3GPP TSG CN Plenary Meeting #19 **NP-030101**
12th – 14th March 2003 Birmingham, UK.

Source: TSG CN WG4

Title: Corrections on IP-based Multimedia Services Cx/Dx-interface

Agenda item: 8.1

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
23.008	065	1	N4-030241	Rel-5	Clarification of IMPU barring handling	F	5.3.0
29.228	030	1	N4-030242	Rel-5	Clarification of IMPU barring handling	F	5.2.0
23.008	067	1	N4-030251	Rel-5	Definition of the Subscribed Media Profile Identifier	F	5.3.0
29.228	040	1	N4-030252	Rel-5	Definition of the Subscribed Media Profile Identifier	F	5.2.0
29.228	024	1	N4-030240	Rel-5	Clarification of the HSS behaviour in REGISTRATION and DE_REGISTRATION procedures at IMPU checking time	F	5.2.0
29.228	025	1	N4-030238	Rel-5	Clarification of service profile download at service profile modification.	F	5.2.0
29.228	026		N4-030014	Rel-5	Error in definition of Service Point of Interest class	F	5.2.0
29.228	027		N4-030015	Rel-5	Deletion of Annex F	F	5.2.0
29.228	028		N4-030016	Rel-5	Filter ID field removal in InitialFilterCriteria class	F	5.2.0
29.228	029		N4-030017	Rel-5	Clarification of User-Authorization-Type AVP usage within UAR	F	5.2.0
29.228	031	1	N4-030243	Rel-5	Update TS 29.228 after Diameter has become RFC	F	5.2.0
29.229	012	1	N4-030244	Rel-5	Update TS 29.229 after Diameter has become RFC	F	5.2.0
29.228	032	1	N4-030245	Rel-5	The default public user identity in the Server-Assignment-Answer	F	5.2.0
29.228	033	1	N4-030246	Rel-5	Replacement of the NAS-Session-Key AVP	F	5.2.0
29.229	013		N4-030077	Rel-5	Replacement of the NAS-Session-Key AVP	F	5.2.0
29.228	034	2	N4-030247	Rel-5	Corrections to service profile	F	5.2.0
29.228	035	2	N4-030312	Rel-5	Clarification on Re-allocation of S-CSCF	F	5.2.0
29.229	015	1	N4-030277	Rel-5	Clarification on Re-allocation of S-CSCF	F	5.2.0
29.228	037	3	N4-030314	Rel-5	Handling of non supported data in the S-CSCF when the profile is being updated	F	5.2.0
29.229	018	1	N4-030237	Rel-5	Handling of non supported data in the S-CSCF when the profile is being updated	F	5.2.0
29.228	038	1	N4-030261	Rel-5	Change of SPI to SPT	F	5.2.0
29.328	019	1	N4-030268	Rel-5	Change of SPI to SPT	F	5.2.1
29.229	014		N4-030079	Rel-5	Correction to the values of User-Authorizatin-Type AVP	F	5.2.0

3GPP TSG CN WG4 Meeting #18 **N4-030241**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **23.008** **CR** **065** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification of IMPU barring handling
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/12/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Alignment with IMS stage 2 for handling of IP multimedia communication for barred public user identities.
Summary of change:	⌘	Barred IMPUs are related to all IMS communication and not limited to IMS sessions. Re-registrations can not modify the From identity, so barred IMPUs will be present in re-registrations if they were present in the registration procedure. This implies that the rules for registration regarding barring IMPU is extensible to re-registration, i.e., re-registration must be allowed with barred ID.
Consequences if not approved:	⌘	Misconcept of Barred IMPUs and when to apply the barring.

Clauses affected:	⌘	3.1.3

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		TS 29.228-030
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

3.1.3 Barring indication

Flag associated to each public identity to indicate that the identity is barred ~~for~~ from~~the initiation or termination of sessions in the IMS domain~~any IMS communication (except registrations and re-registrations).

The Barring indication is permanent subscriber data and is stored in the HSS and in the S-CSCF.

End of modified section

3GPP TSG CN WG4 Meeting #18
Dublin, EIRE, 10th – 14th February 2003

N4-030251

CR-Form-v7

CHANGE REQUEST

⌘ **23.008** **CR** **067** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Definition of the Subscribed Media Profile Identifier
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	11/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	To clearify the handling of subscribed media
Summary of change:	⌘	Information on subscribed media is downloaded from HSS to S-CSCF. The information on subscribed media is provided in the form of a profile identifier; details of the allowed media parameters associated with the profile identifier are configured in the S-CSCF.
Consequences if not approved:	⌘	Handling of subscribed media remains unclear

Clauses affected:	⌘	3.5.1, 5.3

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	29.228-040
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3.5.1 Subscribed Media Profile Identifier

The Subscribed Media Profile Identifier identifies a set~~shall provide a list~~ of session description parameters ~~media types~~ that the subscriber is authorized to request. The translation from the Profile Identifier to the set of subscribed media is performed in the S-CSCF based on operator configuration. ~~This shall include SDP Media Types, Transport Protocols, Media Format and Bandwidth. The format of the list and the parameters contained within is FFS.~~

The Subscribed Media Profile Identifier is permanent data stored in the HSS and in the S-CSCF.

~~3.5.1 Void~~

****Next modification**********

5.3 IP Multimedia Service Data Storage

Table 3: Overview of data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	TYPE
Private User Identity	3.1.1	M	M		-	P
Public Identity	3.1.2	M	M		-	P
Barring Indication	3.1.3	M	M		-	P
Registration Status	3.2.1	M	-		-	T
S-CSCF Name	3.2.2	M	-		-	T
Diameter Client Address of S-CSCF	3.2.3	M	-		-	T
Diameter Server Address of HSS	3.2.3	-	M		-	T
RAND, XRES, CK, IK and AUTN	3.3.1	M	C		-	T
Server Capabilities	3.4.1	C	C		-	P
Subscribed Media Profile Identifier	3.5.1	C	C		-	P
Initial Filter Criteria	3.5.2	C	C		-	P
Service Indication	3.5.4	M	-		M	P
GsmSCF address for IM CSI	3.8.4	C	-		-	P
IM-SSF address for IM CSI	3.8.5	C	-		-	T
O-IM-CSI	3.8.1	C	-	C	-	P
VT-IM-CSI	3.8.2	C	-	C	-	P
D-IM-CSI	3.8.3	C	-	C	-	P

3GPP TSG CN WG4 Meeting #18 **N4-030240**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **024** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification of the HSS behaviour in REGISTRATION and DE_REGISTRATION procedures at IMPU checking time.
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Public Identities registration states are checked when the User_Authorization_Type value received in the UAR is equal to REGISTRATION or DE_REGISTRATION (never in the REGISTRATION_AND_CAPABILITIES value). When checking the registration state of the public identity received, the same error code (DIAMETER_SUBSEQUENT_REGISTRATION) is returned irrespective of the value of User-Authorization-Type (REGISTRATION or DE_REGISTRATION). Ambiguity in definition of HSS behaviour for public identities not registered when User-Authorization-Type is different from DE_REGISTRATION.
Summary of change:	⌘	HSS behaviour (which error code has to be returned) has to be defined in the DE_REGISTRATION case when the IMPU is registered or unregistered. Clarify that the public identity state is checked only at REGISTRATION or DE_REGISTRATION User-Authorization-Type values.
Consequences if not approved:	⌘	Misinterpretation of HSS behaviour at registration and de-registration procedure when IMPUs are checked.

Clauses affected:	⌘	6.1.1, 6.1.2, 6.1.4.1, Table 6.3.5

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	

	X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

6.1 Location management procedures

6.1.1 User registration status query

---------Beginning of first modified section----------

6.1.1.1 Detailed behaviour

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

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

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

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

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

     - If so, continue to step 4.

     - If not, Vendor-Specific-Result shall be set to DIAMETER_AUTHORIZATION_REJECTED.

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

   - If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not Vendor-Specific-Result shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). Continue to step 5.

   - If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.

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

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

   - If it is registered, the HSS shall return the stored S-CSCF name. No ~~and never any~~ S-CSCF capabilities shall be present in the response. ~~In case the~~If User-Authorization-Type is equal to REGISTRATION, ~~and~~ Vendor-Specific-Result ~~is~~shall be set to DIAMETER_SUBSEQUENT_REGISTRATION. If User-Authorization-Type ~~it~~ is equal to DE-REGISTRATION, Vendor-Specific-Result ~~is~~shall be set to DIAMETER_SUCCESS.~~The HSS shall not return any S-CSCF capabilities.~~

   - If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name ~~and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION~~. If it may be necessary to select a new S-CSCF, the HSS shall also return S-CSCF capabilities. Considering the information received from the HSS, the I-CSCF shall determine whether it has or not to select a new S-CSCF. ~~In case~~If ~~the~~ User-Authorization-Type is equal to REGISTRATION, Vendor-Specific-Result ~~is~~shall be set to DIAMETER_SUBSEQUENT_REGISTRATION. If User-Authorization-Type ~~it~~ is equal to DE-REGISTRATION, Vendor-Specific-Result ~~is~~shall be set to DIAMETER_SUCCESS.

- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
    - If the value of User-Authorization-Type is ~~equal to~~ DE_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Vendor-Specific-Result to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.
    - If the value of User-Authorization-Type is ~~different from DE_REGISTRATION~~~~equal to~~ REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
        - If there is at least one identity of the user that is registered the HSS shall return the S-CSCF name assigned for the user and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
        - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. If it may be necessary to select a new S-CSCF, the HSS shall also return S-CSCF capabilities. Considering the information received from the HSS, the I-CSCF shall determine whether it has or not to select a new S-CSCF.
        - If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The returned capabilities shall satisfy the most restrictive service profile of the user. The list of S-CSCF capabilities may be empty, to indicate to the I-CSCF that it may select any available S-CSCF. Vendor-Specific-Result shall be set to DIAMETER_FIRST_REGISTRATION. The HSS shall not return any S-CSCF name.

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

---------End of first modified section----------

---------Beginning of second modified section----------

6.1.2 S-CSCF registration/deregistration notification

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

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

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

Table 6.1.2.1: S-CSCF registration/deregistration notification request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	C	User public identity or list of user public identities. At least one public identity shall be present if User-Name is not present in the request.

S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity (See 7.3)	User-Name	C	User private identity. It shall be present if it is available when the S-CSCF issues the request. It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER. In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present. This indicates that all public identities shall be de-registered.
Server Assignment Type (See 7.8)	Server-Assignment-Type	M	Type of update the S-CSCF requests in the HSS (e.g: de-registration). See 3GPP TS 29.229 [5] for all the possible values.
User Data Request Type (See 7.15)	User-Data-Request-Type	M	Part of the user profile the S-CSCF requests from the HSS (e.g: complete profile). See 3GPP TS 29.229 [5] for all the possible values.
User Data Already Available (See 7.16)	User-Data-Already-Available	M	This indicates if the user profile is already available in the S-CSCF.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command. This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent ~~in case~~as a consequence of a~~the~~ session termination~~ng the session~~ for an unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	M	User private identity.
Registration result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of registration.

User Profile (See 7.7)	User-Data	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT. If the Server-Assignment-Type in the request is equal to REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER the User-Data AVP shall be present according to the rules defined in the section 6.6. 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 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging-Information	O	Addresses of the charging functions.

6.1.2.1 Detailed behaviour

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---------End of second modified section----------

---------Beginning of third modified section----------

6.1.4.1 Detailed behaviour

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

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

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

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

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

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

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

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

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

---------End of third modified section----------

---------End of fourth modified section----------

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be ~~included~~ present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, Base 64 encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. One example of the format of the SIP-Authenticate AVP is: 'nonce=" dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 "' where the nonce " dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 " contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1).
Authorization Information (See 7.9.4)	SIP-Authorization	M	In shall contain, base 64 encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES. One example of the format of the SIP-Authorization AVP is: 'response="6629fae49393a05397450978507c4ef1"' where response="6629fae49393a05397450978507c4ef1" contains, base64 encoded, XRES.
Confidentiality Key (See 7.9.5)	NAS-Session-Key	O	This information element may contain the confidentiality key. NAS-Session-Key is a grouped AVP. When present the following describes its content: - NAS-Key-Direction equal to BIDIRECTIONAL. - NAS-Key-Type equal to CIPHER_KEY. - NAS-Key-Data contains the confidentiality key.
Integrity Key (See 7.9.6)	NAS-Session-Key	M	This information element shall contain the integrity key. NAS-Session-Key is a grouped AVP. When present the following describes its content: - NAS-Key-Direction equal to BIDIRECTIONAL. - NAS-Key-Type equal to INTEGRITY_KEY. - NAS-Key-Data contains the integrity key.

---------Beginning of fourth modified section----------

3GPP TSG CN WG4 Meeting #18 **N4-030238**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **025** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Clarification of service profile download at service profile modification.
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Unclear service profile download mechanism when modifications occur in the user profile
Summary of change:	⌘	Clarify that when a modification in the user profile occurs and the HSS performs the download, the complete registered part of the user profile, the unregistered part of both parts will be downloaded, not only changes (following TS 23.228, 5.1.5). The S-CSCF will then overwrite the concerned profile. Clarify that when there is implicit registration, all the public identities are included in the S-CSCF initiated request, with the corresponding service profiles (modified and non- modified).
Consequences if not approved:	⌘	Mis-interpretation of the content of the user profile in the update operation initiated by the HSS.

Clauses affected:	⌘	6.2.2, 6.5.2, 6.6.1

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

6.2.2 HSS initiated update of User Profile

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

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

Table 6.2.2.1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	M	User private identity.
User profile (See 7.7)	User-Data	M	Updated ~~service~~ user profile (see section 6.6.1), with the format defined in chapter 7.7~~8.8~~.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given multimedia user. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

Table 6.2.2.2: User Profile Update response

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

6.2.2.1 Detailed behaviour

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

The S-CSCF shall overwrite, for the public user identities indicated in the request, current information with the information received from the HSS.

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

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

Table 6.2.2.1.1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_SUCCESS_NOT SUPPORTED_USER_DATA	The request succeeded. However, the S-CSCF informs

	the HSS that the received subscription data contained information, which was not recognised or supported.
DIAMETER_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.

End of modified section

Beginning of modified section

6.5.2 HSS initiated procedures

6.5.2.1 ~~(void)~~Update of User Profile

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

6.5.2.2 De-registration

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

End of modified section

Beginning of modified section

6.6.1 HSS initiated update of User Profile

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

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

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

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

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030014**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **026** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Error in definition of Service Point of Interest class
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	ServicePointofInterest class diagram not related to paragraph explanation
Summary of change:	⌘	Title and paragraph explanation in annex B.2.3 are aligned.
Consequences if not approved:	⌘	Misinterpretation of Trigger Point and Service Point of Interest.

