3GPP TSG CN Plenary Meeting #17 NP-020449
4th – 6th September 2002 Biarritz, FRANCE.

Source: TSG CN WG4

Title: IMS

Agenda item: 8.1 IMS Cx-/Dx-interface

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
23.008	055	1	N4-021030	Rel5	Definition of the Subscribed media parameter	F	5.1.0
29.228	001	2	N4-021022	Rel5	Clarification of implicit registration	F	5.0.0
29.228	002	1	N4-021023	Rel5	Clarification of user registration status query	F	5.0.0
29.228	003	1	N4-021024	Rel5	Clarification of HSS initiated update of user profile	F	5.0.0
29.228	004	2	N4-021025	Rel5	Clarification of MAR command	F	5.0.0
29.228	005	1	N4-021026	Rel5	Conditionality of the SIP-Auth-Data-Item in MAA command	F	5.0.0
29.228	006	2	N4-021096	Rel5	Definition of the Subscribed media parameter	F	5.0.0
29.229	001		N4-020853	Rel5	To add a reference to the new IETF RFC on SCTP checksum	F	5.0.0
29.229	003		N4-020896	Rel5	Wrong format of Charging Function Addresses	F	5.0.0
29.229	005		N4-021027	Rel5	Editorial mistake in the definition of command MAA	F	5.0.0

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021030

CR-Form-v7

CHANGE REQUEST

⌘ **23.008**	**CR**	**055**	⌘ **rev**	**1**	⌘ Current version:	**5.1.0** ⌘

*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 parameter		
Source: ⌘	CN4		
Work item code: ⌘	IMS-CCR	***Date:*** ⌘	18/07/2002
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: ⌘ The S-CSCF needs to know what are the medias subscribed by the subscriber: it has to check the SDP parameters in the SIP message in order to remove all the non-subscribed media, codec…

The CN1 group based its work on this assumption, as shown in the following text extracted from the **TS 24.229**, chapter 6 "Application usage of SDP":

6.3 Procedures at the S-CSCF

When the S-CSCF receives an INVITE or reINVITE, the S-CSCF shall examine the media parameters in the received SDP, and remove those media streams which are not allowed based on the subscription. The S-CSCF will also remove those codecs from the approved media streams which are not allowed by the subscription. If the S-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the S-CSCF should ignore the b= lines.

The CN4 group has then to specify the "subscribed media" format and the transfer of this information to the S-CSCF.

Summary of change: ⌘ This CR specifies the "Subscribed Media" parameter

Consequences if not approved: ⌘ Inconsistency between CN1 and CN4 specifications.

Clauses affected: ⌘

Y	N

Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 29.228 CR 006
			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   ******

0.1 References

…

[48] IETF RFC 2486: "The Network Access Identifier"

[49] 3GPP TS 33.203 "Access security for IP-based services"

[50] 3GPP TS 23.002 “Network architecture”

[51] draft-ietf-aaa-diameter-08.txt: "Diameter Base Protocol", work in progress

[52] 3GPP TS 33.102 "Security architecture"

[53] 3GPP TS 23.218 "IP Multimedia (IM) call model"

[54] 3GPP TS 29.328 "IP Multimedia (IM) Subsystem Sh Interface; Signalling flows and message contents (Release 5)"

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

[56] 3GPP TS 29.228 "IP Multimedia Subsystem Cx and Dx Interfaces"

******   NEXT MODIFIED SECTION   ******

3.5 Data related to Application and service triggers

For definition and handling of these data see 3GPP TS 23.218 [53]

~~.~~3.5.1 ~~Subscribed Media~~Core Network Service Authorisation

The Core Network Service Authorisation shall provide a list of Subscribed Media ~~shall provide a list of media types~~ that the subscriber is authorized to request. -Each subscribed media~~This~~ ~~shall~~ may include the following parameters (only the media parameter is mandatory):

- Media: type of the media (corresponds to the "m" parameter of the SDP field). See [55] for the coding (e.g. audio, video).
- Direction-tag: down link, up link or both (include in the "a" parameter of the SDP field). See [55] for the coding (e.g. sendrecv).
- Codec: comma-separated list of codecs authorized for this media (include in the "a" parameter of the SDP field). See [55] for the coding (e.g. H.261, AMR).
- MaxBandwidth: maximum bandwidth authorized for the media (corresponds to the "b" parameter of the SDP field). See [55] for the coding (e.g. 25.4).

