned for that user, the HSS may return information
18 about the required S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF.
19 The Server-Capabilities AVP may be present. The HSS shall send the same server
20 capability set that is sent in the user registration status response during the registration. If
21 Server-Capabilities AVP is not present, the I-CSCF shall understand that any S-CSCF is
22 suitable to serve the user. The Server-Name AVP shall not be present. The Experimental-
23 Result-Code shall be set to DIAMETER_UNREGISTERED_SERVICE.
 - 24 + If it is not registered and has no unregistered services related data the response shall contain
25 Experimental-Result-Code set to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

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

29 **6.2 User data handling procedures**

30 **6.2.1 User Profile download**

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

33 **6.2.2 HSS initiated update of User Profile**

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

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

1

Table 6.2.2.1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	M	User private identity.
User Profile (See 7.7)	User-Data	M	Updated user profile (see section 6.6.1), with the format defined in chapter 7.7.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given multimedia user. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

2

3

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 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.

4

6.2.2.1 Detailed behaviour

6 The HSS shall make use of this procedure to update relevant user profile information in the S-CSCF. See
7 chapter 6.6.1 for the rules of user profile updating.

8 The S-CSCF shall overwrite, for the public user identities indicated in the request, current information with
9 the information received from the HSS, except in the error situations detailed in table 6.2.2.1.1.

10 If the S-CSCF receives more data than it can accept, it shall return the corresponding error code to the HSS
11 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
12 the user. The HSS shall initiate a network-initiated de-registration procedure towards the S-CSCF with
13 Deregistration-Reason set to SERVER_CHANGE, which will trigger the assignment of a new S-CSCF.

14 Table 6.2.2.1.1 details the valid result codes that the S-CSCF can return in the response.

15

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 subscription data contained information, which was not recognised or supported, i.e. profile information which is not correctly encoded according to the XML schema or

	standardised profile information which cannot be interpreted by the S-CSCF due to unsupported S-CSCF capabilities.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in S-CSCF.
DIAMETER_ERROR_TOO_MUCH_DATA	The request failed. The S-CSCF informs to the HSS that it tried to push too much data into the S-CSCF.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

1

2 **6.3 Authentication procedures**

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

6 - To retrieve authentication vectors from the HSS.

7 - To resolve synchronization failures between the sequence numbers in the UE and the HSS.

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

10

Table 6.3.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	M	This information element contains the public identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the user private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Tables 6.3.2 and 6.3.3 for the contents of this information element. The content shown in table 6.3.2 shall be used for a normal authentication request; the content shown in table 6.3.3 shall be used for an authentication request after synchronization failure.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.

Routing Information (See 7.13)	Destination-Host	C	<p>If the S-CSCF knows the HSS name this AVP shall be present.</p> <p>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.</p> <p>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.</p>
-----------------------------------	------------------	---	--

1

2

Table 6.3.2: Authentication Data content – request

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

3

4

Table 6.3.3: Authentication Data content – request, synchronization failure

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For this release it shall contain “Digest-AKAv1-MD5”.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of nonce and AUTS binary encoded.

5

6

Table 6.3.4: Authentication answer

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

Authentication Data (See 7.9)	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero 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 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.

1

2

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For this release it shall contain “Digest-AKAv1-MD5”.
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See [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. -

3

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 user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.
2. Check that the private and public identities belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

10

- 1 3. Check that the authentication scheme indicated in the request is supported. If not Experimental-Result-
2 Code shall be set to DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED.
- 3 4. If the request indicates there is a synchronization failure, the HSS shall process AUTS as described in
4 [3] and return the requested authentication information. The Result-Code shall be set to
5 DIAMETER_SUCCESS.
- 6 5. Check the registration status of the public identity received in the request:
- 7 + If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF
8 name stored in the HSS:
- 9 -- If they are different, the HSS shall store the S-CSCF name. The HSS shall download
10 Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items
11 received in the command Multimedia-Auth-Request. It shall also set for this public identity the
12 flag that indicates the identity is pending of the confirmation of the authentication. The Result-
13 Code shall be set to DIAMETER_SUCCESS.
- 14 -- If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum
15 specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The
16 Result-Code shall be set to DIAMETER_SUCCESS.
- 17 + If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or
18 there is an S-CSCF keeping the user profile stored), the HSS shall compare the S-CSCF name
19 received in the request to the S-CSCF name stored in the HSS:
- 20 -- If they are different, the HSS shall store the S-CSCF name. The HSS shall download
21 Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items
22 received in the command Multimedia-Auth-Request. It shall also set for this public identity the
23 flag that indicates the identity is pending of the confirmation of the authentication. The Result-
24 Code shall be set to DIAMETER_SUCCESS.
- 25 -- If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum
26 specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It
27 shall also set for this public identity the flag that indicates the identity is pending of the
28 confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.
- 29 + If it is not registered, the HSS shall store the S-CSCF name. The HSS shall download
30 Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the
31 command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the
32 identity is pending of the confirmation of the authentication. The Result-Code shall be set to
33 DIAMETER_SUCCESS.
- 34 Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be
35 set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

36 **6.4 void**

37 **6.5 Implicit registration**

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

41 What follows is an extension of the affected basic procedures.

42 **6.5.1 S-CSCF initiated procedures**

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

1 **6.5.1.1 Registration**

2 The notification of a registration of a public identity affects all the public identities that are configured in
3 the HSS to be registered implicitly. The profile information downloaded in the response contains the list of
4 implicitly registered public identities. This allows the S-CSCF to know the implicitly registered public
5 identities. The S-CSCF shall take from the list of implicitly registered public user identities the first identity
6 which has the syntax of a SIP URI and which is not barred, and use this as the default public user identity.

7 **6.5.1.2 De-registration**

8 The de-registration of a public identity implies the de-registration of all the corresponding implicitly
9 registered public identities, both in the HSS and in the S-CSCF. The S-CSCF shall include in the request
10 single public identity for deregistering all the corresponding implicitly registered public identities in the
11 implicitly registered public user ID set.

12 The de-registration of a private identity implies the de-registration of all the corresponding public identities,
13 both in the HSS and in the S-CSCF.

14 **6.5.1.3 Authentication**

15 Setting the flag for a public identity that indicates a pending authentication implies setting the
16 "authentication pending" flag for each corresponding implicitly registered public identity in the HSS.

17 **6.5.1.4 Downloading the user profile**

18 If the S-CSCF requests to download a user profile from HSS, the user profile information in the response
19 shall contain the list of corresponding implicitly registered public identities with the associated service
20 profiles.

21 **6.5.2 HSS initiated procedures**

22 **6.5.2.1 Update of User Profile**

23 A request sent by the HSS to update the service profile associated to a user public identity shall include all
24 the corresponding implicitly registered public identities, with their respective service profiles (even if not
25 updated).

26 **6.5.2.2 De-registration**

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

29 The de-registration of a private identity implies the de-registration of all the corresponding public identities,
30 both in the HSS and in the S-CSCF.

31 **6.6 Download of relevant user data**

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

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

37 If User-Data-Already-Available is set to USER_DATA_ALREADY_AVAILABLE and the requested
38 profile is not up-to-date (according to the indications stored in HSS defined in 6.6.1) the HSS shall
39 download the requested profile, according to the value of User-Data-Request-Type.