Clauses affected:	⌘	B.2.3			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

B.2.3 ~~Trigger Point~~Service Point of Interest

The following picture gives an outline of the UML model of ~~Filter Criteria~~Service Point of Interest class:

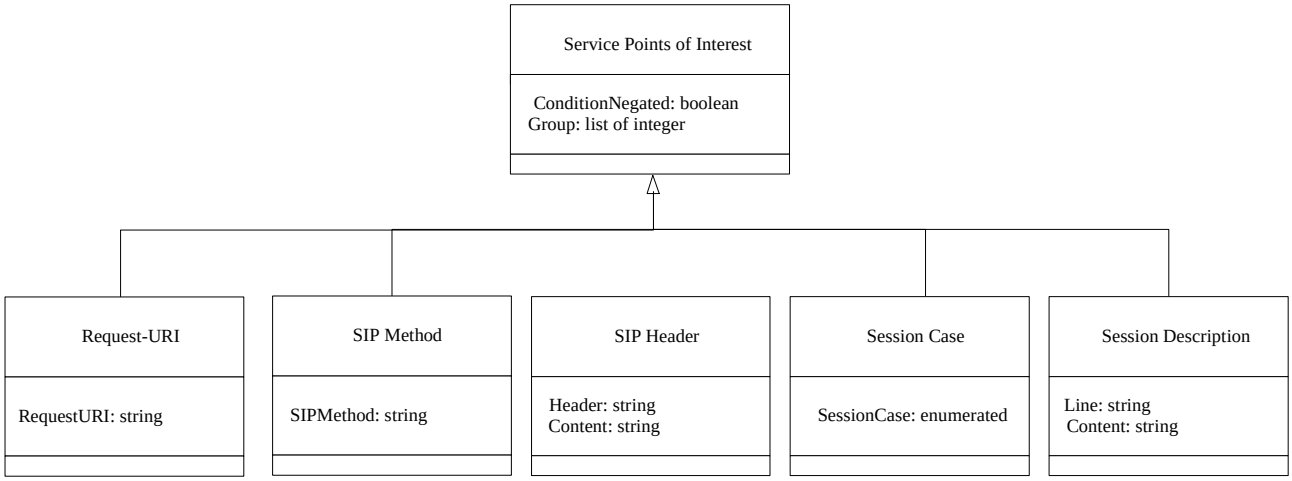


Figure B.2.3.1: Service Point of Interest~~Trigger Point~~

End of modified section

3GPP TSG CN WG4 Meeting #18
Dublin, EIRE, 10th – 14th February 2003

N4-030015

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **027** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Deletion of Annex F
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	There is already a reference to the XML schema in Annex E, so the Annex F text is already present in the normative Annex E.
Summary of change:	⌘	Removal of Annex F.
Consequences if not approved:	⌘	Duplication of information

Clauses affected:	⌘	Annex F			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

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

~~The file CxDataTypes.xsd, attached to this specification, contains the XML schema with the data description for Cx interface.~~

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030016**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **028** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Filter ID field removal in InitialFilterCriteria class
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	There is a mis-alignment between Figure B.2.2.1.1 and the text below it. The text describes the attribute FilterId which is not present in the figure..
Summary of change:	⌘	Removal of the sentence describing FilterId as an attribute of the Initial Filter Criteria class.
Consequences if not approved:	⌘	Inconsistency between Figure B.2.2.1.1 and the descriptive text below it.

Clauses affected:	⌘	B.2.2

Other specs affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

B.2.2 Initial Filter Criteria

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

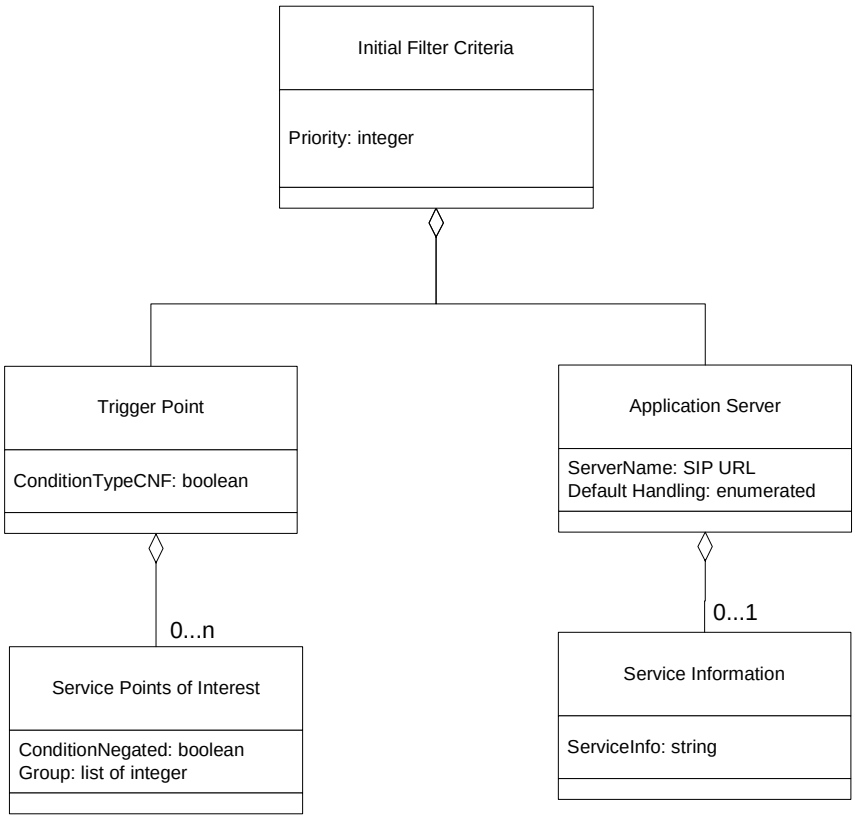


Figure B.2.2.1.1: Initial Filter Criteria

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

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030017**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **029** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Clarification of User-Authorization-Type AVP usage within UAR
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Wrong implemented CR.
Summary of change:	⌘	According to CR-016 (N4-021514), the User_Authorization_Type AVP in UAR message is not clearly defined. Behaviour at REGISTRATION and DE-REGISTRATION procedures was not correctly implemented.
Consequences if not approved:	⌘	Wrong implementation of User_Authorization_Type AVP in UAR.

Clauses affected:	⌘	6.1.1			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

6.1.1 User registration status query

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

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

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

Table 6.1.1.1 : User registration status query

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	User public identity to be registered
Visited Network Identifier (See 7.1)	Visited-Network-Identifier	M	Identifier that allows the home network to identify the visited network
Type of Authorization (See 7.14)	User-Authorization-Type	C	Type of authorization requested by the I-CSCF. If the request corresponds to a de-registration, i.e. Expires field in the REGISTER method is equal to zero, this AVP ~~may~~ shall be ~~absent~~ present ~~from~~ in the command and the value shall be set to DE-REGISTRATION. If the request corresponds to an initial registration or a re-registration, i.e. Expires field in the REGISTER method is not equal to zero then this AVP may ~~not~~ be ~~present~~ absent ~~in~~ from the command. If present its value shall be set to REGISTRATION. If the request corresponds to an initial registration or a re-registration, and the I-CSCF explicitly queries the S-CSCF capabilities, then this AVP shall be present in the command and the value shall be set to REGISTRATION_AND_CAPABILITIES. The I-CSCF shall use this value when the user's current S-CSCF, which is stored in the HSS, cannot be contacted and a new S-CSCF needs to be selected.
Private User Identity (See 7.3)	User-Name	M	User private identity
Routing Information (See 7.13)	Destination-Host, Destination-Realm	C	If the I-CSCF knows HSS name Destination-Host AVP shall be present in the command. Otherwise, only Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the I-CSCF.

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030242**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **030** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification of IMPU barring handling
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/12/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	Alignment with IMS stage 2 for handling of IP multimedia communication for barred public user identities.
Summary of change:	⌘	Barred IMPUs are related to all IMS communication and not limited to IMS sessions. Re-registrations can not modify the From identity, so barred IMPUs will be present in re-registrations if they were present in the registration procedure. This implies that the rules for registration regarding barring IMPU is extensible to re-registration, i.e., re-registration must be allowed with barred ID.
Consequences if not approved:	⌘	Misconcept of Barred IMPUs and when to apply the barring.

Clauses affected:	⌘	2, B.2.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		TS 23.008-065
			X	Test specifications		
			X	O&M Specifications		

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

2 References

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

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

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

[4] 3GPP TS 23.002 “Network architecture”.

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

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

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

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

End of modified section

Beginning of modified section

B.2.1 Public Identification

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

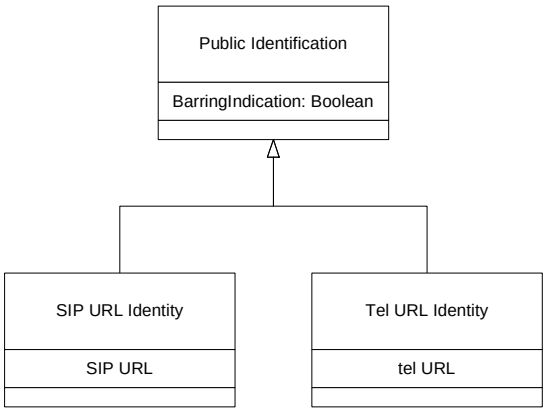


Figure B.2.1.1: Public Identification

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

The attribute BarringIndication is of type Boolean. If it is set to TRUE, the S-CSCF shall prevent that public identity from being used ~~to establish multimedia sessions~~in any IMS communication ~~procedure (both originating and terminating sessions are barred~~excluding except registrations and re-registrations~~)~~, as specified in 3GPP TS 24.229 [8].

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030243**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **031** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Update TS 29.228 after Diameter has become RFC
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Alignment with IETF Diameter Base Protocol
Summary of change:	⌘	Alignment with the new Experimental-Result AVP.
Consequences if not approved:	⌘	Misalignment with the Diameter standard protocol

Clauses affected:	⌘	6.1, 6.2, 6.3, A.3

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

2 References

…

[9] draft-ietf-aaa-diameter-17, "Diameter Base Protocol", work in progress

End of modified section

Beginning of modified section

6.1 Location management procedures

6.1.1 User registration status query

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

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

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

Table 6.1.1.1 : User registration status query

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	User public identity to be registered
Visited Network Identifier (See 7.1)	Visited-Network-Identifier	M	Identifier that allows the home network to identify the visited network

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

Table 6.1.1.2 : User registration status response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / ~~Vendor-Specific~~Experimental-Result	M	Result of the operation. Result-Code AVP ~~will~~shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP ~~will~~shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the user.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

6.1.1.1 Detailed behaviour

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

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

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

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

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

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

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

- If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not ~~Vendor-Specific-Result~~Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). Continue to step 5.
- If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.
- If it is REGISTRATION_AND_CAPABILITIES, the HSS shall check that the user is allowed to roam in the visited network (if not ~~Vendor-Specific-Result~~Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). The HSS shall return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy the most restrictive service profile of the user. The list of capabilities may be empty, to indicate to the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name. Stop processing.

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

- If it is registered, the HSS shall return the stored S-CSCF name and ~~Vendor-Specific-Result~~Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
- If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name and ~~Vendor-Specific-Result~~Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. If it may be necessary to select a new S-CSCF, the HSS shall also return S-CSCF capabilities. Considering the information received from the HSS, the I-CSCF shall determine whether it has or not to select a new S-CSCF.
- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
  - If the value of User-Authorization-Type is equal to DE_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the ~~Vendor-Specific-Result~~Experimental-Result-Code to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.
  - If the value of User-Authorization-Type is different from DE_REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
    - If there is at least one identity of the user that is registered the HSS shall return the S-CSCF name assigned for the user and ~~Vendor-Specific-Result~~Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
    - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored), the HSS shall return the stored S-CSCF name and ~~Vendor-Specific-Result~~Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. If it may be necessary to select a new S-CSCF, the HSS shall also return S-CSCF capabilities. Considering the information received from the HSS, the I-CSCF shall determine whether it has or not to select a new S-CSCF.
    - If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The returned capabilities shall satisfy the most restrictive service profile of the user. The list of S-CSCF capabilities may be empty, to indicate to the I-CSCF that it may select any available S-CSCF. ~~Vendor-Specific-Result~~Experimental-Result-Code shall be set to DIAMETER_FIRST_REGISTRATION. The HSS shall not return any S-CSCF name.

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

6.1.2 S-CSCF registration/deregistration notification

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

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

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

Table 6.1.2.1: S-CSCF registration/deregistration notification request

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

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

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	M	User private identity.
Registration result (See 7.6)	Result-Code / ~~Vendor-Specific-Result~~Experimental-Result	M	Result of registration. Result-Code AVP ~~will~~shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP ~~will~~shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile (See 7.7)	User-Data	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT. 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 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging-Information	O	Addresses of the charging functions.

6.1.2.1 Detailed behaviour

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.1.3 Network initiated de-registration by the HSS, administrative

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

HSS may decide to de-register:

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

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

Table 6.1.3.1 : Network Initiated Deregistration by HSS request

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

Table 6.1.3.2 : Network Initiated Deregistration by HSS response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / ~~Vendor-Specific~~Experimental-Result	M	This information element indicates the result of de-registration. Result-Code AVP ~~will~~shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP ~~will~~shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

6.1.3.1 Detailed behaviour

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

The HSS may de-register:

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

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

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

6.1.4 User location query

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

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

Table 6.1.4.1 : User Location query

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

Table 6.1.4.2 : User Location response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / ~~Vendor-Specific~~Experimental-Result	M	Result of the operation. Result-Code AVP ~~will~~shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP ~~will~~shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

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

6.1.4.1 Detailed behaviour

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

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

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

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

   - If it is not registered, but has services related to unregistered state, the HSS shall check if at least there is at least one identity or the user with an S-CSCF name assigned:If this is the case the HSS shall return the S-CSCF name assigned for that user. The Server-Name AVP shall contain the SIP URL of the server. The Server-Capabilities AVP shall not be present. The Result-Code shall be set to DIAMETER_SUCCESS.

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

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

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

6.2 User data handling procedures

6.2.1 User Profile download

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

6.2.2 HSS initiated update of User Profile

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

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

Table 6.2.2.1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description

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

Table 6.2.2.2: User Profile Update response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / ~~Vendor-Specific~~Experimental-Result	M	This information element indicates the result of the update of User Profile in the S-CSCF. Result-Code AVP ~~will~~shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP ~~will~~shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

6.2.2.1 Detailed behaviour

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

The S-CSCF shall overwrite, for the identities indicated in the request, current information with the information received from the HSS.