~~SDP Media Types, Transport Protocols, Media Format and Bandwidth. The format of the list and the parameters contained within is FFS.~~

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

~~3.5.1 Void~~

****** NEXT MODIFIED SECTION ******

5.3 IP Multimedia Service Data Storage

Table 3: Overview of data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	AS	TYPE
Private User Identity	3.1.1	M	M	-	P
Public Identity	3.1.2	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
Core Network Service Authorisation	3.5.1	C	C		P
Initial Filter Criteria	3.5.2	C	C	-	P
Service Indication	3.5.4	M	-	M	P

****** END OF MODIFICATIONS ******

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021022

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **001** ⌘ **rev** **2** ⌘ Current version: **5.0.0** ⌘

*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 implicit registration			
Source: ⌘	CN4			
Work item code: ⌘	IMS-CCR		***Date:*** ⌘	30/07/2002
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: ⌘	The effects of implicit registration on the authentication procedure are not explained and the HSS initiated procedures require more precision. The user profile updating has no relationship with implicit registration.
Summary of change: ⌘	A new subclause is proposed to be added into 6.5.1 to clarify the effects of implicit registration on user authentication. Subclause 6.5.2.1 is deleted. The subclause 6.5.2.2 is proposed to be updated to specify more precisely the "corresponding public identities".
Consequences if not approved: ⌘	The unclear implicit registration concept would cause interoperability problems.

Clauses affected: ⌘	6.5			
	Y	**N**		
Other specs affected: ⌘		**X**	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	
Other comments: ⌘				

6.5 Implicit registration

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

What follows is an extension of the affected basic procedures.

6.5.1 S-CSCF initiated procedures

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

6.5.1.1 Registration

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

6.5.1.2 De-registration

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

6.5.1.3 Authentication

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

6.5.2 HSS initiated procedures

6.5.2.1 ~~User profile updating~~(void)

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

6.5.2.2 De-registration

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

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021023

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **002** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

*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 user registration status query		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	30/07/2002
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:	⌘	The TS 29.228 does not specify the (error) situation when the User-Authorization-Type AVP has value DE_REGISTRATION and any of the user's public IDs is not registered (i.e. no S-CSCF assigned).
Summary of change:	⌘	The result code DIAMETER_ERROR_IDENTITY_NOT_REGISTERED is proposed to be used in the above mentioned case.
Consequences if not approved:	⌘	The unspecified error case would cause the usage of different result codes and possible interoperability problems.

Clauses affected:	⌘	6.1.1.1

Other specs affected: ⌘

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

Other comments:	⌘	

6.1 Location management procedures

6.1.1 User registration status query

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

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

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

Table 6.1.1.1 : User registration status query

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

Table 6.1.1.2 : User registration status response

Information element name	Mapping to Diameter AVP	Cat.	Description

Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of the operation
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the user.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

6.1.1.1 Detailed behaviour

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

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

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

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

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

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

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

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

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

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

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

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

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

- ~~If there is not and the User-Authorization-Type received in the request has value DE_REGISTRATION, the HSS shall set the Vendor-Specific-Result to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response. The HSS shall not return any S-CSCF name or S-CSCF capabilities.~~

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.

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021024

CR-Form-v7

CHANGE REQUEST

⌘	**29.228**	**CR**	**003**	⌘ **rev**	**1**	⌘	Current version:	**5.0.0** ⌘

*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 HSS initiated update of user profile		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	30/07/2002
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:	⌘	The wording in the subclause 6.6.1 is not uniform.
Summary of change:	⌘	The term unregistered is proposed to be used.
Consequences if not approved:	⌘	Different wording would complicate the interpretation of the specification.

Clauses affected:	⌘	6.6				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

6.6 Download of relevant user data

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

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

If User-Data-Already-Available is set to USER_DATA_ALREADY_AVAILABLE and the requested profile is not up-to-date (according to the indications stored in HSS defined in 6.6.~~3~~1) the HSS shall download the requested profile, according to the value of User-Data-Request-Type.

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

6.6.1 HSS initiated update of User Profile

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

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

6.6.2 S-CSCF operation

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

3GPP TSG CN WG4 Meeting #15 **N4-021025**
Helsinki, Finland, 29th July – 2nd August 2002

CR-Form-v7

CHANGE REQUEST

⌘	**29.228**	**CR**	**004**	⌘ **rev**	**2**	⌘	Current version:	**5.0.0**	⌘

*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 MAR command		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	30/07/2002
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:	⌘	The case when a new S-CSCF sends a MAR for a user that was already registered is not detailed. The currently specified detailed behaviour of MAR command does not allow the possible change of the S-CSCF during re-registration, thus there is inconsistency between subclauses 6.3.1 and 8.1.1.
Summary of change:	⌘	The S-CSCF name is checked also when the registration status of the public identity is registered.
Consequences if not approved:	⌘	The recovery in re-registration timeout situations is not possible and the inconsistency between subclauses 6.3.1 and 8.1.1 remains.