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

1 **6.6.1 HSS initiated update of User Profile**

2 The update of user profile information in the S-CSCF includes all the identities in an implicitly registered
3 set. See 6.5.2.1.

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

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

9 If the user is unregistered (i.e. registered as a consequence of a terminating call or there is a S-CSCF
10 keeping the user profile stored) and there is a change in the registered part of the user profile, the HSS shall
11 set a flag indicating that the registered part of the profile is not up-to-date in the S-CSCF. The HSS shall
12 not initiate any push toward the S-CSCF.

13 **6.6.2 S-CSCF operation**

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

18 **6.7 S-CSCF Assignment**

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

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

27 As a first choice, the I-CSCF shall select an S-CSCF that has all the mandatory and optional capabilities for
28 the user. Only if that is not possible shall the I-CSCF apply a ‘best-fit’ algorithm. If more than one S-CSCF
29 is identified that supports all mandatory capabilities the I-CSCF may then consider optional capabilities in
30 selecting a specific S-CSCF. The ‘best-fit’ algorithm is implementation dependent and out of the scope of
31 this specification.

32 It is the responsibility of the operator to ensure that there are S-CSCFs which have the “mandatory”
33 capabilities indicated by the HSS for any given user. However, configuration errors may occur. If such
34 errors occur and they prevent the I-CSCF from selecting an S-CSCF which meets the “mandatory”
35 capabilities indicated by the HSS, the I-CSCF shall inform the HSS via the O&M subsystem.

36 As an alternative to selecting an S-CSCF based on the list of capabilities received from the HSS, it is
37 possible to steer users to certain S-CSCFs. To do this, the operator may include one or more S-CSCF
38 names as part of the capabilities of the user profile. The reason for the selection (e.g. all the users belonging
39 to the same company/group could be in the same S-CSCF to implement a VPN service) and the method of
40 selection are operator issues and out of the scope of this specification.

41 **7 Information element contents**

42 **7.1 Visited Network Identifier**

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

1 **7.2 Public User Identity**

2 This information element contains the public identity of the user.

3 **7.3 Private User Identity**

4 This information element contains the private identity of the user.

5 **7.4 S-CSCF Name**

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

7 **7.5 S-CSCF Capabilities**

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

10 **7.6 Result**

11 This information element contains result of an operation. See [5] for the possible values.

12 **7.7 User Profile**

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

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

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

17 **7.8 Server Assignment Type**

18 Indicates the type of server assignment. See [5] for the list of existing values.

19 **7.9 Authentication Data**

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

21 **7.9.1 Item Number**

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

23 **7.9.2 Authentication Scheme**

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

26 For the current release this scheme is “Digest-AKAv1-MD5”.

27 **7.9.3 Authentication Information**

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

30 **7.9.4 Authorization Information**

31 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].

1 **7.9.5 Confidentiality Key**

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

3 **7.9.6 Integrity Key**

4 This information element contains the integrity key. See [3].

5 **7.10 Number Authentication Items**

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

7 **7.11 Reason for de-registration**

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

9 **7.12 Charging information**

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

12 **7.13 Routing information**

13 Information to route requests.

14 **7.14 Type of authorization**

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

16 **7.15 User Data Request Type**

17 Part of the user profile the S-CSCF requests from the HSS. See [5] for a list of values.

18 **7.16 User Data Already Available**

19 This information element indicates to the HSS if the user profile is already available in the S-CSCF. See [5]
20 for a list of values.

21 **8 Error handling procedures**

22 **8.1 Registration error cases**

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

25 **8.1.1 Cancellation of the old S-CSCF**

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

30 In this case the new S-CSCF is assigned for the user and if registrations in the previously assigned S-CSCF
31 exist for the user, these registrations in the old S-CSCF are handled locally in the old S-CSCF, e.g. re-
32 registration timers in the old S-CSCF will cancel the registrations. Alternatively, the HSS may de-register

1 the registrations in the old S-CSCF by using the Registration-Termination-Request command. In this case
2 the de-registration must be done in the following order:

- 3 1. Deregistration-Reason AVP value set to NEW_SERVER_ASSIGNED, for the public identity,
4 which is registered in the new S-CSCF.
- 5 2. Deregistration-Reason AVP value set to SERVER_CHANGE, for the user public identities, which
6 are not registered in the new S-CSCF.

7 **8.1.2 Error in S-CSCF name**

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

- 11 - DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED if the S-CSCF name sent in the
12 Server-Assignment-Request command is different than assigned S-CSCF name, and therefore the
13 request cannot be successfully processed.
- 14 - DIAMETER_ERROR_IN_ASSIGNMENT_TYPE if the S-CSCF name sent in the Server-
15 Assignment-Request command is the same S-CSCF name as the assigned S-CSCF name, but
16 Server-Assignment-Type is not allowed, e.g. the user is registered and the S-CSCF sends Server-
17 Assignment-Request indicating the assignment for the unregistered user.

18 **9 Protocol version identification**

19 See [5].

20 **10 Operational Aspects**

21 See [5].

22

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

3 **A.1 Introduction**

4 This appendix gives mappings from Cx to Diameter protocol elements. Diameter protocol elements are
 5 defined in [5].

6 **A.2 Cx message to Diameter command mapping**

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

8
 9

Table A.2.1: Cx message to Diameter command mapping

Cx message	Source	Destination	Command-Name	Abbreviation
Cx-Query + Cx-Select-Pull	I-CSCF	HSS	User-Authorization-Request	UAR
Cx-Query Resp + Cx-Select-Pull Resp	HSS	I-CSCF	User-Authorization-Answer	UAA
Cx-Put + Cx-Pull	S-CSCF	HSS	Server-Assignment-Request	SAR
Cx-Put Resp + Cx-Pull Resp	HSS	S-CSCF	Server-Assignment-Answer	SAA
Cx-Location-Query + Location Query + Cx-LocQuery	I-CSCF	HSS	Location-Info-Request	LIR
Cx-Location-Query Resp + 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

10

11 **A.3 Cx message parameters to Diameter AVP mapping**

12 The following table gives an overview about the mapping:

1

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
S-CSCF Capabilities	Server-Capabilities
Result	Result-Code / Experimental-Result
User Profile	User-Data
Server Assignment Type	Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item Number	SIP-Item-Number
Authentication Scheme	SIP-Authentication-Scheme
Authentication Information	SIP-Authenticate
Authorization Information	SIP-Authorization
Confidentiality Key	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