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

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

Table 6.2.2.1.1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_SUCCESS_NOT SUPPORTED_USER_DATA	The request succeeded. However, the S-CSCF informs the HSS that the received subscription data contained information, which was not recognised or supported.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in S-CSCF.
DIAMETER_ERROR_TOO_MUCH_DATA	The request failed. The S-CSCF informs to the HSS that it tried to push too much data into the S-CSCF.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

6.3 Authentication procedures

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

- To retrieve authentication vectors from the HSS.

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

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

Table 6.3.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	This information element contains the public identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the user private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Tables 6.3.2 and 6.3.3 for the contents of this information element. The content shown in table 6.3.2 shall be used for a normal authentication request; the content shown in table 6.3.3 shall be used for an authentication request after synchronization failure.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name this AVP shall be present. This information is available if the MAR belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent in case of the initial registration. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the client.

Table 6.3.2: Authentication Data content – request

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

Table 6.3.3: Authentication Data content – request, synchronization failure

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of nonce and AUTS, base 64 encoded. S-CSCF shall include the nonce sent to the terminal and the auts directive received from the terminal. See 3GPP TS 33.203 [3] for further details about RAND and AUTS. See [7] for further details about based 64 encoding. One example of content is: 'nonce=" dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 ", auts="5ccc069c403ebaf9f0171e9517f40e41"' where nonce "dcd98b7102dd2f0e8b11d0f600bfb0c093" contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1) and auts "5ccc069c403ebaf9f0171e9517f40e41" contains, base 64 encoded, AUTS.
Routing Information (See 7.13)	Destination-Host	M	In this case the MAR belongs to an already existing registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.

Table 6.3.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	User public identity
Private User Identity (See 7.3)	User-Name	M	User private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	Number of authentication vectors delivered 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 / ~~Vendor-Specific~~Experimental-Result	M	Result of the operation. Result-Code AVP ~~will~~shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP ~~will~~shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be included present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, Base 64 encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. One example of the format of the SIP-Authenticate AVP is: 'nonce=" dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 "' where the nonce " dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 " contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1).
Authorization Information (See 7.9.4)	SIP-Authorization	M	In shall contain, base 64 encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES. One example of the format of the SIP-Authorization AVP is: 'response="6629fae49393a05397450978507c4ef1"' where response="6629fae49393a05397450978507c4ef1" contains, base64 encoded, XRES.
Confidentiality Key (See 7.9.5)	NAS-Session-Key	O	This information element may contain the confidentiality key. NAS-Session-Key is a grouped AVP. When present the following describes its content: - NAS-Key-Direction equal to BIDIRECTIONAL. - NAS-Key-Type equal to CIPHER_KEY. - NAS-Key-Data contains the confidentiality key.
Integrity Key (See 7.9.6)	NAS-Session-Key	M	This information element shall contain the integrity key. NAS-Session-Key is a grouped AVP. When present the following describes its content: - NAS-Key-Direction equal to BIDIRECTIONAL. - NAS-Key-Type equal to INTEGRITY_KEY. - NAS-Key-Data contains the integrity key.

6.3.1 Detailed behaviour

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

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

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

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

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

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

- If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

  - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It ~~will~~ shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

  - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored), the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

  - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It ~~will~~ shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

  - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It ~~will~~ shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it is not registered, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It ~~will~~ shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

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

End of modified section

Beginning of modified section

A.3 Cx message parameters to Diameter AVP mapping

The following table gives an overview about the mapping:

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

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

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030245**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **032** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	The default public user identity in the Server-Assignment-Answer
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	11/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	The TS 24.229 (v.5.3.0) sets a requirement for HSS to put the public user identities into special order in the Server-Assignment-Answer (SAA) message. The subclause 5.4.1.2.2 (Protected REGISTER) of 24.229 says: "The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF."
Summary of change:	⌘	It is proposed a clarification to the implicit registration, that the first non-barred public user identity, which has the syntax of SIP URI, in the list of public identities downloaded to S-CSCF indicates the default public user identity.
Consequences if not approved:	⌘	Misalignment with TS 24.229

Clauses affected:	⌘	6.5.1.1

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

-------- First modified section---------

6.5 Implicit registration

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

What follows is an extension of the affected basic procedures.

6.5.1 S-CSCF initiated procedures

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

6.5.1.1 Registration

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

6.5.1.2 De-registration

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

6.5.1.3 Authentication

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

6.5.2 HSS initiated procedures

6.5.2.1 (void)

6.5.2.2 De-registration

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

3GPP TSG CN WG4 Meeting #18 **N4-030246**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **033** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Replacement of the NAS-Session-Key AVP
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	11/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The newest version of NASREQ Internet Draft (draft-ietf-aaa-diameter-nasreq-10.txt) does not contain anymore a definition of NAS-Session-Key AVP. In order to avoid unstable dependencies to Internet Drafts new 3GPP specific AVPs should be specified for integrity and confidentiality keys to replace the NAS-Session-Key AVP in MAR command.
Summary of change:	⌘	The NAS-Session-Key AVP is proposed to be replaced by new Integrity-Key and Confidentiality-Key AVPs.
Consequences if not approved:	⌘	There is no standard AVP definition for security keys.

Clauses affected:	⌘	6.3, A.3

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		CR 29.229-013
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

-------- First modified section---------

6.3 Authentication procedures

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

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

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

Table 6.3.1: Authentication request

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	M	This information element contains the public identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the user private identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested
Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Tables 6.3.2 and 6.3.3 for the contents of this information element. The content shown in table 6.3.2 shall be used for a normal authentication request; the content shown in table 6.3.3 shall be used for an authentication request after synchronization failure.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name this AVP shall be present. This information is available if the MAR belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent in case of the initial registration. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the client.

Table 6.3.2: Authentication Data content – request

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

Table 6.3.3: Authentication Data content – request, synchronization failure

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of nonce and AUTS, base 64 encoded. S-CSCF shall include the nonce sent to the terminal and the auts directive received from the terminal. See 3GPP TS 33.203 [3] for further details about RAND and AUTS. See [7] for further details about based 64 encoding. One example of content is: 'nonce=" dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 ", auts="5ccc069c403ebaf9f0171e9517f40e41"' where nonce "dcd98b7102dd2f0e8b11d0f600bfb0c093" contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1) and auts "5ccc069c403ebaf9f0171e9517f40e41" contains, base 64 encoded, AUTS.
Routing Information (See 7.13)	Destination-Host	M	In this case the MAR belongs to an already existing registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.

Table 6.3.4: Authentication answer

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

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be included present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, Base 64 encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. One example of the format of the SIP-Authenticate AVP is: 'nonce=" dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 "' where the nonce " dcd98b7102dd2f0e8b11d0f600bfb0c06629fae49393a05397450978507c4ef1 " contains, base 64 encoded, RAND (dcd98b7102dd2f0e8b11d0f600bfb0c0) and AUTN (6629fae49393a05397450978507c4ef1).
Authorization Information (See 7.9.4)	SIP-Authorization	M	~~In~~ It shall contain, base 64 encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES. One example of the format of the SIP-Authorization AVP is: 'response="6629fae49393a05397450978507c4ef1"' where response="6629fae49393a05397450978507c4ef1" contains, base64 encoded, XRES.
Confidentiality Key (See 7.9.5)	~~NAS-Session-Key~~Confidentiality-Key	O	This information element, if present, ~~may~~ shall contain the confidentiality key. It shall be base 64 encoded. ~~NAS-Session-Key is a grouped AVP. When present the following describes its content:~~ ~~-NAS-Key-Direction equal to BIDIRECTIONAL.~~ ~~-NAS-Key-Type equal to CIPHER_KEY.~~ ~~-NAS-Key-Data contains the confidentiality key.~~
Integrity Key (See 7.9.6)	~~NAS-Session-Key~~Integrity-Key	M	This information element shall contain the integrity key. It shall be base 64 encoded. ~~NAS-Session-Key is a grouped AVP. When present the following describes its content:~~ ~~-NAS-Key-Direction equal to BIDIRECTIONAL.~~ ~~-NAS-Key-Type equal to INTEGRITY_KEY.~~ ~~-NAS-Key-Data contains the integrity key.~~

6.3.1 Detailed behaviour

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

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

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

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

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

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

- If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

  - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It will also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

  - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored), the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

  - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It will also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

  - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It will also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it is not registered, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It will also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER_SUCCESS.

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

-------- Second modified section---------

A.3 Cx message parameters to Diameter AVP mapping

The following table gives an overview about the mapping:

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

Cx parameter	AVP Name
Visited Network Identifier	Visited-Network-Identifier
Public User ID	Public-Identity
Private User ID	User-Name
S-CSCF name	Server-Name
S-CSCF capabilities	Server-Capabilities
Result	Result-Code / Vendor-Specific-Result
User profile	User-Data
Server Assignment Type	Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item Number	SIP-Item-Number
Authentication Scheme	SIP-Authentication-Scheme
Authentication Information	SIP-Authenticate
Authorization Information	SIP-Authorization
Confidentiality Key	~~NAS-Session~~Confidentiality-Key
Integrity Key	~~NAS-Session~~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

3GPP TSG CN WG4 Meeting #18 **N4-030247**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **034** ⌘**rev** **2** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Corrections to service profile
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	11/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The cardinalities of the initial Filter Criteria and Service Point of Interest are not correct.
Summary of change:	⌘	It is proposed to have a lower bound of zero (0) for iFC and a lower bound of one (1) for SPI. The inconsistencies between the annex E and the CxDataType.xsd file are corrected.
Consequences if not approved:	⌘	It is not possible to create IMS subscription without iFC and the Cx resources are not used efficiently.

Clauses affected:	⌘	Annex B.2.2, Annex C, Annex E and CxDataType.xsd

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

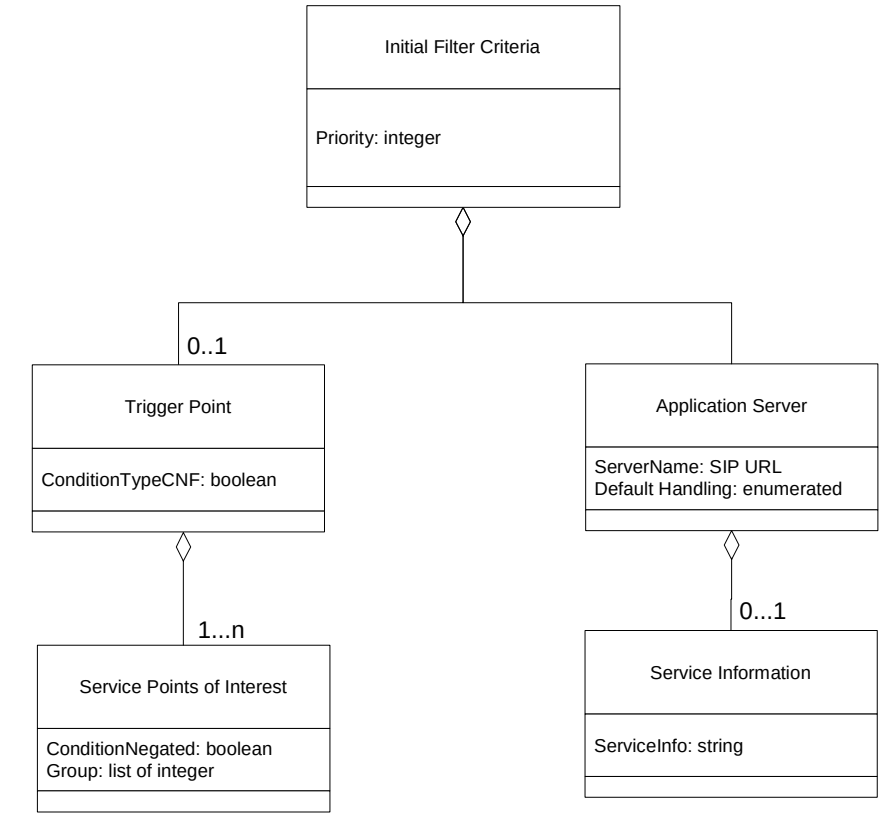
downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

-------- First modified section---------

B.2.2 Initial Filter Criteria

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



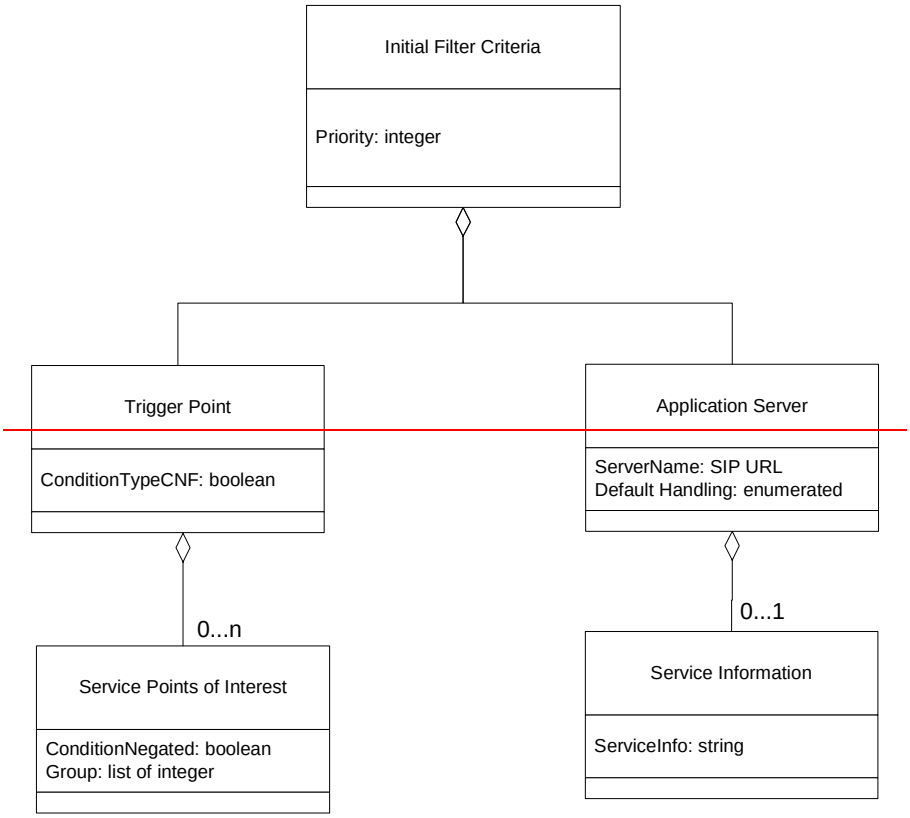


Figure B.2.2.1.1: Initial Filter Criteria

Each instance of the Initial Filter Criteria class is composed of ~~one~~ zero or one instance of a Trigger Point class and one instance of an Application Server class. ~~FilterID identifies the particular instance of the Filter Criteria class.~~ Priority indicates the priority of the Filter Criteria. The higher the Priority Number the lower the priority of the Filter Criteria is;

i.e., a Filter Criteria with a higher value of Priority Number shall be assessed after the Filter Criteria with a smaller Priority Number have been assessed. The same priority shall not be assigned to more than one ~~As~~initial Filter Criterion. ConditionTypeCNF is a boolean that is TRUE when the Trigger Point associated with the FilterCriteria is a boolean expresion in Conjuctive Normal Form (CNF) and FALSE if the Trigger Point is expressed in Disjunctive Normal Form (DNF) (see Annex C).