Clauses affected:	⌘	6.3.1				
		Y	N			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

6.3 Authentication procedures

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

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

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

Table 6.3.1: Authentication request

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

Table 6.3.2: Authentication Data content – request

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

Table 6.3.3: Authentication Data content – request, synchronization failure

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

Table 6.3.4: Authentication answer

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

Table 6.3.5: Authentication Data content – response

Information	Mapping to	Cat.	Description

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

6.3.1 Detailed behaviour

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

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

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

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

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

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

   + If it is registered, the HSS shall 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.

   ~~+ If it is registered the name of the S-CSCF received in the request is the same as the name of the S-CSCF stored in the HSS and there is no S-CSCF name available in the request, the HSS shall return the requested authentication information to the S-CSCF. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.~~

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

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

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

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021026

CR-Form-v7

CHANGE REQUEST

⌘ **29.228** **CR** **005** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

*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:	⌘	Conditionality of the SIP-Auth-Data-Item in MAA command		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	30/07/2002
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:	⌘	In the registration, when the S-CSCF has already authentication vectors for the user, but it has to update the public identity's registration state in the HSS (e.g. the user is registering after unregistered state), sending of MAR command with SIP-Number-Auth-Items equal to zero is required. In this case the MAA shall not include any authentication items.
Summary of change:	⌘	The SIP-Auth-Data-Item AVP in the table 6.3.4 is proposed to be conditional.
Consequences if not approved:	⌘	Public identity's registration state will be inconsistent between HSS and S-CSCF.

Clauses affected:	⌘	6.3

Other specs affected: ⌘

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

Other comments:	⌘	

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	~~M~~C	If the SIP-Number-Auth-Items AVP is equal to zero then this AVP shall not be present. ~~Otherwise, the SIP-Number-Auth-Items AVP shall indicate the number of SIP-Auth-Data-Item AVPs present in the Authentication answer.~~ See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Vendor-Specific-Result	M	Result of the operation

Table 6.3.5: Authentication Data content – response

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

6.3.1 Detailed behaviour

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

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

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

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

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

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

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

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

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

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

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021096

CR-Form-v7

CHANGE REQUEST

⌘ **29.228 CR 006** ⌘ **rev 2** ⌘ Current version: **5.0.0** ⌘

*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 parameter		
Source: ⌘	CN4		
Work item code: ⌘	IMS-CCR	***Date:*** ⌘	18/07/2002
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: ⌘ The S-CSCF needs to know what are the medias subscribed by the subscriber: it has to check the SDP parameters in the SIP message in order to remove all the non-subscribed media, codec…

The CN1 group based its work on this assumption, as shown in the following text extracted from the **TS 24.229**, chapter 6 "Application usage of SDP":

6.3 Procedures at the S-CSCF

When the S-CSCF receives an INVITE or reINVITE, the S-CSCF shall examine the media parameters in the received SDP, and remove those media streams which are not allowed based on the subscription. The S-CSCF will also remove those codecs from the approved media streams which are not allowed by the subscription. If the S-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the S-CSCF should ignore the b= lines.

The CN4 group has then to specify the "subscribed media" format and the transfer of this information to the S-CSCF.

Summary of change: ⌘ This CR defines the "Core Network Service Authorisation"

Consequences if not approved: ⌘ Inconsistency between CN1 and CN4 specifications and interoperability issues.