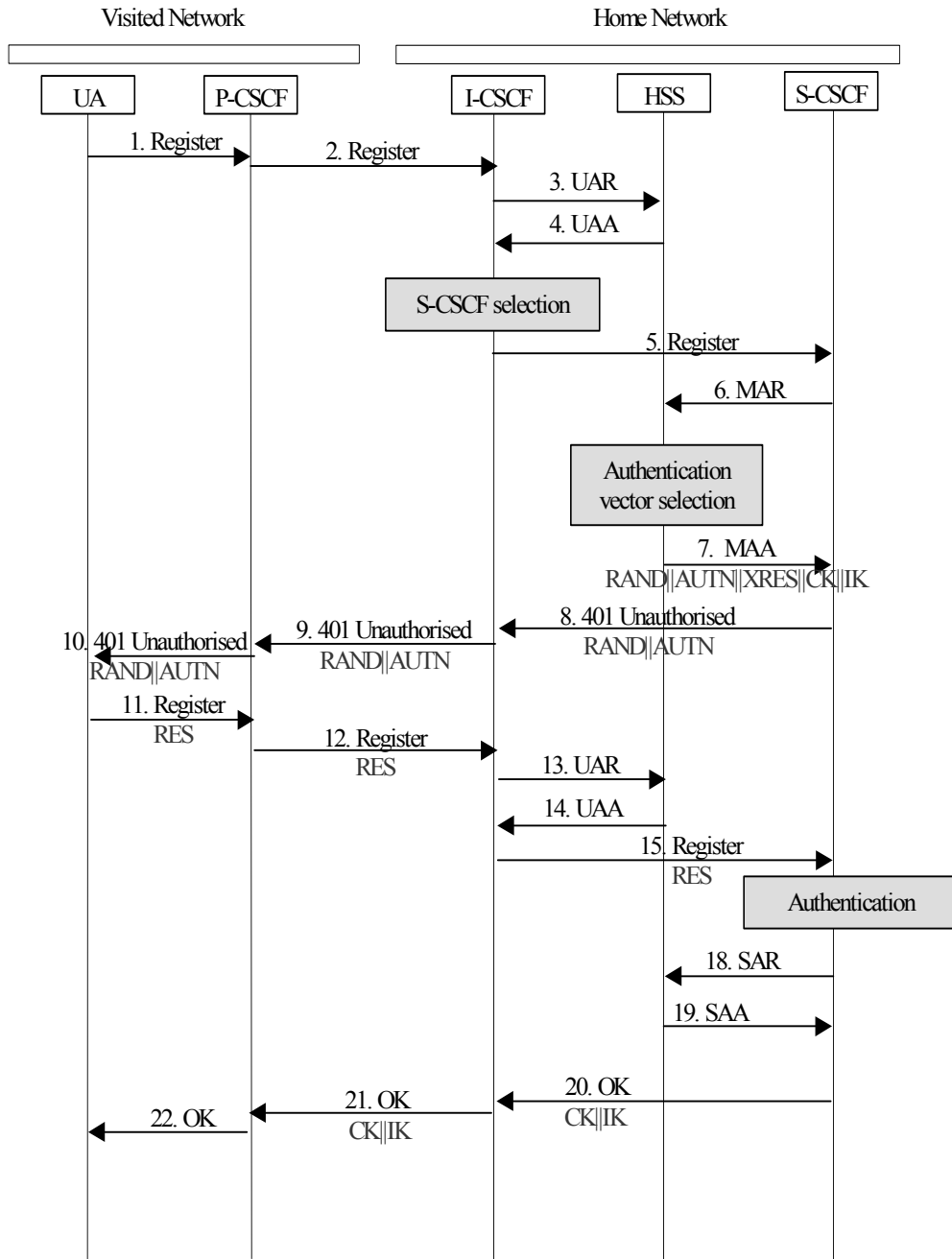
2

3 **A.4 Message flows**

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

6

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

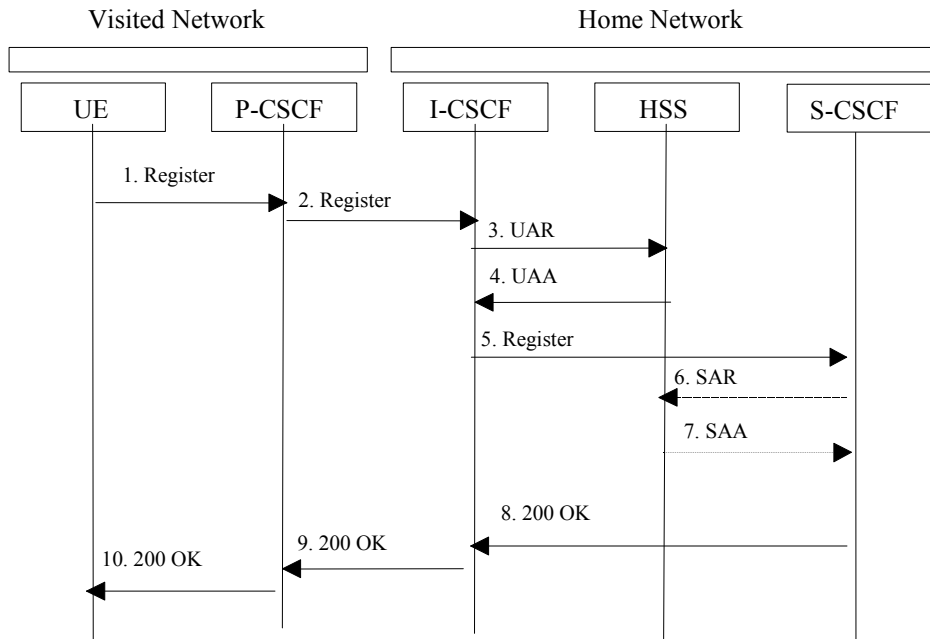


2

3

Figure A.4.1.1: Registration – user not registered

1 **A.4.2 Registration – user currently registered**

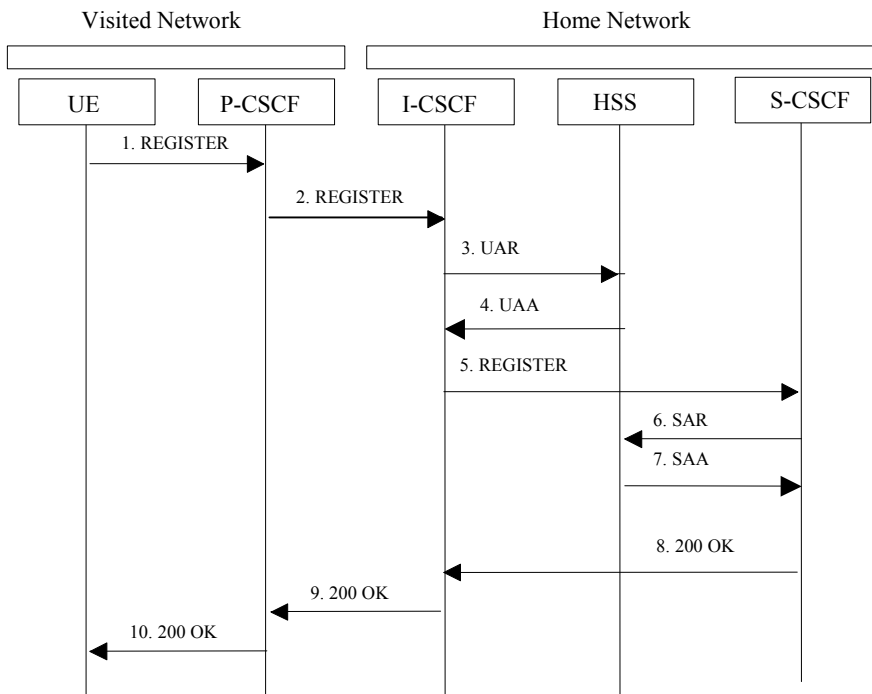


2

3

Figure A.4.2.1: Re-registration

4 **A.4.3 Mobile initiated de-registration**



5

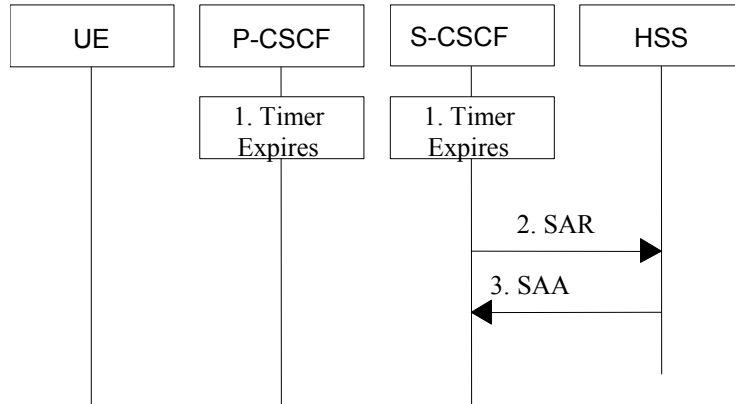