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

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

Each Trigger Point is composed by ~~0~~ 1 to n instances of the class Service Points of Interest.

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

The Application Server class contains zero or one instance of the Service Information class. Service Information class allows to download to S-CSCF information that is to be transferred transparently to an Application Server when the trigger points of a filter criterion are satisfied. ServiceInformation is a string conveying that information. See 3GPP TS 23.218 [7] for a description of the use of this information element.

-------- Second modified section---------

Annex C (informative): Conjunctive and Disjunctive Normal Form

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

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

Taking as an example the following trigger:

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

The trigger can be split into the following atomic expressions:

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

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

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

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

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

The XML representation of the trigger is:

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

                      <SPI>
                          <ConditionNegated>1</ConditionNegated>
                          <Group>1</Group>
                          <SIPHeader>
                              <Header>From</Header>
                              <Content>”joe”</Content>
                          </SIPHeader>
                      </SPI>
                  </TriggerPoint>
                  <ApplicationServer>
```

```
                    <ServerName>sip:AS1@homedomain.com</ServerName>
                    <DefaultHandling>0</DefaultHandling>
                </ApplicationServer>
            </InitialFilterCriteria>
        </ServiceProfile>
    </IMSSubscription>
</testDatatype>
```

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

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

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

The XML representation of the trigger is:

```
<?xml version=”1.0” encoding=”UTF-8”?>
<testDatatype xmlns:xsi=”http://www.w3.org/2001/XMLSchema-instance” xsi:noNamespaceSchemaLocation=”D:\
CxDataType.xsd”>
    <IMSSubscription>
      <PrivateID>IMPI1@homedomain.com</PrivateID>
      <ServiceProfile>
        <PublicIdentity>
          <BarringIndication>1</BarringIndication>
          <Identity> sip:IMPU1@homedomain.com </Identity>
        </PublicIdentity>
        <PublicIdentity>
          <Identity> sip:IMPU2@homedomain.com </Identity>
        </PublicIdentity>”””””
        <InitialFilterCriteria>
”””         <Priority>0</Priority>
          <TriggerPoint>
            <ConditionTypeCNF>0</ConditionTypeCNF>
            <SPI>
              <ConditionNegated>0</ConditionNegated>
              <Group>0</Group>
              <Method>INVITE</Method>
            </SPI>
            <SPI>
              <ConditionNegated>0</ConditionNegated>
              <Group>1</Group>
              <Method>MESSAGE</Method>
            </SPI>
            <SPI>
              <ConditionNegated>0</ConditionNegated>
              <Group>2</Group>
              <Method>SUBSCRIBE</Method>
            </SPI>
            <SPI>
              <ConditionNegated>1</ConditionNegated>
              <Group>2</Group>
              <SIPHeader>
                <Header>From</Header>
                <Content>”joe”</Content>
              </SIPHeader>
            </SPI>
          </TriggerPoint>
          <ApplicationServer>
            <ServerName>sip:AS1@homedomain.com</ServerName>
```

```
                    <DefaultHandling index=”0">0</DefaultHandling>
                </ApplicationServer>
            </InitialFilterCriteria>
        </ServiceProfile>
    </IMSSubscription>
</testDatatype>
```

-------- Third modified section---------

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

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

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

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

Data type	Tag	Base type	Comments
~~T~~tPriority	Priority	Integer	>= 0
~~T~~gtGroupID	Group	Integer	>= 0
~~T~~dtDefaultHandling	DefaultHandling	enumerated	Possible values: 0 (SESSION_CONTINUED) 1 (SESSION_TERMINATED)
tDirectionOfRequest	SessionCase	enumerated	Possible values: 0 (ORIGINATING_SESSION) 1 TERMINATING_SESSION 2 (TERMINATING_UNREGISTERED)
~~T~~ptPrivateID	PrivateID	anyURI	Syntax described in RFC 2486
tSIP_URL	~~Public~~Identity	anyURI	Syntax described in RFC 3261
tTEL_URL	~~Public~~Identity	anyURI	Syntax described in RFC 2806
~~Tpublic~~tIdentity	~~Public~~Identity	(union)	Union of tSIP_URL and tTEL_URL
~~T~~stServiceInfo	ServiceInfo	string	
~~T~~stString	RequestURI, Method, Header, Content, Line	string	
~~T~~btBool	ConditionTypeCNF, ConditionNegated, BarringIndication	boolean	Possible values: 0 (false) 1 (true)

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

Data type	Tag	Compound of		
		Tag	Type	Cardinality
~~T~~tIMSSubscription	IMSSubscription	PrivateID	tPrivateID	1
		ServiceProfile	tServiceProfile	(1 to n)
~~T~~stServiceProfile	ServiceProfile	PublicIdentity	tPublicIdentity	(1 to n)
		InitialFilterCriteria	tInitialFilterCriteria	(~~1~~ 0 to n)
tPublicIdentity	PublicIdentity	BarringIndication	tBool	1
		Identity	tIdentity	1
t~~T~~InitialFilterCriteria	InitialFilterCriteria	Priority	~~T~~tPriority	1
		TriggerPoint	~~T~~tTrigger	(0 to 1)
		ApplicationServer	tApplicationServer	1
~~T~~tTrigger	TriggerPoint	ConditionTypeCNF	tBool	1
		SPI	~~T~~tSiPoInt	(~~0~~ 1 to n)
~~T~~stSiPoInt	SPI	ConditionNegated	~~T~~tBool	(0 to 1)
		Group	~~T~~tGroupID	(1 to n)
		Choice of: RequestURI	~~T~~tString	1
		Choice of: Method	~~T~~tString	1
		Choice of: SIPHeader	~~T~~tHeader	1
		Choice of: SessionCase	tDirectionOfRequest	1
		Choice of: SessionDescription	tSessionDescription	1
~~T~~htHeader	SIPHeader	Header	~~T~~tString	1
		Content	~~T~~tString	(0 to 1)
~~T~~tSessionDescriptio	SessionDescription	Line	~~T~~tString	1

n		Content	~~T~~tString	(0 to 1)
~~T~~tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	(0 to 1)
		ServiceInfo	~~T~~tServiceInfo	(0 to 1)
NOTE: “n” shall be interpreted as non-bounded.				

-------- Fifth modified section---------

(The attached CxDataType.xsd file)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:simpleType name="tPriority" final="list restriction">
    <xs:restriction base="xs:int">
      <xs:minInclusive value="0"/>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="tGroupID" final="list restriction">
    <xs:restriction base="xs:int">
      <xs:minInclusive value="0"/>
    </xs:restriction>
  </xs:simpleType>
    <xs:simpleType name="tDefaultHandling" final="list restriction">
    <xs:restriction base="xs:unsignedByte">
      <xs:maxInclusive value="1"/>
      <xs:enumeration value="0">
        <xs:annotation>
          <xs:documentation>
            <label xml:lang="en">SESSION_CONTINUED</label>
            <definition xml:lang="en">Session Continued</definition>
          </xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="1">
        <xs:annotation>
          <xs:documentation>
            <label xml:lang="en">SESSION_TERMINATED</label>
            <definition xml:lang="en">Session Terminated</definition>
          </xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="tDirectionOfRequest" final="list restriction">
    <xs:restriction base="xs:unsignedByte">
      <xs:maxInclusive value="3"/>
      <xs:enumeration value="0">
        <xs:annotation>
          <xs:documentation>
            <label xml:lang="en">ORIGINATING_SESSION</label>
            <definition xml:lang="en">Originating Session</definition>
          </xs:documentation>
```

```
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="1">
          <xs:annotation>
            <xs:documentation>
              <label xml:lang="en">TERMINATING_SESSION</label>
              <definition xml:lang="en">Terminating Session</definition>
            </xs:documentation>
          </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="2">
          <xs:annotation>
            <xs:documentation>
              <label xml:lang="en">TERMINATING_UNREGISTERED</label>
              <definition xml:lang="en">Terminating Session for unregistered
user</definition>
            </xs:documentation>
          </xs:annotation>
        </xs:enumeration>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tPrivateID" final="list restriction">
      <xs:restriction base="xs:anyURI"/> </xs:simpleType>
    <xs:simpleType name="tSIP_URL" final="list restriction">
      <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="tTEL_URL" final="list restriction">
      <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="tIdentity" final="list restriction">
      <xs:union memberTypes="tSIP_URL tTEL_URL"/>
    </xs:simpleType>
    <xs:simpleType name="tServiceInfo" final="list restriction">
      <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tString" final="list restriction">
      <xs:restriction base="xs:string">
        <xs:minLength value="0"/>
      </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tBool">
      <xs:restriction base="xs:boolean">
      </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tIMSSubscription">
      <xs:sequence>
        <xs:element name="PrivateID" type="tPrivateID"/>
        <xs:element name="ServiceProfile" type="tServiceProfile"
maxOccurs="unbounded"/>
        <xs:any namespace="##Other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tServiceProfile">
      <xs:sequence>
        <xs:element name="PublicIdentity" type="tPublicIdentity"
      maxOccurs="unbounded"/>
        <xs:element name="InitialFilterCriteria" type="tInitialFilterCriteria"
minOccurs="0" maxOccurs="unbounded"/>
        <xs:any namespace="##Other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
```

```
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tInitialFilterCriteria">
    <xs:sequence>
      <xs:element name="Priority" type="tPriority"/>
      <xs:element name="TriggerPoint" type="tTrigger" minOccurs="0"/>
      <xs:element name="ApplicationServer" type="tApplicationServer"/>
      <xs:any namespace="##Other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tTrigger">
    <xs:sequence>
      <xs:element name="ConditionTypeCNF" type="tBool"/>
      <xs:element name="SPI" type="tSiPoInt" minOccurs="0"
maxOccurs="unbounded"/>
      <xs:any namespace="##Other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tSiPoInt">
    <xs:sequence>
      <xs:element name="ConditionNegated" type="tBool" default="0"
minOccurs="0"/>
      <xs:element name="Group" type="tGroupID" maxOccurs="unbounded"/>
      <xs:any namespace="##Other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
      <xs:choice>
        <xs:element name="RequestURI" type="tString"/>
        <xs:element name="Method" type="tString"/>
        <xs:element name="SIPHeader" type="tHeader"/>
        <xs:element name="SessionCase" type="tDirectionOfRequest"/>
        <xs:element name="SessionDescription" type="tSessionDescription"/>
      </xs:choice>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tHeader">
    <xs:sequence>
      <xs:element name="Header" type="tString"/>
      <xs:element name="Content" type="tString" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tSessionDescription">
    <xs:sequence>
      <xs:element name="Line" type="tString"/>
      <xs:element name="Content" type="tString" minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tApplicationServer">
    <xs:sequence>
      <xs:element name="ServerName" type="tSIP_URL"/>
      <xs:element name="DefaultHandling" type="tDefaultHandling"
minOccurs="0"/>
      <xs:element name="ServiceInfo" type="tServiceInfo" minOccurs="0"/>
      <xs:any namespace="##Other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
  <xs:complexType name="tPublicIdentity">
    <xs:sequence>
      <xs:element name="BarringIndication" type="tBool" default="0"
minOccurs="0"/>
      <xs:element name="Identity" type="tIdentity"/>
```

```
    </xs:sequence>
  </xs:complexType>
  <xs:element name="IMSSubscription" type="tIMSSubscription"/>
</xs:schema>
```

3GPP TSG CN WG4 Meeting #18 **N4-030312**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **035** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification on Re-allocation of S-CSCF
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	12/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	There is an ambiguity concerning the behaviour of the I-CSCF receiving the result DIAMETER_SUBSEQUENT_REGISTRATION in response of User Registration Status Query. The same result is given by the HSS for the cases "registered user" and "unregistered user" that forces the I-CSCF to check the presence of S-CSCF capabilities in the response before determining the need of S-CSCF selection.
Summary of change:	⌘	It is proposed to implement "DIAMETER_SERVER_SELECTION" as a new Vendor-Specific-Result, in order to distinguish the case in which the selection of a new S-CSCF is required for a unregistered user.
Consequences if not approved:	⌘	The I-CSCF would not be able to determine its action on the sole result DIAMETER_SUBSEQUENT_REGISTRATION.

Clauses affected:	⌘	6.1.1.1			
Other specs affected:	⌘	Y: X / N:	Other core specifications	⌘	29.229-015r1
		Y: / N: X	Test specifications		
		Y: / N: X	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

6.1.1.1 Detailed behaviour

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

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

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

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

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

     - If so, continue to step 4.

     - If not, Vendor-Specific-Result shall be set to DIAMETER_AUTHORIZATION_REJECTED.

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

   - If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not Vendor-Specific-Result shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). Continue to step 5.

   - If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.

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

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

   - If it is registered , the HSS shall return the stored S-CSCF name and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

   - If it is unregistered (i.e registered as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored), ~~the HSS shall return the stored S-CSCF name and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION.~~then:

     - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

     - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Vendor-Specific-Result set to DIAMETER_SERVER_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.

   - If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:

     - If the value of User-Authorization-Type is equal to DE_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Vendor-Specific-Result to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.

- If the value of User-Authorization-Type is different from DE_REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
  - If there is at least one identity of the user that is registered, the HSS shall return the S-CSCF name assigned for the user and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
  - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored), ~~the HSS shall return the stored S-CSCF name and Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION.~~ then:
    - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Vendor-Specific-Result set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
    - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Vendor-Specific-Result set to DIAMETER_SERVER_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
  - If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the list of S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The returned S-CSCF capabilities shall satisfy the most restrictive service profile of the user. The list of S-CSCF capabilities may be empty, to indicate to the I-CSCF that it may select any available S-CSCF. Vendor-Specific-Result shall be set to DIAMETER_FIRST_REGISTRATION. The HSS shall not return any S-CSCF name.

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

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030314**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **037** ⌘ **rev** **3** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Handling of non supported data in the S-CSCF when the profile is being updated.
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	When the S-CSCF receives the updated profile from the HSS and some of these data are not understood by the S-CSCF, currently the serving is updating his profile and sending the DIAMETER_SUCCESS_NOT_SUPPORTED_DATA notification back to the HSS. However, data should not be updated when they are not understood since this situation could end up in an incoherent data storing.
Summary of change:	⌘	Clarify that the S-CSCF will overwrite the profile from the HSS only when data are supported or recognised.
Consequences if not approved:	⌘	Incoherent data storing.

Clauses affected:	⌘	Table 6.2.2.1.1

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	29.229-018
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

6.2.2.1 Detailed behaviour

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

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

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

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

Table 6.2.2.1.1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_~~SUCCESS~~ERROR_NOT SUPPORTED_USER_DATA	The request ~~succeeded~~failed. ~~However,~~T ~~t~~he 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.~~interpretation requires capabilities which the S-CSCF does not support~~.
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.

End of modified section

3GPP TSG-CN4 Meeting #18
Dublin, Ireland, 10-14 February, 2003

Tdoc N4-030261

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **038** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Change of SPI to SPT
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	31/1/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	At the last CN#17 plenary in September, CR against 23.218 (CN1) regarding change of SPI to SPT was agreed, but corresponding CR against 29.228 and 29.328 was left out without change about 4 months. This CR against 29.228 is submitted for alignment with 23.218.
Summary of change:	⌘	SPI (Service Points of Interest) is replaced with SPT(Service Point Trigger) for the purpose of alignment with 23.218.
Consequences if not approved:	⌘	The misalignment still remains between 23.218 and 29.228/29.328.
Clauses affected:	⌘	B2.2, B2.3, Annex C, Annex E

Other specs affected:	Y	N		⌘	
	X		Other core specifications	⌘	29.328-019
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	The corresponding CR(N4-030268) against 29.328 and is affected each other.

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

----------Start of Change----------

Annex B (informative): User profile UML model

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

B.1 General description

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

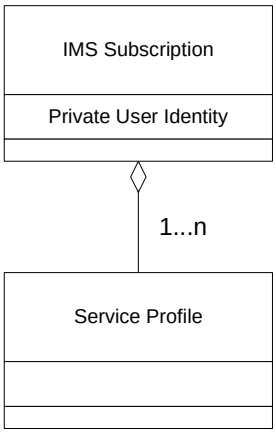


Figure B.1.1: User Profile

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

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

B.2 Service profile

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

:

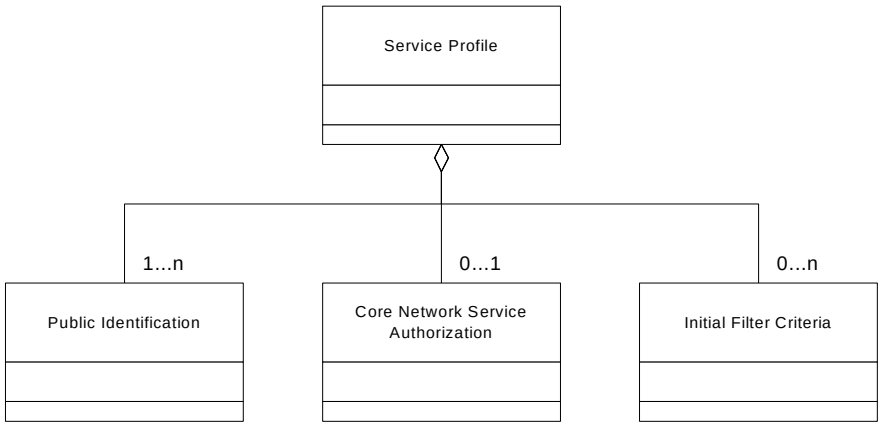


Figure B.2.1: Service Profile

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

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

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

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

B.2.1 Public Identification

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

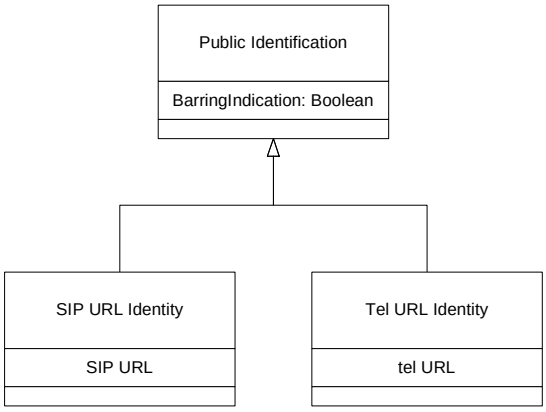


Figure B.2.1.1: Public Identification

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

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

B.2.2 Initial Filter Criteria

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

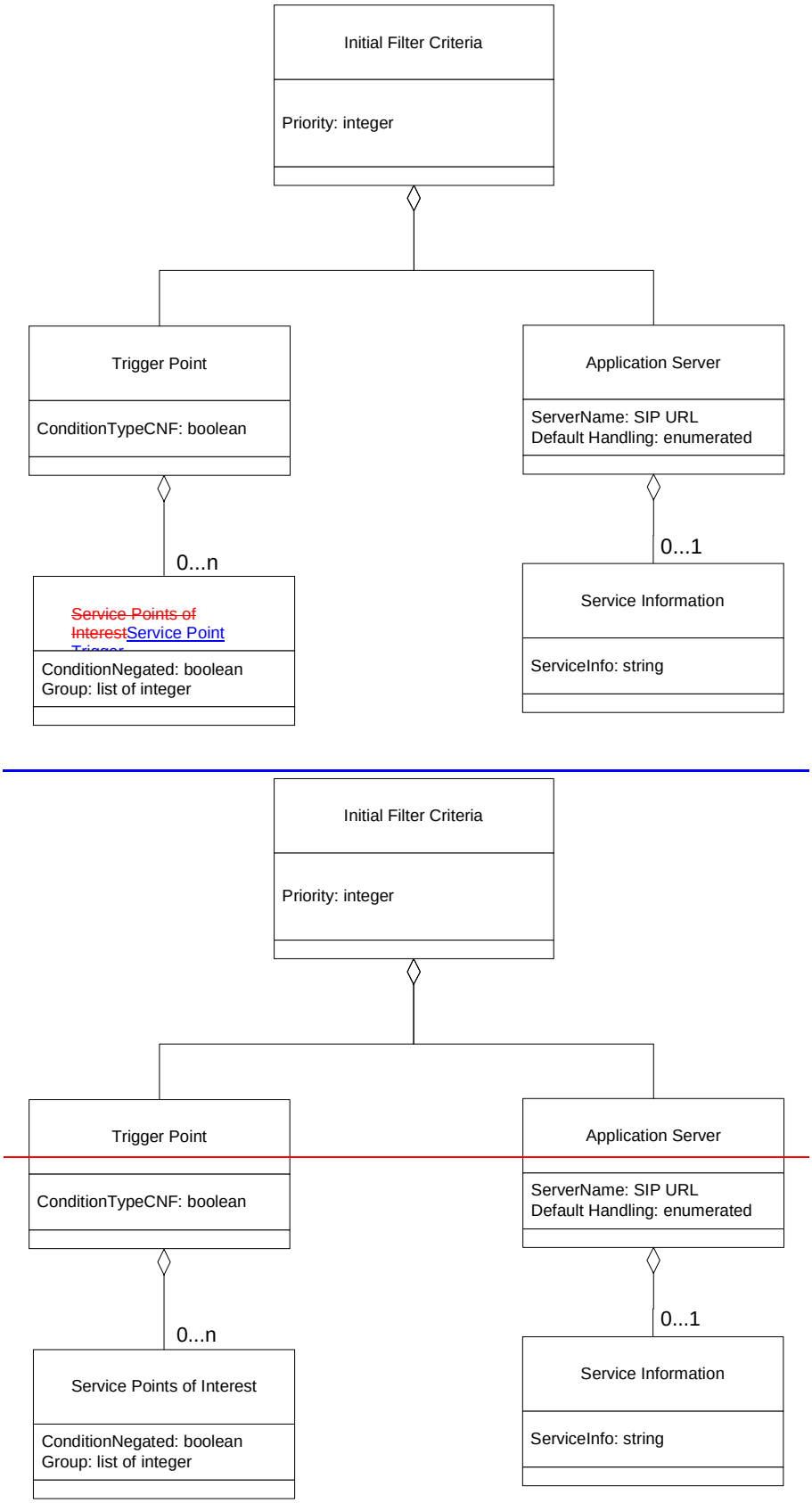


Figure B.2.2.1.1: Initial Filter Criteria

Each instance of the Initial Filter Criteria class is composed of one instance of a Trigger Point class and one instance of an Application Server class. FilterID identifies the particular instance of the Filter Criteria class. Priority indicates the

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

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

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

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

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

The Application Server class contains zero or one instance of the Service Information class. Service Information class allows to download to S-CSCF information that is to be transferred transparently to an Application Server when the trigger points of a filter criterion are satisfied. ServiceInformation is a string conveying that information. See 3GPP TS 23.218 [7] for a description of the use of this information element.

B.2.3 ~~Trigger Point~~Service Point Trigger

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

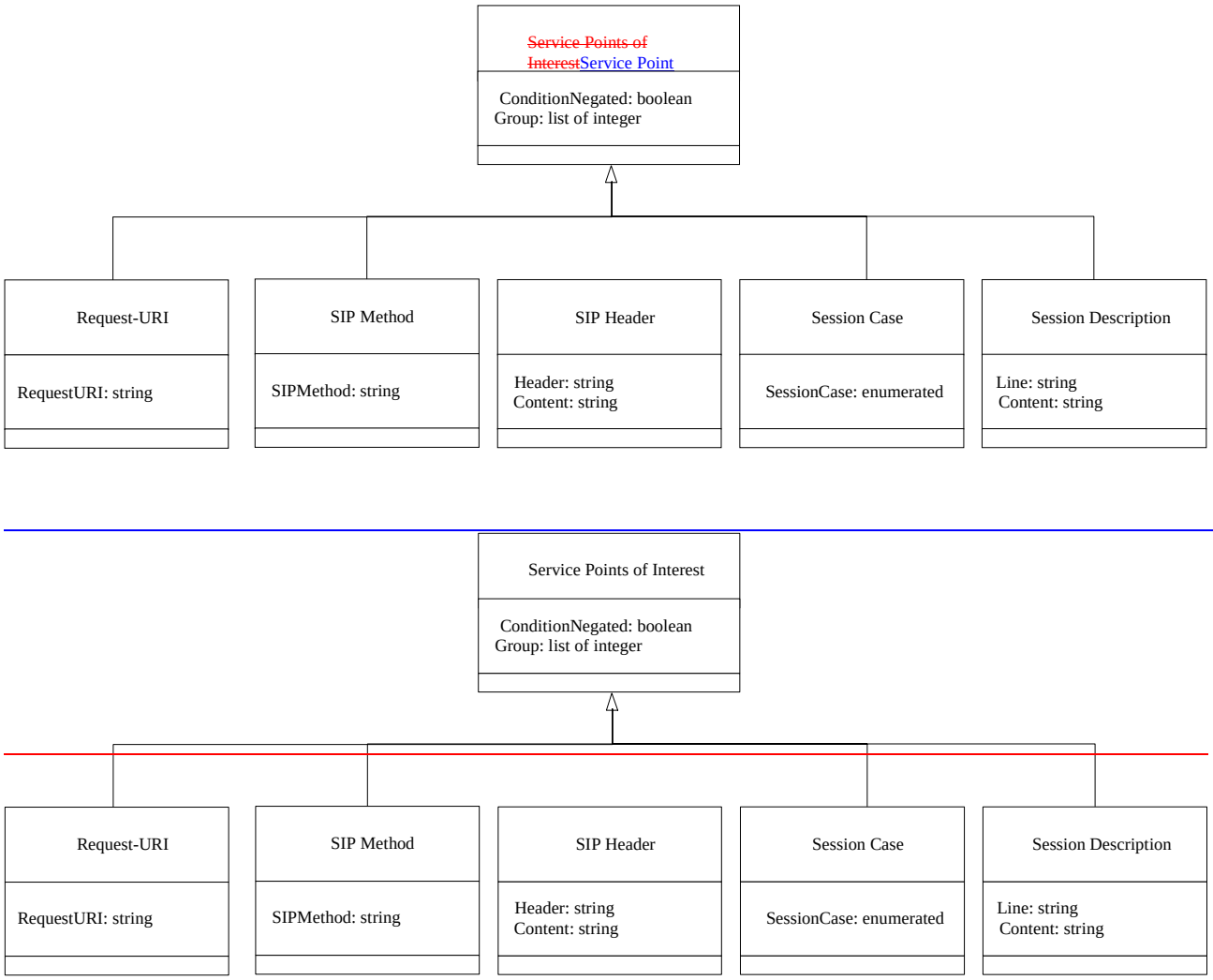


Figure B.2.3.1: Trigger Point

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

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

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

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

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

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

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

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

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

(1 ".*Jo.*": meaning that a given header contains the sub string "Jo" at any position.

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

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

Session Description Information class defines ~~SPI~~SPT for the content of any SDP field within the body of a SIP Method. The Line attribute identifies the line inside the session description. Content is a string defining the content of the line identified by Line. Perl-like regular expressions shall be taken as a model for regular expressions for this function (as described above).