6

Figure A.4.3.1: Mobile initiated de-registration

1 **A.4.4 Network initiated de-registration**

2 **A.4.4.1 Registration timeout**

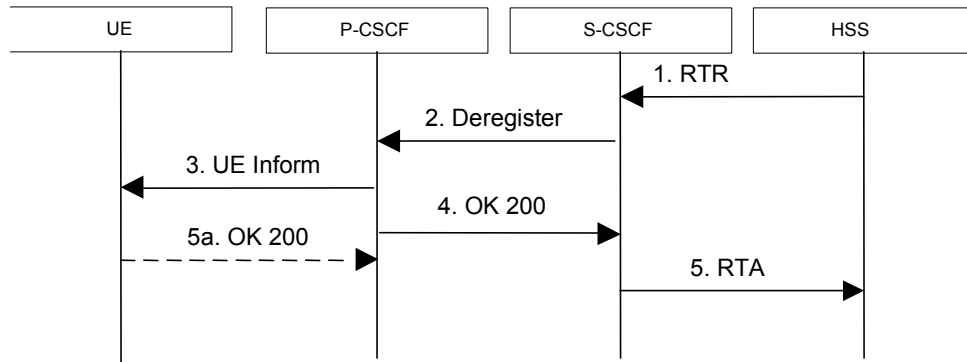
3



4

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

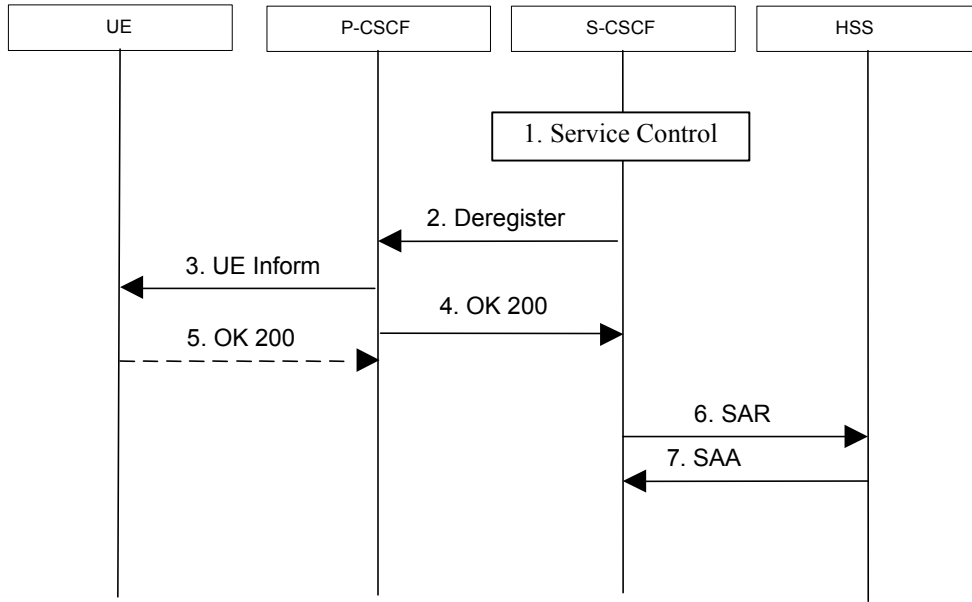
6 **A.4.4.2 Administrative de-registration**



7

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

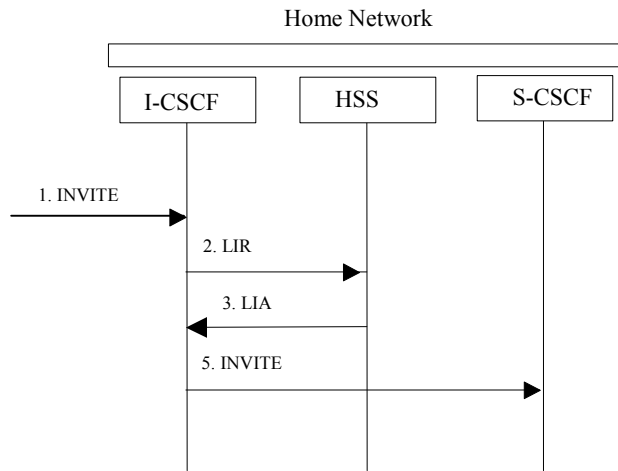
1 **A.4.4.3 De-registration initiated by service platform**



2

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

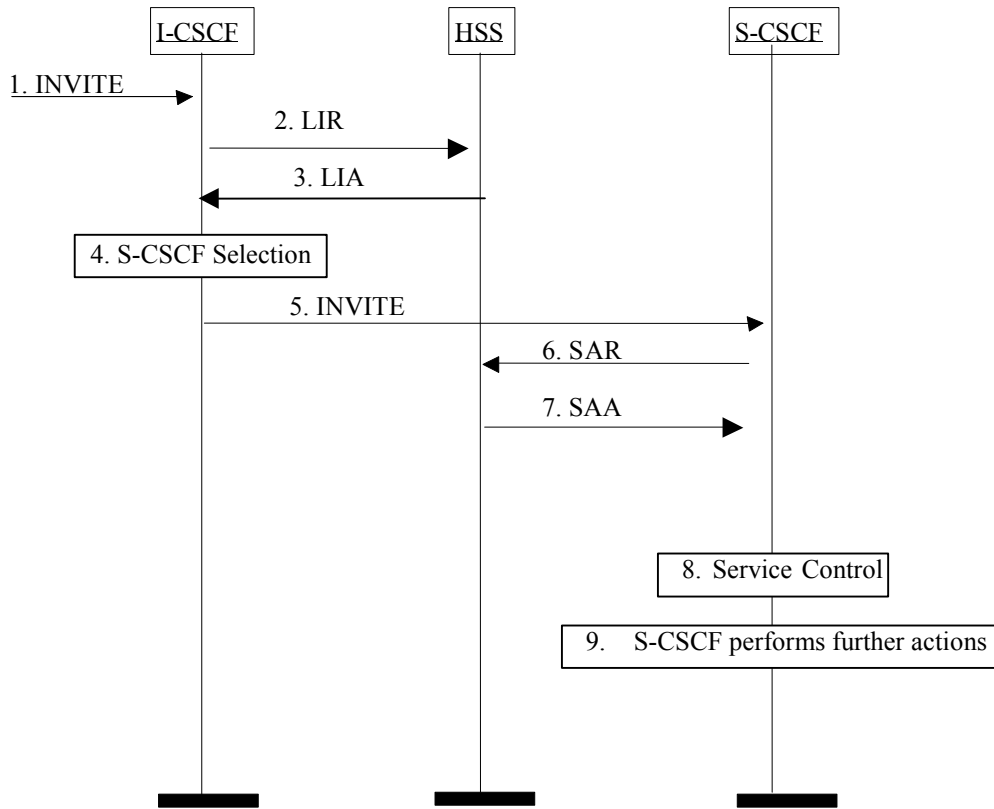
4 **A.4.5 MT SIP session set-up**



5

6 **Figure A.4.5.1: MT SIP session set-up**

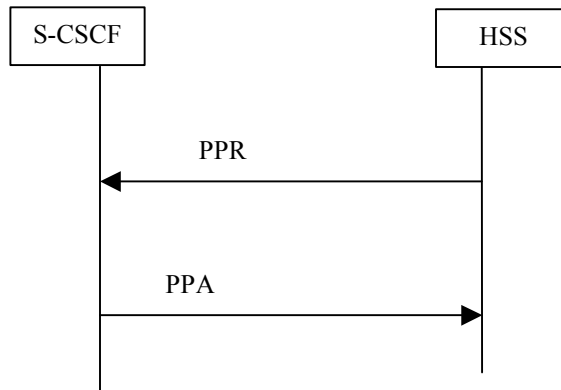
1 **A.4.6 Initiation of a session to a non-registered user**



2
3

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

4 **A.4.7 User Profile update**



5
6
7

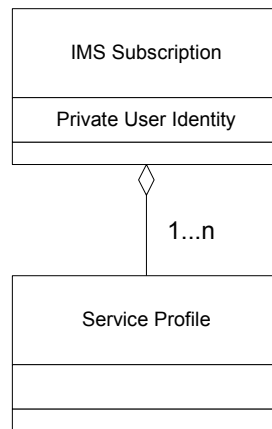
Figure A.4.7.1: User Profile update

1 **Annex B (informative):**
 2 **User Profile UML model**

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

6 **B.1 General description**

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



9

10

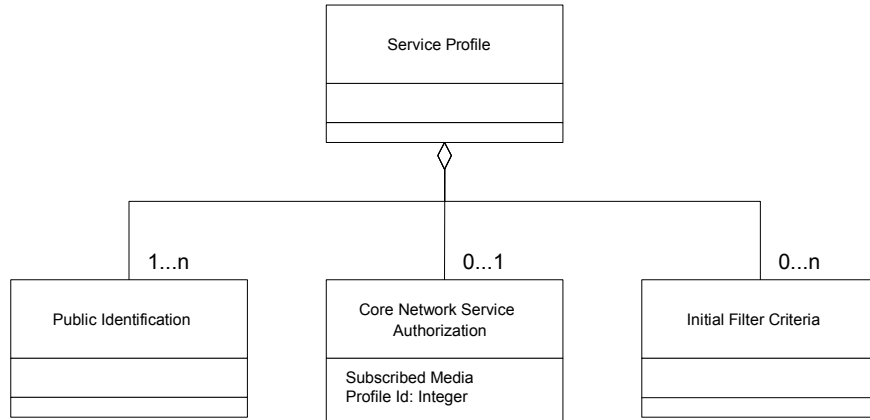
Figure B.1.1: User Profile

11 IMS Subscription class contains as a parameter the private user identity of the user in NAI format.
 12 Each instance of the IMS Subscription class contains one or several instances of the class Service Profile.
 13 Service Profile class contains the meaningful data in the user profile: Public Identification, Core Network
 14 Service Authorization and Initial Filter Criteria.

15 **B.2 Service profile**

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

17 :



1
2

Figure B.2.1: Service Profile

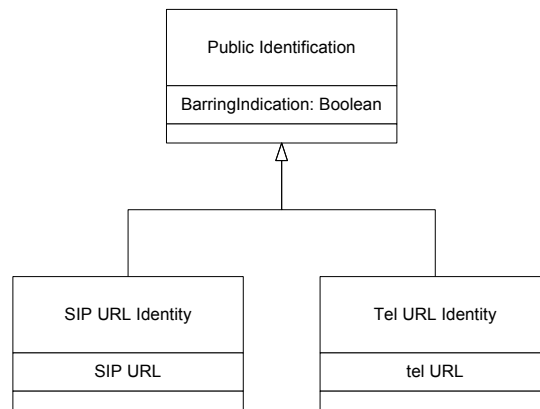
3 Each instance of the Service Profile class consists of one or several instances of the class Public
 4 Identification. Public Identification class contains the public identities of the user associated with that
 5 service profile. The information in the Core Network Service Authorization and Initial Filter Criteria
 6 classes apply to all public identity instances, which are included in one Service profile class. If no instance
 7 of the class Core Network Service Authorization is present, no filtering related to subscribed media applies
 8 in S-CSCF.

9 Each instance of the Service Profile class contains zero or one instance of the class Core Network Service
 10 Authorization. If no instance of the class Core Network Service Authorization is present, no filtering
 11 related to subscribed media applies in S-CSCF.

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

14 **B.2.1 Public Identification**

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



16
17

Figure B.2.1.1: Public Identification

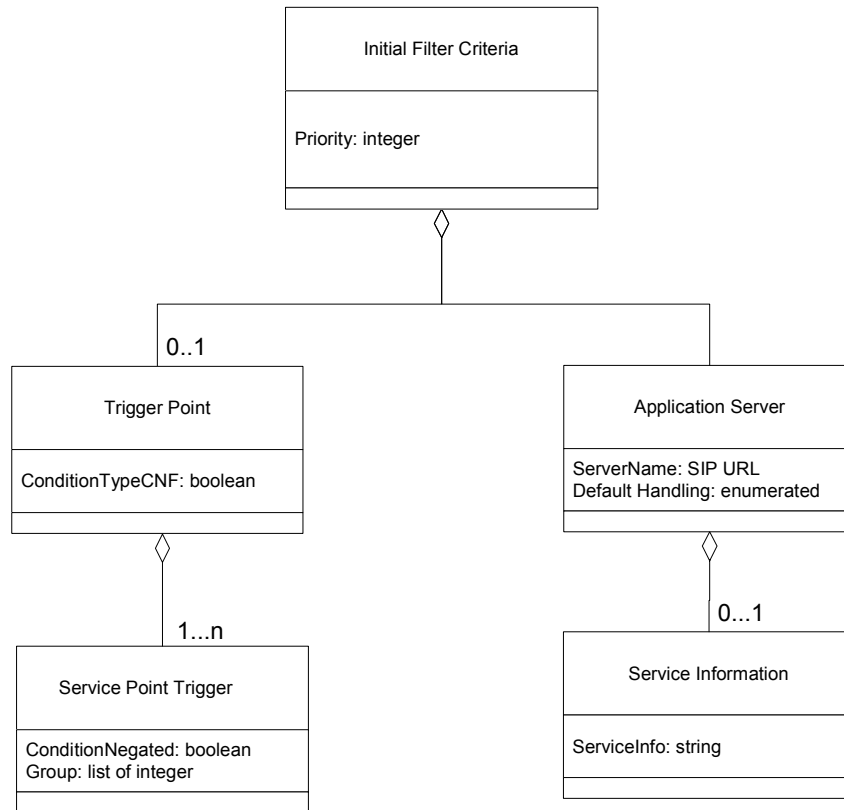
18 Public Identification class can contain either SIP URL Identity, i.e. SIP URL, or Tel URL Identity class, i.e.
 19 tel URL.