Annex C (informative): Conjunctive and Disjunctive Normal Form

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

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

Taking as an example the following trigger:

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

The trigger can be split into the following atomic expressions:

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

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

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

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

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

The XML representation of the trigger is:

```
<?xml version=”1.0” encoding=”UTF-8”?>

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

        <IMSSubscription>

          <PrivateID>IMPI1@homedomain.com</PrivateID>

          <ServiceProfile>

              <PublicIdentity>

                  <BarringIndication>1</BarringIndication>

                  <Identity> sip:IMPU1@homedomain.com </Identity>
```

```
                </PublicIdentity>
                <PublicIdentity>
                    <Identity> sip:IMPU2@homedomain.com </Identity>
                </PublicIdentity>
”””””           <InitialFilterCriteria>
””              <Priority>0</Priority>
                <TriggerPoint>
                    <ConditionTypeCNF>1</ConditionTypeCNF>
                    <SPISPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>INVITE</Method>
                    </SPISPT>
                    <SPISPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>MESSAGE</Method>
                    </SPISPT>
                    <SPISPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>SUBSCRIBE</Method>
                    </SPISPT>
                    <SPISPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>1</Group>
                        <Method>INVITE</Method>
                    </SPISPT>
                    <SPISPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>1</Group>
                        <Method>MESSAGE</Method>
                    </SPISPT>

                    <SPISPT>
```

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

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

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

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

The XML representation of the trigger is:

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

```
            </PublicIdentity>
            <PublicIdentity>
                <Identity> sip:IMPU2@homedomain.com </Identity>
            </PublicIdentity>”””””
            <InitialFilterCriteria>
”””             <Priority>0</Priority>
                <TriggerPoint>
                    <ConditionTypeCNF>0</ConditionTypeCNF>
                    <~~SPI~~SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>0</Group>
                        <Method>INVITE</Method>
                    </~~SPI~~SPT>
                    <~~SPI~~SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>1</Group>
                        <Method>MESSAGE</Method>
                    </~~SPI~~SPT>
                    <~~SPI~~SPT>
                        <ConditionNegated>0</ConditionNegated>
                        <Group>2</Group>
                        <Method>SUBSCRIBE</Method>
                    </~~SPI~~SPT>
                    <~~SPI~~SPT>
                        <ConditionNegated>1</ConditionNegated>
                        <Group>2</Group>
                        <SIPHeader>
                            <Header>From</Header>
                            <Content>”joe”</Content>
                        </SIPHeader>
                    </~~SPI~~SPT>
                </TriggerPoint>
                <ApplicationServer>
                    <ServerName>sip:AS1@homedomain.com</ServerName>
                    <DefaultHandling index=”0">0</DefaultHandling>
```

```
                    </ApplicationServer>
                </InitialFilterCriteria>
            </ServiceProfile>
        </IMSSubscription>
</testDatatype>
```

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

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

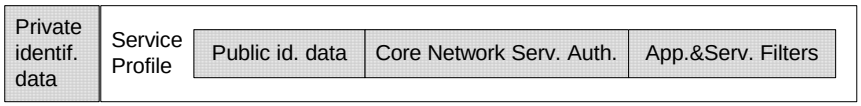


Figure C.1: Example of in-line format of user profile

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

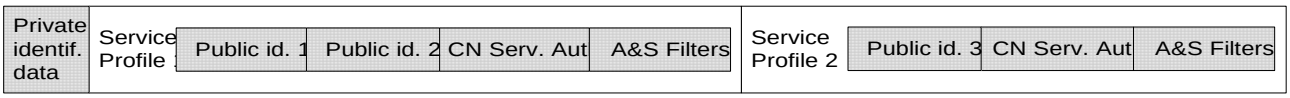


Figure C.2: Example of in-line format of user profile

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

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

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

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

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

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

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

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

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

The file CxDataTypes.xsd, attached to this specification, contains the XML schema with the data description for Cx interface.

----------End of Change----------

```
<?xml version="1.0" encoding="UTF-8"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified">

    <xs:simpleType name="tPriority" final="list restriction">

        <xs:restriction base="xs:int">

            <xs:minInclusive value="0"/>

        </xs:restriction>

    </xs:simpleType>

    <xs:simpleType name="tGroupID" final="list restriction">

        <xs:restriction base="xs:int">

            <xs:minInclusive value="0"/>

        </xs:restriction>

    </xs:simpleType>

    <xs:simpleType name="tDefaultHandling" final="list restriction">

        <xs:restriction base="xs:unsignedByte">

            <xs:maxInclusive value="1"/>

            <xs:enumeration value="0">

                <xs:annotation>

                    <xs:documentation>

                        <label xml:lang="en">SESSION_CONTINUED</label>

                        <definition xml:lang="en">Session Continued</definition>

                    </xs:documentation>

                </xs:annotation>

            </xs:enumeration>

            <xs:enumeration value="1">

                <xs:annotation>

                    <xs:documentation>

                        <label xml:lang="en">SESSION_TERMINATED</label>

                        <definition xml:lang="en">Session Terminated</definition>

                    </xs:documentation>

                </xs:annotation>

            </xs:enumeration>

        </xs:restriction>

    </xs:simpleType>

    <xs:simpleType name="tDirectionOfRequest" final="list restriction">
```

```
    <xs:restriction base="xs:unsignedByte">
        <xs:maxInclusive value="3"/>
        <xs:enumeration value="0">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">ORIGINATING_SESSION</label>
                    <definition xml:lang="en">Originating Session</definition>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="1">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">TERMINATING_SESSION</label>
                    <definition xml:lang="en">Terminating Session</definition>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
        <xs:enumeration value="2">
            <xs:annotation>
                <xs:documentation>
                    <label xml:lang="en">TERMINATING_UNREGISTERED</label>
                    <definition xml:lang="en">Terminating Session for unregistered user</definition>
                </xs:documentation>
            </xs:annotation>
        </xs:enumeration>
    </xs:restriction>
</xs:simpleType>
<xs:simpleType name="tPrivateID" final="list restriction">
    <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="tSIP_URL" final="list restriction">
    <xs:restriction base="xs:anyURI"/>
</xs:simpleType>
<xs:simpleType name="tTEL_URL" final="list restriction">
```

```
        <xs:restriction base="xs:anyURI"/>
    </xs:simpleType>
    <xs:simpleType name="tIdentity" final="list restriction">
        <xs:union memberTypes="tSIP_URL tTEL_URL"/>
    </xs:simpleType>
    <xs:simpleType name="tServiceInfo" final="list restriction">
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tString" final="list restriction">
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="tBool">
        <xs:restriction base="xs:boolean"/>
    </xs:simpleType>
    <xs:simpleType name="tSubscribedMediaProfileId" final="list restriction">
        <xs:restriction base="xs:int">
            <xs:minInclusive value="0"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:complexType name="tIMSSubscription">
        <xs:sequence>
            <xs:element name="PrivateID" type="tPrivateID"/>
            <xs:element name="ServiceProfile" type="tServiceProfile" maxOccurs="unbounded"/>
            <xs:any namespace="##Other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tServiceProfile">
        <xs:sequence>
            <xs:element name="PublicIdentity" type="tPublicIdentity" maxOccurs="unbounded"/>
            <xs:element name="CoreNetworkServicesAuthorization" type="tCoreNetworkServicesAuthorization"
minOccurs="0" maxOccurs="1"/>
```

```
            <xs:element name="InitialFilterCriteria" type="tInitialFilterCriteria" maxOccurs="unbounded"/>
            <xs:any namespace="##Other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tCoreNetworkServicesAuthorization">
        <xs:sequence>
            <xs:element name="SubscribedMediaProfileId" type="tSubscribedMediaProfileId" minOccurs="0"/>
            <xs:any namespace="##Other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tInitialFilterCriteria">
        <xs:sequence>
            <xs:element name="Priority" type="tPriority"/>
            <xs:element name="TriggerPoint" type="tTrigger" minOccurs="0"/>
            <xs:element name="ApplicationServer" type="tApplicationServer"/>
            <xs:any namespace="##Other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tTrigger">
        <xs:sequence>
            <xs:element name="ConditionTypeCNF" type="tBool"/>
            <xs:element name="SPI" type="tSiPoInt" minOccurs="0" maxOccurs="unbounded"/>
            <xs:any namespace="##Other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="tSiPoInt">
        <xs:sequence>
            <xs:element name="ConditionNegated" type="tBool" default="0" minOccurs="0"/>
            <xs:element name="Group" type="tGroupID" maxOccurs="unbounded"/>
            <xs:any namespace="##Other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
            <xs:choice>
                <xs:element name="RequestURI" type="tString"/>
                <xs:element name="Method" type="tString"/>
                <xs:element name="SIPHeader" type="tHeader"/>
                <xs:element name="SessionCase" type="tDirectionOfRequest"/>
```

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

3GPP TSG CN WG4 Meeting #18 **N4-030252**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **040** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Definition of the Subscribed Media Profile Identifier
Source:	⌘	CN4
Work item code:	⌘	IMS
Date:	⌘	12/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	To clearify the handling of subscribed media
Summary of change:	⌘	Information on subscribed media is downloaded from HSS to S-CSCF. The information on subscribed media is provided in the form of a profile identifier; details of the allowed media parameters associated with the profile identifier are configured in the S-CSCF.
Consequences if not approved:	⌘	Handling of subscribed media remains unclear

Clauses affected:	⌘	B2, Annex E

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	CR 23.008-067
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

B.1 General description

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

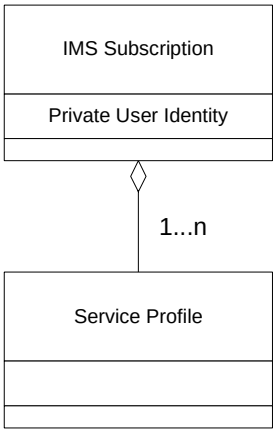


Figure B.1.1: User Profile

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

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

B.2 Service profile

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

:

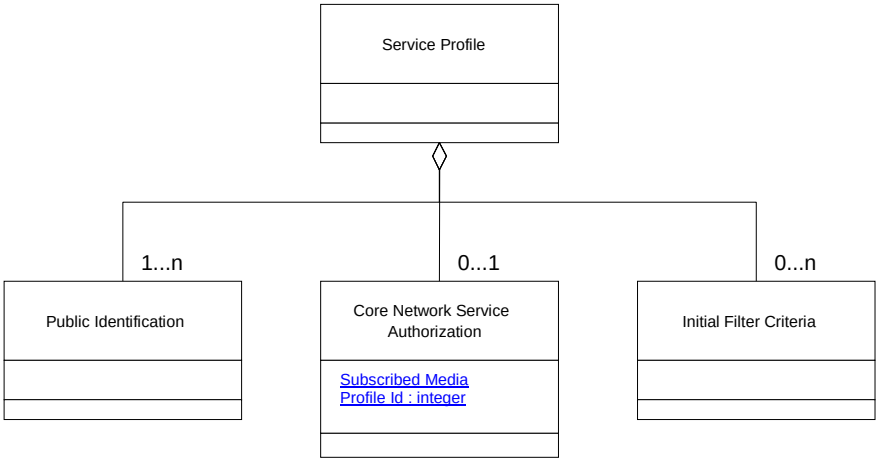


Figure B.2.1: Service Profile

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

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

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

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

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

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

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

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

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

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)
		~~SubscribedMediaProfileID~~CoreNetworkServicesAuthorization	t~~SubscribedMediaProfileID~~CoreNetworkServicesAuthorization	(0 to 1)
tCoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	SubscribedMediaProfileId	tSubscribedMediaProfileId	(0 to 1)
tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1
		TriggerPoint	tTrigger	(0 to 1)
		ApplicationServer	tApplicationServer	1
tTrigger	Trigger	SPI	tSiPoInt	(0 to n)
		ConditionTypeCNF	tBool	1
tSiPoInt	SPI	ConditionNegated	tBool	(0 to 1)
		Group	tGroupID	(1 to n)
		Choice of: RequestURI	tString	1
		Choice of: Method	tString	1
		Choice of: SIPHeader	tHeader	1
		Choice of: SessionCase	tDirectionOfRequest	1
		Choice of: SessionDescription	tSessionDescription	1
tHeader	SIPHeader	Header	tString	1
		Content	tString	(0 to 1)
tSessionDescription	SessionDescription	Line	tString	1
		Content	tString	(0 to 1)

tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	(0 to 1)
		ServiceInfo	tServiceInfo	(0 to 1)
NOTE: “n” shall be interpreted as non-bounded.				

3GPP TSG CN WG4 Meeting #18 **N4-030244**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.229** **CR** **012** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Update TS 29.229 after Diameter has become RFC
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	15/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Alignment with IETF Diameter Base Protocol
Summary of change:	⌘	Modifications according to the new command code and AVP headers format. Alignment with the new Experimental-Result AVP. Command Codes by IANA inserted.
Consequences if not approved:	⌘	Misalignment with the Diameter standard protocol

Clauses affected:	⌘	2, 3.1, 5.6, 6, 6.1, 6.4

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

2 References

The following documents contain provisions, which through reference in this text constitute provisions of the present document.

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

[1] 3GPP TS 29.228 “IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents (Release 5)”

[2] 3GPP TS 33.210 “3G Security; Network Domain Security; IP Network Layer Security (Release 5)”

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

[4] IETF RFC 2396: “Uniform Resource Identifiers (URI): generic syntax”

[5] IETF RFC 2960 “Stream Control Transmission Protocol”

[6] draft-ietf-aaa-diameter-~~10~~17~~.txt~~, “Diameter Base Protocol”, work in progress

[7] IETF RFC 2234 “Augmented BNF for syntax specifications”

[8] IETF RFC 2806 “URLs for Telephone Calls”

[9] draft ietf-aaa-diameter-nasreq-09.txt, “Diameter NASREQ Extensions”, work in progress

[10] IETF RFC 3309: “SCTP Checksum Change”

[11] 3GPP TS 29.329 “Sh Interface based on the Diameter protocol; protocol details”

[12] draft-loughney-aaa-cc-3gpp-01, “Diameter Command Codes for 3GPP Release 5”

3 Definitions, symbols and abbreviations

3.1 Definitions

Refer to [6] for the definitions of some terms used in this document.

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

Attribute-Value Pair: see [6], it corresponds to an Information Element in a Diameter message.

Diameter Multimedia client: a client that implements the Diameter Multimedia application. The client is one of the communicating Diameter peers that usually initiate transactions. Examples in 3GPP are the I-CSCF and S-CSCF.

Diameter Multimedia server: a server that implements the Diameter Multimedia application. A Diameter Multimedia server that also supported the NASREQ and MobileIP applications would be referred to as a Diameter server. An example of a Diameter Multimedia server in 3GPP is the HSS.

Registration: SIP-registration.

Server: SIP-server.

User data: user profile data.

End of modified section

Beginning of modified section

5.6 Advertising Application Support

The HSS, S-CSCF and I-CSCF shall advertise support of the Diameter Multimedia Application by including the value of 3GPP (10415) in the Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands, and by including the value of 3GPP (10415) in the Vendor-Id AVP and the value of the application identifier (see chapter 6) in the Auth-Application-Id AVP, both in the Vendor-Specific-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands.

6 Diameter application for Cx interface

This clause specifies a Diameter application that allows a Diameter Multimedia server and a Diameter Multimedia client:

- to exchange location information
- to authorize a user to access the IMS
- to exchange authentication information
- to download and handle changes in the user data stored in the server

The Cx interface protocol is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (-http://www.iana.org/assignments/enterprise-numbers) is 10415.

The Diameter application identifier assigned to the Cx/Dx interface application ~~protocol~~ is ~~number 1~~ TBD (pending of allocation by IANA).

6.1 Command-Code values

This section defines Command-Code values for this Diameter application.

Every command is defined by means of the ABNF syntax [7], according to the rules in [6]. Whenever the definition and use of an AVP is not specified in this document, what is stated in [6] shall apply.

The command codes for the Cx/Dx interface application are taken from the range allocated by IANA in [12] as assigned in this specification. For these commands, the Application-ID field shall be set to TBD (application identifier of the Cx/Dx interface application, pending of allocation by IANA).

The following Command Codes are defined in this specification:

Table 6.1.1: Command-Code values

Command-Name	Abbreviation	Code	Section
User-Authorization-Request	UAR	~~1~~300	6.1.1
User-Authorization-Answer	UAA	~~1~~300	6.1.2
Server-Assignment-Request	SAR	~~2~~301	6.1.3

Server-Assignment-Answer	SAA	~~2~~301	6.1.4
Location-Info-Request	LIR	~~3~~302	6.1.5
Location-Info-Answer	LIA	~~3~~302	6.1.6
Multimedia-Auth-Request	MAR	~~4~~303	6.1.7
Multimedia-Auth-Answer	MAA	~~4~~303	6.1.8
Registration-Termination-Request	RTR	~~5~~304	6.1.9
Registration-Termination-Answer	RTA	~~5~~304	6.1.10
Push-Profile-Request	PPR	~~6~~305	6.1.11
Push-Profile-Answer	PPA	~~6~~305	6.1.12

6.1.1 User-Authorization-Request (UAR) Command

The User-Authorization-Request (UAR) command, indicated by the Command-Code field set to ~~1~~300 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request the authorization of the registration of a multimedia user.

Message Format

< User-Authorization-Request> ::= < Diameter Header: ~~10415: 1~~300, TBD, REQ, PXY >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ User-Name }
{ Public-Identity }
{ Visited-Network-Identifier }
[User-Authorization-Type]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.2 User-Authorization-Answer (UAA) Command

The User-Authorization-Answer (UAA) command, indicated by the Command-Code field set to ~~1~~ 300 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the User-Authorization-Request command. The Result-Code AVP or ~~Vendor-Specific~~Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in [6].

Message Format

< User-Authorization-Answer> ::= < Diameter Header: ~~10415: 1~~300, TBD>
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[~~Vendor-Specific~~Experimental-Result]
{ Auth-Session-State }

{ Origin-Host }
{ Origin-Realm }
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.3 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to ~~2~~ 301 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request it to store the name of the server that is currently serving the user.

Message Format

<Server-Assignment-Request> ::= < Diameter Header: ~~10415: 2~~301, TBD, REQ, PXY >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
[User-Name]
***[Public-Identity]**
[Server-Name]
{ Server-Assignment-Type }
{ User-Data-Request-Type }
{ User-Data-Already-Available }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.4 Server-Assignment-Answer (SAA) Command

The Server-Assignment-Answer (SAA) command, indicated by the Command-Code field set to ~~2~~ 301 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Server-Assignment-Request command. The Result-Code or ~~Vendor-Specific~~Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in [6]. If Result-Code or ~~Vendor-Specific~~Experimental-Result does not inform about an error, the User-Data AVP shall contain the information that the S-CSCF needs to give service to the user.

Message Format

<Server-Assignment-Answer> ::= < Diameter Header: ~~10415: 2~~301, TBD >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[~~Vendor-Specific~~Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ User-Name }
~~-~~**[User-Data]**
[Charging-Information]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.5 Location-Info-Request (LIR) Command

The Location-Info-Request (LIR) command, indicated by the Command-Code field set to 302 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request name of the server that is currently serving the user.

Message Format

<Location-Info-Request> ::= < Diameter Header: ~~10415:~~ 302, TBD, REQ, PXY >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Destination-Host]
{ Destination-Realm }
{ Public-Identity }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.6 Location-Info-Answer (LIA) Command

The Location-Info-Answer (LIA) command, indicated by the Command-Code field set to 302 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Location-Info-Request command. The Result-Code or ~~Vendor-Specific~~Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in [6].

Message Format

<Location-Info-Answer> ::= < Diameter Header: ~~10415:~~ 302, TBD >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[~~Vendor-Specific~~Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[Server-Name]
[Server-Capabilities]
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.7 Multimedia-Auth-Request (MAR) Command

The Multimedia-Auth-Request (MAR) command, indicated by the Command-Code field set to ~~4~~ 303 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia client to a Diameter Multimedia server in order to request security information.

Message Format

< Multimedia-Auth-Request > ::= < Diameter Header: ~~10415: 4~~303, TBD, REQ >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Realm }
[Destination-Host]
{ User-Name }
{ Public-Identity }
[SIP-Auth-Data-Item]

–**[SIP-Number-Auth-Items]**
[Server-Name]
* [AVP]
* [Proxy-Info]
* [Route-Record]

6.1.8 Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA) command, indicated by the Command-Code field set to ~~4~~ 303 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Multimedia-Auth-Request command. The Result-Code or ~~Vendor-Specific~~Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in [6].

Message Format

< Multimedia-Auth-Answer > ::= < Diameter Header: ~~10415: 4~~303, TBD >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[~~Vendor-Specific~~Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
[User-Name]
[Public-Identity]
-**[SIP-Number-Auth-Items]**
*** [SIP-Auth-Data-Item]**
* [AVP]
* [Proxy-Info]
* [Route-Record]

6.1.9 Registration-Termination-Request (RTR) Command

The Registration-Termination-Request (RTR) command, indicated by the Command-Code field set to ~~5~~ 304 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to request the de-registration of a user.

Message Format

<Registration-Termination-Request> ::= < Diameter Header: ~~10415: 5~~304, TBD, REQ >
< Session-Id >
———————{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
———————{ Destination-Realm }
———————{ User-Name }
***[Public-Identity]**
{ DeRegistration-Reason }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.10 Registration-Termination-Answer (RTA) Command

The Registration-Termination-Answer (RTA) command, indicated by the Command-Code field set to ~~5~~ 304 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Registration-Termination-Request command. The Result-Code or ~~Vendor-Specific~~Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in [6].

Message Format

<Registration-Termination-Answer> ::= < Diameter Header: ~~10415: 5~~304, TBD >

< Session-Id >
~~————————————~~{ Vendor-Specific-Application-Id }
~~————————————~~[Result-Code]
[~~Vendor-Specific~~Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.11 Push-Profile-Request (PPR) Command

The Push-Profile-Request (PPR) command, indicated by the Command-Code field set to ~~6~~ 305 and the 'R' bit set in the Command Flags field, is sent by a Diameter Multimedia server to a Diameter Multimedia client in order to update the subscription data of a multimedia user in the Diameter Multimedia client whenever a modification has occurred in the subscription data that constitutes the data used by the client.

Message Format

< Push-Profile-Request > ::= < Diameter Header: ~~10415: 6~~305, TBD, REQ >
< Session-Id >
{ Vendor-Specific-Application-Id }
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
{ Destination-Host }
{ Destination-Realm }
{ User-Name }
{ User-Data }
*[AVP]
*[Proxy-Info]
*[Route-Record]

6.1.12 Push-Profile-Answer (PPA) Command

The Push-Profile-Answer (PPA) command, indicated by the Command-Code field set to ~~6~~ 305 and the 'R' bit cleared in the Command Flags field, is sent by a client in response to the Push-Profile-Request command. The Result-Code or ~~Vendor-Specific~~Experimental-Result AVP may contain one of the values defined in section 6.2 in addition to the values defined in [6].

Message Format

< Push-Profile-Answer > ::=< Diameter Header: ~~10415: 6~~305, TBD >
< Session-Id >
{ Vendor-Specific-Application-Id }
[Result-Code]
[~~Vendor-Specific~~Experimental-Result]
{ Auth-Session-State }
{ Origin-Host }
{ Origin-Realm }
*[AVP]
*[Proxy-Info]
*[Route-Record]

End of modified section

Beginning of modified section

6.2 Result-Code AVP values

This section defines new result code values that must be supported by all Diameter implementations that conform to this specification. When one of the result codes defined here is included in a response, it shall be inside an ~~Vendor-Specific~~Experimental-Result AVP and Result-Code AVP shall be absent.

End of modified section

Beginning of modified section

6.3 AVPs

The following table describes the Diameter AVPs defined for the Cx interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in this specification shall be set to 3GPP (10415).

… [text skipped for clarity]

End of modified section

Beginning of modified section

6.4 Use of namespaces

This clause contains the namespaces that have either been created in this specification, or the values assigned to existing namespaces managed by IANA.

~~This specification assigns the values 1-6 from the Command Code namespace managed by 3GPP for its Diameter vendor-specific application number 1. See section 6.1 for the assignment of the namespace in this specification.~~

6.4.1 AVP codes

This specification assigns the values 1-26 from the AVP Code namespace managed by 3GPP for its Diameter vendor-specific applications. See section 6.3 for the assignment of the namespace in this specification.

This specification makes use of the NAS-Session-Key AVP defined in [9].

6.4.2 ~~Vendor-Specific~~Experimental-Result-Code AVP values

This specification has assigned ~~Vendor-Specific~~Experimental-Result-Code AVP values 2001-2005 and 5001-5008. See section 6.2.

6.4.3 Command Code values

This specification assigns the values 300-305 from the range allocated by IANA to 3GPP in -[12].

6.4.4 Application-ID value

IANA has allocated the value TBD for the 3GPP Cx interface application.

End of modified section

3GPP TSG CN WG4 Meeting #18 **N4-030077**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.229** **CR** **013** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Replacement of the NAS-Session-Key AVP
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	08/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The newest version of NASREQ Internet Draft (draft-ietf-aaa-diameter-nasreq-10.txt) does not contain anymore a definition of NAS-Session-Key AVP. In order to avoid unstable dependencies to Internet Drafts new 3GPP specific AVPs should be specified for integrity and confidentiality keys to replace the NAS-Session-Key AVP in MAR command.
Summary of change:	⌘	The NAS-Session-Key AVP is proposed to be replaced by new Integrity-Key and Confidentiality-Key AVPs.
Consequences if not approved:	⌘	There is no standard AVP definition for security keys.

Clauses affected:	⌘	2, 6.3, 6.3.13, 6.3.27, 6.3.28, 6.4.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		CR 29.228-033
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

2 References

The following documents contain provisions, which through reference in this text constitute provisions of the present document.

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

[1] 3GPP TS 29.228 “IP Multimedia (IM) Subsystem Cx and Dx interface; signalling flows and message contents (Release 5)”

[2] 3GPP TS 33.210 “3G Security; Network Domain Security; IP Network Layer Security (Release 5)”

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

[4] IETF RFC 2396: “Uniform Resource Identifiers (URI): generic syntax”

[5] IETF RFC 2960 “Stream Control Transmission Protocol”

[6] draft-ietf-aaa-diameter-10.txt, “Diameter Base Protocol”, work in progress

[7] IETF RFC 2234 “Augmented BNF for syntax specifications”

[8] IETF RFC 2806 “URLs for Telephone Calls”

[9] void ~~draft-ietf-aaa-diameter-nasreq-09.txt, “Diameter NASREQ Extensions”, work in progress~~

[10] IETF RFC 3309: “SCTP Checksum Change”

[11] 3GPP TS 29.329 “Sh Interface based on the Diameter protocol; protocol details”

-------- Second modified section---------

6.3 AVPs

The following table describes the Diameter AVPs defined for the Cx interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted.

Table 6.3.1: Diameter Multimedia Application AVPs

				AVP Flag rules				
Attribute Name	**AVP Code**	**Section defined**	**Value Type**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Visited-Network-Identifier	1	6.3.1	OctetString	M, V				No
Public-Identity	2	6.3.2	UTF8String	M, V				N
Server-Name	3	6.3.3	UTF8String	M,V				No
Server-Capabilities	4	6.3.4	Grouped	M, V				No
Mandatory-Capability	5	6.3.5	Unsigned32	M, V				No

Optional-Capability	6	6.3.6	Unsigned32	M, V				No
User-Data	7	6.3.7	OctetString	M, V				No
SIP-Number-Auth-Items	8	6.3.8	Unsigned32	M, V				No
SIP-Authentication-Scheme	9	6.3.9	UTF8String	M, V				No
SIP-Authenticate	10	6.3.10	OctetString	M, V				No
SIP-Authorization	11	6.3.11	OctetString	M, V				No
SIP-Authentication-Context	12	6.3.12	OctetString	M, V				No
SIP-Auth-Data-Item	13	6.3.13	Grouped	M, V				No
SIP-Item-Number	14	6.3.14	Unsigned32	M, V				No
Server-Assignment-Type	15	6.3.15	Enumerated	M, V				No
Deregistration-Reason	16	6.3.16	Grouped	M, V				No
Reason-Code	17	6.3.17	Enumerated	M, V				No
Reason-Info	18	6.3.18	UTF8String	M, V				No
Charging-Information	19	6.3.19	Grouped	M, V				No
Primary-Event-Charging-Function-Name	20	6.3.20	DiameterURI	M, V				No
Secondary-Event-Charging-Function-Name	21	6.3.21	DiameterURI	M, V				No
Primary-Charging-Collection-Function-Name	22	6.3.22	DiameterURI	M, V				No
Secondary-Charging-Collection-Function-Name	23	6.3.23	DiameterURI	M, V				No
User-Authorization-Type	24	6.3.24	Enumerated	M, V				No
User-Data-Request-Type	25	6.3.25	Enumerated	M, V				No
User-Data-Already-Available	26	6.3.26	Enumerated	M, V				No
Confidentiality-Key	27	6.3.27	OctetString	M, V				No
Integrity-Key	28	6.3.28	OctetString	M, V				No
NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see [6]. NOTE 2: Depending on the concrete command.								

-------- Third modified section---------

6.3.13 SIP-Auth-Data-Item AVP

The SIP-Auth-Data-Item (AVP code 13) is of type Grouped, and contains the authentication and/or authorization information for the Diameter client.

AVP format

SIP-Auth-Data-Item :: = < AVP Header : TBD >

[SIP-Item-Number]

[SIP-Authentication-Scheme]

[SIP-Authenticate]

[SIP-Authorization]

[SIP-Authentication-Context]

[Confidentiality-Key]

[Integrity-Key]

~~*[NAS-Session-Key]~~

* [AVP]

-------- Fourth modified section---------

6.3.27 Confidentiality-Key AVP

The Confidentiality-Key (AVP code 27) is of type OctetString, and contains the Confidentiality Key (CK).