20 The attribute BarringIndication is of type Boolean. If it is set to TRUE, the S-CSCF shall prevent that
 21 public identity from being used in any IMS communication except registrations and re-registrations, as
 22 specified in [8].

1 **B.2.2 Initial Filter Criteria**

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

3



4

5

Figure B.2.2.1: Initial Filter Criteria

6 Each instance of the Initial Filter Criteria class is composed of zero or one instance of a Trigger Point class
 7 and one instance of an Application Server class. Priority indicates the priority of the Filter Criteria. The
 8 higher the Priority Number the lower the priority of the Filter Criteria is; i.e., a Filter Criteria with a higher
 9 value of Priority Number shall be assessed after the Filter Criteria with a smaller Priority Number have
 10 been assessed. The same priority shall not be assigned to more than one initial Filter Criterion.

11 ConditionTypeCNF is a boolean that is TRUE when the Trigger Point associated with the FilterCriteria is a
 12 boolean expression in Conjunctive Normal Form (CNF) and FALSE if the Trigger Point is expressed in
 13 Disjunctive Normal Form (DNF) (see Annex C).

14 Trigger Point class describes the trigger points that should be checked in order to find out if the indicated
 15 Application Server should be contacted or not. Each TriggerPoint is a boolean expression in Conjunctive or
 16 Disjunctive Normal form (CNF or DNF). The absence of Trigger Point instance will indicate an
 17 unconditional triggering to Application Server.

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

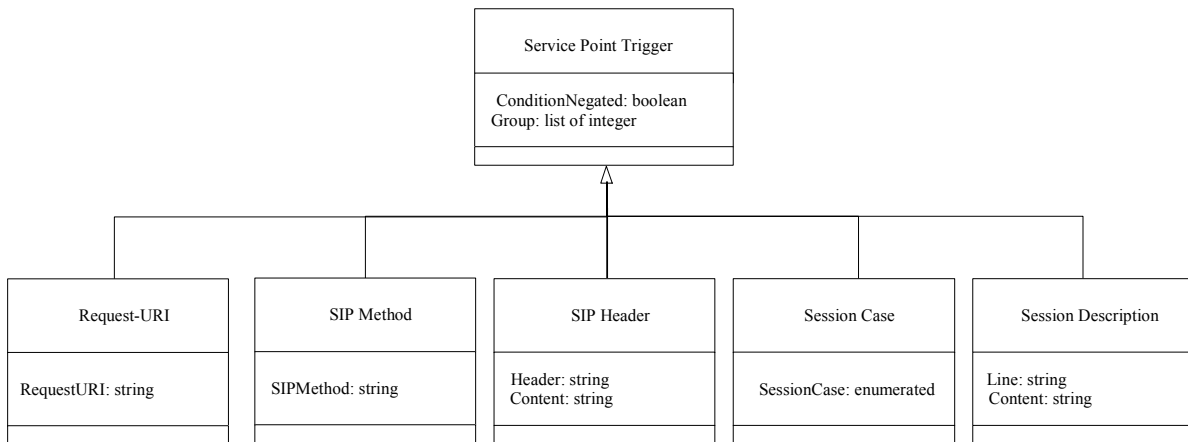
22 Each Trigger Point is composed by 1 to n instances of the class Service Point Trigger.

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

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

9 **B.2.3 Service Point Trigger**

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



11
12

13

Figure B.2.3.1: Service Point Trigger

14 The attribute Group of the class Service Point Trigger allows the grouping of SPTs that will configure the
 15 sub-expressions inside a CNF or DNF expression. For instance, in the following CNF expression
 16 $(A+B).(C+D)$, A+B and C+D would correspond to different groups.

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

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

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

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

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

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

- 1 (1 "Joe": meaning that a given header matches exactly with the string "Joe".
- 2 (1 "^ (Jo).*": meaning that a given header contains a value that begins with "Jo".
- 3 (1 ".*Jo.*": meaning that a given header contains the substring "Jo" at any position.
- 4 The absence of the Content attribute and ConditionNegated = TRUE indicates that the SPT is the absence
5 of a determined SIP header.
- 6 Session Case class represents an enumerated type, with possible values "Originating", "Terminating",
7 "Terminating_Unregistered" indicating if the filter should be used by the S-CSCF handling the Originating,
8 Terminating or Terminating for an unregistered end user services.
- 9 Session Description Information class defines SPT for the content of any SDP field within the body of a
10 SIP Method. The Line attribute identifies the line inside the session description. Content is a string defining
11 the content of the line identified by Line. Perl-like regular expressions shall be taken as a model for regular
12 expressions for this function (as described above).
- 13
- 14

1 **Annex C (informative):** 2 **Conjunctive and Disjunctive Normal Form**

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

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

9 Taking as an example the following trigger:

10 Method = "INVITE" OR Method = "MESSAGE" OR (Method="SUBSCRIBE" AND NOT Header =
11 "from" Match = "joe")

12 *The trigger can be split into the following atomic expressions:*

- 13 • *Method="INVITE"*
- 14 • *Method="MESSAGE"*
- 15 • *Method="SUBSCRIBE"*
- 16 • *NOT header="from" Match="joe"*

17
18 *Grouping the atomic expressions, the CNF expression equivalent to the previous example looks like:*

19
20 *(Method="INVITE" OR Method = "MESSAGE" OR Method="SUBSCRIBE") AND (Method="INVITE"*
21 *OR Method = "MESSAGE" OR (NOT Header = "from" Match = "joe"))*

22
23 *This result in two "OR" groups linked by "AND" (CNF):*

- 24 • *(Method="INVITE" OR Method = "MESSAGE" OR Method="SUBSCRIBE")*
- 25 • *(Method="INVITE" OR Method = "MESSAGE" OR (NOT Header = "from" Content =*
26 *"joe"))*