-------- Fifth modified section---------

6.3.28 Integrity-Key AVP

The Integrity-Key (AVP code 28) is of type OctetString, and contains the Integrity Key (IK).

-------- Sixth modified section---------

6.4.1 AVP codes

This specification assigns the values 1-~~26~~ 28 from the AVP Code namespace managed by 3GPP for its Diameter vendor-specific applications. See section 6.3 for the assignment of the namespace in this specification.

~~This specification makes use of the NAS-Session-Key AVP defined in [9].~~

3GPP TSG CN WG4 Meeting #18
Dublin, EIRE, 10th – 14th February 2003

N4-030079

CR-Form-v7

CHANGE REQUEST

⌘ **29.229** **CR** **014** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Correction to the values of User-Authorizatin-Type AVP
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	24/01/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The numerical value of REGISTRATION_AND_CAPABILITIES is incorrect.
Summary of change:	⌘	The value of REGISTRATION_AND_CAPABILITIES is proposed to be 2 instead of 3.
Consequences if not approved:	⌘	Interoperability problems.

Clauses affected:	⌘	6.3.24			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

6.3.24 User-Authorization-Type AVP

The User-Authorization-Type AVP (AVP code 24) is of type Enumerated, and indicates the type of user authorization being performed in a User Authorization operation, i.e. UAR command. The following values are defined:

REGISTRATION (0)

This value is used in case of the initial registration or re-registration. I-CSCF determines this from the Expires field in the SIP REGISTER method if it is not equal to zero.

This is the default value.

DE_REGISTRATION (1)

This value is used in case of the de-registration. I-CSCF determines this from the Expires field in the SIP REGISTER method if it is equal to zero.

REGISTRATION_AND_CAPABILITIES (~~3~~2)

This value is used in case of initial registration or re-registration and when the I-CSCF explicitly requests S-CSCF capability information from the HSS. 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

3GPP TSG CN WG4 Meeting #18 **N4-030277**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.229** **CR** **015** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification on Re-allocation of S-CSCF
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	12/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	29.229 is unclear on the definition and the use of the result DIAMETER_SUBSEQUENT_REGISTRATION. The same result is given by the HSS for the cases "registered user" and "unregistered user" that forces the I-CSCF to check the presence of S-CSCF capabilities in the response before determining the need of S-CSCF selection.
Summary of change:	⌘	Clarify the definitions of the "success" errors and add the DIAMETER_SUCCESS_SERVER_SELECTION (2006) as a new Result-Code AVP value, in order to distinguish the case in which the selection of a new S-CSCF is required for a unregistered user.
Consequences if not approved:	⌘	Misalignment with 29.228

Clauses affected:	⌘	6.2.1, 6.4.2			
Other specs affected:	⌘	Y: X / N:	Other core specifications	⌘	29.228-035r1
		Y: / N: X	Test specifications		
		Y: / N: X	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of first modification

6.2 Result-Code AVP values

This section defines new result code values that must be supported by all Diameter implementations that conform to this specification. When one of the result codes defined here is included in a response, it shall be inside a Vendor-Specific-Result AVP and Result-Code AVP shall be absent.

6.2.1 Success

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

6.2.1.1 DIAMETER_FIRST_REGISTRATION (2001)

~~The user is authorized to register in this server. The user was not registered yet.~~The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF shall be assigned to that user.

6.2.1.2 DIAMETER_SUBSEQUENT_REGISTRATION (2002)

~~The user is authorized to register in this server. The user was already registered (same or another public identity).~~The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF is already assigned and there is no need to select a new one.

6.2.1.3 DIAMETER_UNREGISTERED_SERVICE (2003)

~~A query for location information is received for a public identity that has not been registered before. The user to which this identity belongs can be given service even in this situation.~~The HSS informs the I-CSCF that:

- The public identity is not registered but has services related to unregistered state;
- A S-CSCF shall be assigned to the user.

6.2.1.4 DIAMETER_SUCCESS_NOT_SUPPORTED_USER_DATA (2004)

The S-CSCF informs HSS that the received subscription data contained information, which was not recognised or supported.

6.2.1.5 DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED (2005)

The HSS informs to the S-CSCF that ~~the de-registration was successful but the S-CSCF name is not stored in the HSS.~~:

- The de-registration is completed;
- The S-CSCF name is not stored in the HSS.

6.2.1.6 DIAMETER_SERVER_SELECTION (2006)

The HSS informs the I-CSCF that:

- The user is authorized to register this public identity;
- A S-CSCF is already assigned for services related to unregistered state;
- It may be necessary to assign a new S-CSCF to the user.

End of the first modification

Beginning of second modification

6.4.2 Vendor-Specific-Result-Code AVP values

This specification has assigned Vendor-Specific-Result-Code AVP values 2001-~~2005~~ 2006 and 5001-5008. See section 6.2.

End of the second modification

3GPP TSG CN WG4 Meeting #18 **N4-030237**
Dublin, EIRE, 10th – 14th February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **29.229** **CR** **018** ⌘**rev** **1** ⌘ Current version: **5.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Handling of non supported data in the S-CSCF when the profile is being updated.
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	10/02/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	When the S-CSCF receives the updated profile from the HSS and some of these data are not understood by the S-CSCF, the S-CSCF assumes the event as an error, so it gives the DIAMETER_ERROR_NOT_SUPPORTED_DATA notification back to the HSS.
Summary of change:	⌘	Specify that the reported error is DIAMETER_ERROR_NOT_SUPPORTED_DATA instead of DIAMETER_SUCCESS_NOT_SUPPORTED_DATA.
Consequences if not approved:	⌘	Incoherent error.

Clauses affected:	⌘	6.2.1, 6.2.2, 6.4.2

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		29.228-037
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

Beginning of modified section

6.2.1 Success

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

6.2.1.1 DIAMETER_FIRST_REGISTRATION (2001)

The user is authorized to register in this server. The user was not registered yet.

6.2.1.2 DIAMETER_SUBSEQUENT_REGISTRATION (2002)

The user is authorized to register in this server. The user was already registered (same or another public identity).

6.2.1.3 DIAMETER_UNREGISTERED_SERVICE (2003)

A query for location information is received for a public identity that has not been registered before. The user to which this identity belongs can be given service even in this situation.

~~6.2.1.4 DIAMETER_SUCCESS_NOT_SUPPORTED_USER_DATA (2004)~~

~~The S-CSCF informs HSS that the received subscription data contained information, which was not recognised or supported.~~

6.2.1.~~5~~4 DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED (~~2005~~2004)

The HSS informs to the S-CSCF that the de-registration was successful but the S-CSCF name is not stored in the HSS.

6.2.2 Permanent Failures

Errors that fall within the Permanent Failures category are used to inform the peer that the request failed, and should not be attempted again.

6.2.2.1 DIAMETER_ERROR_USER_UNKNOWN (5001)

A message was received for a user that is unknown.

6.2.2.2 DIAMETER_ERROR_IDENTITIES_DONT_MATCH (5002)

A message was received with a public identity and a private identity for a user, and the server determines that the public identity does not correspond to the private identity.

6.2.2.3 DIAMETER_ERROR_IDENTITY_NOT_REGISTERED (5003)

A query for location information is received for a public identity that has not been registered before. The user to which this identity belongs cannot be given service in this situation.

6.2.2.4 DIAMETER_ERROR_ROAMING_NOT_ALLOWED (5004)

The user is not allowed to roam in the visited network.

6.2.2.5 DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED (5005)

The identity being registered has already a server assigned and the registration status does not allow that it is overwritten.

6.2.2.6 DIAMETER_ERROR_AUTH_SCHEME_NOT_SUPPORTED (5006)

The authentication scheme indicated in an authentication request is not supported.

6.2.2.7 DIAMETER_ERROR_IN_ASSIGNMENT_TYPE (5007)

The identity being registered has already the same server assigned and the registration status does not allow the server assignment type.

6.2.2.8 DIAMETER_ERROR_TOO_MUCH_DATA (5008)

The volume of the data pushed to the receiving entity exceeds its capacity.

NOTE: This error code is also used in 3GPP TS 29.329 [11].

6.2.2.9 DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA (5009)

The S-CSCF informs HSS that the received subscription data contained information, which was not recognised or supported.

End of modified section

Beginning of modified section

6.4.2 Vendor-Specific-Result-Code AVP values

This specification has assigned Vendor-Specific-Result-Code AVP values 2001-~~2005~~ 2004 and 5001-~~5008~~5009. See section 6.2.

End of modified section

3GPP TSG-CN4 Meeting #18
Dublin, Ireland, 10-14 February, 2003

Tdoc N4-030268

CR-Form-v7

CHANGE REQUEST

⌘ **29.328** **CR** **019** ⌘ **rev** **2** ⌘ Current version: **5.2.1** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Change of SPI to SPT
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR
Date:	⌘	31/1/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	At the last CN#17 plenary in September, CR against 23.218 (CN1) regarding change of SPI to SPT was agreed, but corresponding CR against 29.228 and 29.328 was lef out without change about 4 months. This CR against 29.328 is submitted for alignment with 23.218
Summary of change:	⌘	SPI (Service Points of Interest) is replaced with SPT(Service Point Trigger) for the purpose of alignment with 23.218.
Consequences if not approved:	⌘	For IMS charging mechanism, it may cause backward compatibility problem in Rel 6.

Clauses affected:	⌘	Annex D			
Other specs affected:	⌘	**Y**	**N**		
		X			29.228-038
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	.			

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

----------Start of Change----------

Annex D (normative): XML schema for the Sh interface user profile

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

Tables D.1 and D.2 describe the data types and the dependencies among them that configure the XML schema.

Table D.1: XML schema for Sh 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)
tIMSUserState	IMSUserState	Enumerated	Possible values: 0 (NOT_REGISTERED) 1 (REGISTERED) 2 (REGISTERED_UNREG_SERVICES) 3 (AUTHENTICATION_PENDING)
tCSUserState	CSUserState	Enumerated	Possible values (as defined in 3GPP TS 23.078): 0 (CAMELBusy) 1 (NetworkDeterminedNotReachable) 2 (AssumedIdle) 3 (NotProvidedfromVLR)
tPSUserState	PSUserState	Enumerated	Possible values (as defined in 3GPP TS 23.078): 0 (Detached) 1 (AttachedNotReachableForPaging) 2 (AttachedReachableForPaging) 3 (ConnectedNotReachableForPaging) 4 (ConnectedReachableForPaging) 5 (NotProvidedFromSGSN)
tLocationNumber	LocationNumber	string	Syntax described in ITU-T Q.763 (base 64

			encoded according to RFC 2045). Lenght >=4 and <=16 (multiples of 4).
tGlobalCellId	GlobalCellId	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 12.
tServiceAreaId	ServiceAreaId	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 12.
tLocationAreaId	LocationAreaId	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 8.
tRoutingAreaId	RoutingAreaId	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 8.
tGeographicalInformation	GeographicalInformation	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 12.
tGeodeticInformation	GeodeticInformation	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length = 16.
tAgeOfLocationInformation	AgeOfLocationInformation	integer	>=0, <=32767
tAddressString	AddressString	string	Syntax described in 3GPP TS 29.002 (base 64 encoded according to RFC 2045). Length >= 4 and <=28 (multiples of 4).
tMSISDN	MSISDN	string	Syntax described in 3GPP TS 23.003.
tSIP_URL	PublicIdentity	anyURI	Syntax described in RFC 3261
tTEL_URL	PublicIdentity	anyURI	Syntax described in RFC 2806
tIMSPublicIdentity	IMSPublicIdentity	(union)	Union of tSIP_URL and tTEL_URL
tServiceInfo	ServiceInfo	string	
tString	RequestURI, Method, Header, Content, Line	string	
tBool	ConditionTypeCNF, ConditionNegated	boolean	Possible values: 0 (false)

			1 (true)

Table D.2: XML schema for Sh interface: complex data types

Data type	Tag	Compound of		
		Tag	Type	Cardinality
tSh-Data	Sh-Data	PublicIdentifiers	tPublicIdentity	0 to 1
		RepositoryData	tTransparentData	0 to 1
		Sh-IMS-Data	tShIMSData	0 to 1
		LocationInformation	tLocationInformation	0 to 1
tTransparentData	RepositoryData	ServiceIndication	string	1
		ServiceData	string	0 to 1
tShIMSData	Sh-IMS-Data	SCSCFName	tSIP_URL	0 to n
		InitialFilterCriteria	tInitialFilterCriteria	0 to 10
		IMSUserState	tIMSUserState	0 to 1
tCSLocationInformation	CSLocationInformation	LocationNumber	tLocationNumber	0 to 1
		CellGlobalId	tGlobalCellId	0 to 1
		ServiceAreaId	tServiceAreaId	0 to 1
		LocationAreaId	tLocationAreaId	0 to 1
		GeographicalInformation	tGeographicalInformation	0 to 1
		GeodeticInformation	tGeodeticInformation	0 to 1
		VLRNumber	tISDNAddress	0 to 1
		MSCNumber	tISDNAddress	0 to 1
		CurrentLocationRetrieved	tBool	0 to 1
		AgeOfLocationInformation	tAgeOfLocationInformation	0 to 1

tPSLocationInformation	PSLocationInformation	CellGlobalId		tGlobalCellId	0 to 1
		ServiceAreaId		tServiceAreaId	0 to 1
		LocationAreaId		tLocationAreaId	0 to 1
		RoutingAreaId		tRoutingAreaId	0 to 1
		GeographicalInformation		tGeographicalInformation	0 to 1
		GeodeticInformation		tGeodeticInformation	0 to 1
		SGSNNumber		tISDNAddress	0 to 1
		CurrentLocationRetrieved		tBool	0 to 1
		AgeOfLocationInformation		tAgeOfLocationInformation	0 to 1
tPublicIdentity	PublicIdentity	IMSPublicIdentity		tIMSPublicIdentity	0 to n
		MSISDN		tMSISDN	0 to n
tInitialFilterCriteria	InitialFilterCriteria	Priority		tPriority	1
		TriggerPoint		tTrigger	0 to 1
		ApplicationServer		tApplicationServer	1
tTrigger	Trigger	~~SPI~~SPT		~~tSiPoInt~~tSePoTri	0 to n
		ConditionTypeCNF		tBool	1
~~tSiPoInt~~tSePoTri	~~SPI~~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.					

Annex E (informative): XML document for the Sh interface user profile

The file ShDataTypes. xsd, attached to this specification, contains the XML schema document with the data description for Sh interface

----------End of Change----------