27
28 *The XML representation of the trigger is:*

29
30 `<?xml version="1.0" encoding="UTF-8"?>`
31 `<testDatatype xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
32 `xsi:noNamespaceSchemaLocation="D:\CxDataType.xsd">`
33 `<IMSSubscription>`
34 `<PrivateID >IMPII@homedomain.com</PrivateID>`
35 `<ServiceProfile >`

```

1      <PublicIdentity >
2          <BarringIndication >1</BarringIndication>
3          <Identity > sip:IMPU1@homedomain.com </Identity>
4      </PublicIdentity>
5      <PublicIdentity >
6          <Identity > sip:IMPU2@homedomain.com </Identity>
7      </PublicIdentity>
8      """" <InitialFilterCriteria >
9      ""    <Priority >0</Priority>
10         <TriggerPoint >
11             <ConditionTypeCNF >1</ConditionTypeCNF>
12             <SPT >
13                 <ConditionNegated >0</ConditionNegated>
14                 <Group >0</Group>
15                 <Method >INVITE</Method>
16             </SPT>
17             <SPT >
18                 <ConditionNegated >0</ConditionNegated>
19                 <Group >0</Group>
20                 <Method >MESSAGE</Method>
21             </SPT>
22             <SPT >
23                 <ConditionNegated >0</ConditionNegated>
24                 <Group >0</Group>
25                 <Method >SUBSCRIBE</Method>
26             </SPT>
27             <SPT >
28                 <ConditionNegated >0</ConditionNegated>
29                 <Group >1</Group>
30                 <Method >INVITE</Method>
31             </SPT>
32             <SPT >

```

```

1           <ConditionNegated >0</ConditionNegated>
2           <Group >1</Group>
3           <Method >MESSAGE</Method>
4       </SPT>
5
6       <SPT >
7           <ConditionNegated >1</ConditionNegated>
8           <Group >1</Group>
9           <SIPHeader >
10              <Header >From</Header>
11              <Content >"joe"</Content>
12          </SIPHeader>
13      </SPT>
14  </TriggerPoint>
15  <ApplicationServer >
16      <ServerName >sip:ASI@homedomain.com</ServerName>
17      <DefaultHandling >0</DefaultHandling>
18  </ApplicationServer>
19  </InitialFilterCriteria>
20 </ServiceProfile>
21 </IMSSubscription>
22 </testDatatype>

```

23

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

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

- 28 • *Method="INVITE"*
- 29 • *Method="MESSAGE"*
- 30 • *Method="SUBSCRIBE" AND (NOT header="from" Match="joe")*

31

32 *The XML representation of the trigger is:*

```

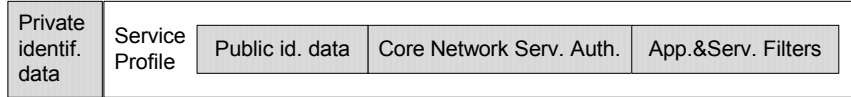
1
2 <?xml version="1.0" encoding="UTF-8"?>
3 <testDatatype xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
4 xsi:noNamespaceSchemaLocation="D:\CxDataType.xsd">
5     <IMSSubscription>
6         <PrivateID >IMPU1@homedomain.com</PrivateID>
7         <ServiceProfile >
8             <PublicIdentity >
9                 <BarringIndication >1</BarringIndication>
10                <Identity > sip:IMPU1@homedomain.com </Identity>
11            </PublicIdentity>
12            <PublicIdentity >
13                <Identity > sip:IMPU2@homedomain.com </Identity>
14            </PublicIdentity>""""
15            <InitialFilterCriteria >
16                ""                <Priority >0</Priority>
17                <TriggerPoint >
18                    <ConditionTypeCNF >0</ConditionTypeCNF>
19                    <SPT >
20                        <ConditionNegated >0</ConditionNegated>
21                        <Group >0</Group>
22                        <Method >INVITE</Method>
23                    </SPT>
24                    <SPT >
25                        <ConditionNegated >0</ConditionNegated>
26                        <Group >1</Group>
27                        <Method >MESSAGE</Method>
28                    </SPT>
29                    <SPT >
30                        <ConditionNegated >0</ConditionNegated>
31                        <Group >2</Group>
32                        <Method >SUBSCRIBE</Method>

```

```
1           </SPT>
2           <SPT >
3               <ConditionNegated >1</ConditionNegated>
4               <Group >2</Group>
5               <SIPHeader >
6                   <Header >From</Header>
7                   <Content >"joe"</Content>
8               </SIPHeader>
9           </SPT>
10          </TriggerPoint>
11          <ApplicationServer >
12              <ServerName >sip:AS1@homedomain.com</ServerName>
13              <DefaultHandling >0</DefaultHandling>
14          </ApplicationServer>
15          </InitialFilterCriteria>
16      </ServiceProfile>
17  </IMSSubscription>
18 </testDatatype>
19
```

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

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



5

6

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

7

8 If more than one service profile is created, for example to assign a different set of filters to public identities
 9 1 and 2 and public identity 3, the information will be packaged in the following way:



10

11

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

12

1 **Annex E (normative):**

2 **XML schema for the Cx interface user profile**

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

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

1

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

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

2

1

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

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

tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1	
		TriggerPoint	tTrigger	(0 to 1)	
		ApplicationServer	tApplicationServer	1	
tTrigger	TriggerPoint	SPT	tSePoTri	(1 to n)	
		ConditionTypeCNF	tBool	1	
tSePoTri	SPT	ConditionNegated	tBool	(0 to 1)	
		Group	tGroupID	(1 to n)	
		Choice of	RequestURI	tString	1
			Method	tString	1
			SIPHeader	tHeader	1
			SessionCase	tDirectionOfRequest	1
SessionDescription	tSessionDescription		1		
tHeader	SIPHeader	Header	tString	1	
		Content	tString	(0 to 1)	
tSessionDescription	SessionDescription	Line	tString	1	
		Content	tString	(0 to 1)	
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1	
		DefaultHandling	tDefaultHandling	(0 to 1)	
		ServiceInfo	tServiceInfo	(0 to 1)	
NOTE: "n" shall be interpreted as non-bounded.					

1

2

1

2 **Annex F (CxDataType.xsd):**

3

```

4 <?xml version="1.0" encoding="UTF-8"?>
5 <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
6 elementFormDefault="qualified" attributeFormDefault="unqualified">
7   <xs:simpleType name="tPriority" final="list restriction">
8     <xs:restriction base="xs:int">
9       <xs:minInclusive value="0"/>
10    </xs:restriction>
11  </xs:simpleType>
12  <xs:simpleType name="tGroupID" final="list restriction">
13    <xs:restriction base="xs:int">
14      <xs:minInclusive value="0"/>
15    </xs:restriction>
16  </xs:simpleType>
17  <xs:simpleType name="tDefaultHandling" final="list restriction">
18    <xs:restriction base="xs:unsignedByte">
19      <xs:maxInclusive value="1"/>
20      <xs:enumeration value="0">
21        <xs:annotation>
22          <xs:documentation>
23            <label
24 xml:lang="en">SESSION_CONTINUED</label>
25              <definition xml:lang="en">Session
26 Continued</definition>
27            </xs:documentation>
28          </xs:annotation>
29        </xs:enumeration>
30        <xs:enumeration value="1">
31          <xs:annotation>
32            <xs:documentation>
33              <label
34 xml:lang="en">SESSION_TERMINATED</label>
35                <definition xml:lang="en">Session
36 Terminated</definition>
37              </xs:documentation>
38            </xs:annotation>
39          </xs:enumeration>
40        </xs:restriction>
41      </xs:simpleType>
42      <xs:simpleType name="tDirectionOfRequest" final="list
43 restriction">
44        <xs:restriction base="xs:unsignedByte">
45          <xs:maxInclusive value="3"/>
46          <xs:enumeration value="0">
47            <xs:annotation>
48              <xs:documentation>
49                <label
50 xml:lang="en">ORIGINATING_SESSION</label>
51                  <definition
52 xml:lang="en">Originating Session</definition>
53                </xs:documentation>
54              </xs:annotation>

```

```

1         </xs:enumeration>
2         <xs:enumeration value="1">
3             <xs:annotation>
4                 <xs:documentation>
5                     <label
6 xml:lang="en">TERMINATING_SESSION</label>
7                     <definition
8 xml:lang="en">Terminating Session</definition>
9                     </xs:documentation>
10                </xs:annotation>
11            </xs:enumeration>
12            <xs:enumeration value="2">
13                <xs:annotation>
14                    <xs:documentation>
15                        <label
16 xml:lang="en">TERMINATING_UNREGISTERED</label>
17                        <definition
18 xml:lang="en">Terminating Session for unregistered user</definition>
19                        </xs:documentation>
20                    </xs:annotation>
21                </xs:enumeration>
22            </xs:restriction>
23        </xs:simpleType>
24        <xs:simpleType name="tPrivateID" final="list restriction">
25            <xs:restriction base="xs:anyURI"/>
26        </xs:simpleType>
27        <xs:simpleType name="tSIP_URL" final="list restriction">
28            <xs:restriction base="xs:anyURI"/>
29        </xs:simpleType>
30        <xs:simpleType name="tTEL_URL" final="list restriction">
31            <xs:restriction base="xs:anyURI"/>
32        </xs:simpleType>
33        <xs:simpleType name="tIdentity" final="list restriction">
34            <xs:union memberTypes="tSIP_URL tTEL_URL"/>
35        </xs:simpleType>
36        <xs:simpleType name="tServiceInfo" final="list restriction">
37            <xs:restriction base="xs:string">
38                <xs:minLength value="0"/>
39            </xs:restriction>
40        </xs:simpleType>
41        <xs:simpleType name="tString" final="list restriction">
42            <xs:restriction base="xs:string">
43                <xs:minLength value="0"/>
44            </xs:restriction>
45        </xs:simpleType>
46        <xs:simpleType name="tBool">
47            <xs:restriction base="xs:boolean"/>
48        </xs:simpleType>
49        <xs:simpleType name="tSubscribedMediaProfileId" final="list
50 restriction">
51            <xs:restriction base="xs:int">
52                <xs:minInclusive value="0"/>
53            </xs:restriction>
54        </xs:simpleType>
55        <xs:complexType name="tIMSSubscription">
56            <xs:sequence>
57                <xs:element name="PrivateID" type="tPrivateID"/>

```

```

1         <xs:element name="ServiceProfile"
2 type="tServiceProfile" maxOccurs="unbounded"/>
3         <xs:any namespace="##Other" processContents="lax"
4 minOccurs="0" maxOccurs="unbounded"/>
5     </xs:sequence>
6 </xs:complexType>
7 <xs:complexType name="tServiceProfile">
8     <xs:sequence>
9         <xs:element name="PublicIdentity"
10 type="tPublicIdentity" maxOccurs="unbounded"/>
11         <xs:element name="CoreNetworkServicesAuthorization"
12 type="tCoreNetworkServicesAuthorization" minOccurs="0"/>
13         <xs:element name="InitialFilterCriteria"
14 type="tInitialFilterCriteria" minOccurs="0" maxOccurs="unbounded"/>
15         <xs:any namespace="##Other" processContents="lax"
16 minOccurs="0" maxOccurs="unbounded"/>
17     </xs:sequence>
18 </xs:complexType>
19 <xs:complexType name="tCoreNetworkServicesAuthorization">
20     <xs:sequence>
21         <xs:element name="SubscribedMediaProfileId"
22 type="tSubscribedMediaProfileId" minOccurs="0"/>
23         <xs:any namespace="##Other" processContents="lax"
24 minOccurs="0" maxOccurs="unbounded"/>
25     </xs:sequence>
26 </xs:complexType>
27 <xs:complexType name="tInitialFilterCriteria">
28     <xs:sequence>
29         <xs:element name="Priority" type="tPriority"/>
30         <xs:element name="TriggerPoint" type="tTrigger"
31 minOccurs="0"/>
32         <xs:element name="ApplicationServer"
33 type="tApplicationServer"/>
34         <xs:any namespace="##Other" processContents="lax"
35 minOccurs="0" maxOccurs="unbounded"/>
36     </xs:sequence>
37 </xs:complexType>
38 <xs:complexType name="tTrigger">
39     <xs:sequence>
40         <xs:element name="ConditionTypeCNF" type="tBool"/>
41         <xs:element name="SPT" type="tSePoTri"
42 maxOccurs="unbounded"/>
43         <xs:any namespace="##Other" processContents="lax"
44 minOccurs="0" maxOccurs="unbounded"/>
45     </xs:sequence>
46 </xs:complexType>
47 <xs:complexType name="tSePoTri">
48     <xs:sequence>
49         <xs:element name="ConditionNegated" type="tBool"
50 default="0" minOccurs="0"/>
51         <xs:element name="Group" type="tGroupID"
52 maxOccurs="unbounded"/>
53     <xs:choice>
54         <xs:element name="RequestURI" type="tString"/>
55         <xs:element name="Method" type="tString"/>
56         <xs:element name="SIPHeader" type="tHeader"/>

```

```

1             <xs:element name="SessionCase"
2 type="tDirectionOfRequest"/>
3             <xs:element name="SessionDescription"
4 type="tSessionDescription"/>
5             </xs:choice>
6             <xs:any namespace="##Other" processContents="lax"
7 minOccurs="0" maxOccurs="unbounded"/>
8         </xs:sequence>
9     </xs:complexType>
10    <xs:complexType name="tHeader">
11        <xs:sequence>
12            <xs:element name="Header" type="tString"/>
13            <xs:element name="Content" type="tString"
14 minOccurs="0"/>
15        </xs:sequence>
16    </xs:complexType>
17    <xs:complexType name="tSessionDescription">
18        <xs:sequence>
19            <xs:element name="Line" type="tString"/>
20            <xs:element name="Content" type="tString"
21 minOccurs="0"/>
22        </xs:sequence>
23    </xs:complexType>
24    <xs:complexType name="tApplicationServer">
25        <xs:sequence>
26            <xs:element name="ServerName" type="tSIP_URL"/>
27            <xs:element name="DefaultHandling"
28 type="tDefaultHandling" minOccurs="0"/>
29            <xs:element name="ServiceInfo" type="tServiceInfo"
30 minOccurs="0"/>
31            <xs:any namespace="##Other" processContents="lax"
32 minOccurs="0" maxOccurs="unbounded"/>
33        </xs:sequence>
34    </xs:complexType>
35    <xs:complexType name="tPublicIdentity">
36        <xs:sequence>
37            <xs:element name="BarringIndication" type="tBool"
38 default="0" minOccurs="0"/>
39            <xs:element name="Identity" type="tIdentity"/>
40        </xs:sequence>
41    </xs:complexType>
42    <xs:element name="IMSSubscription" type="tIMSSubscription"/>
43 </xs:schema>
44
45

```