Clauses affected: ⌘ 2. and B.2.X (new chapter)

Y	N

Other specs affected:	⌘	X		Other core specifications	⌘	TS 23.008 CR 055
			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 ******

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

[8] IETF RFC 2327; “SDP: Session Description Protocol”

****** NEXT MODIFIED SECTION ******

B.2 Service profile

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

:

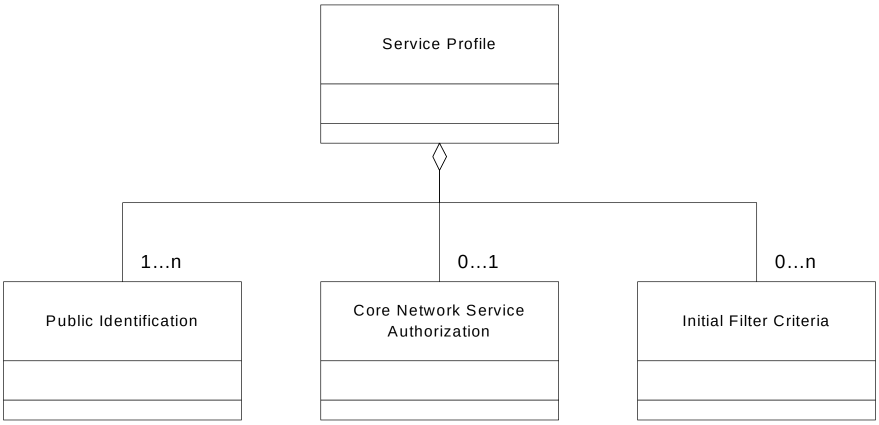

Figure B.2.1: Service Profile

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.

****** NEXT MODIFIED SECTION ******

B.2.x Core Network Service Authorization

The following picture gives an outline of the UML model of Core Network Service Authorization class:

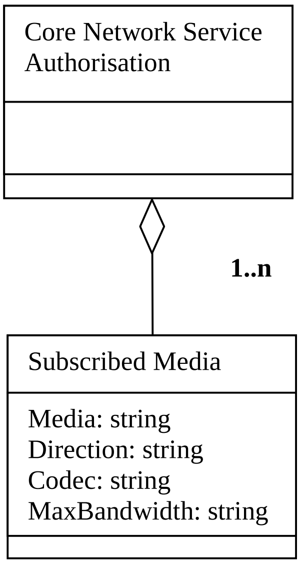

Figure B.2.x.1: Core Network Service Authorisation

Each instance of the Core Network Service Authorization class contains one or several instances of the class SubscribedMedia, defining the media that a user is authorized to use.

The syntax of Subscribed Media contains:

Parameter Name	Parameter Description	Status
Media	Type of the media (corresponds to the "m" parameter of the SDP field). See [8] for the coding (e.g. audio, video)	M
Direction-tag	Direction authorised for the media. It can be down link, up link or both (include in the "a" parameter of the SDP field). If absent, it means that any direction can be used for the media. See [8] for the coding (e.g. sendrecv)	O
Codec	Comma-separated list of codecs authorized for the media (include in	O

	the "a" parameter of the SDP field). If absent, it means that any codec can be used for the media. See [8] for the coding (e.g. H.261, AMR)	
MaxBandwidth	Maximum Bandwidth authorized for the media (corresponds to the "b" parameter of the SDP field related to the media). (Note 1) If absent, it means that no bandwidth restriction applies for the media. See [8] for the coding (e.g. 25.4)	O

Note 1: If multiple codecs are authorised for a single media type, it may be necessary to have multiple instances of subscribed media to assign a specific authorised bandwidth to each codec.

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

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

Data type	Tag	Compound of			
		Tag		Type	Cardinality
tIMSSubscription	IMSSubscription	PrivateID		tPrivateID	1
		ServiceProfile		tServiceProfile	(1 to 20)
		CoreNetworkServiceAuthorisation		tCoreNetworkServiceAuthorisation	(0 to 1)
tServiceProfile	ServiceProfile	PublicIdentity		tPublicIdentity	(1 to 20)
		InitialFilterCriteria		tInitialFilterCriteria	(1 to 10)
tCoreNetworkServiceAuthorisation	CoreNetworkServiceAuthorisation	SubscribedMedia		tSubscribedMedia	(1 to n)
tSubscribedMedia	SubscribedMedia	MediaType		tString	1
		DirectionTag		tString	(0 to 1)
		Codec		tString	(0 to 1)
		MaxBandwidth		tString	(0 to 1)
tInitialFilterCriteria	InitialFilterCriteria	Priority		tPriority	1
		TriggerPoint		tTrigger	(0 to 1)
		ApplicationServer		tApplicationServer	1
tTrigger	Trigger	SPI		tSiPoInt	(0 to 25)
		ConditionTypeCNF		tBool	1
tSiPoInt	SPI	ConditionNegated		tBool	(0 to 1)
		Group		tGroupID	(1 to 25)
		Choice of	Method	tString	1
			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)

******   END OF MODIFICATIONS   ******

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-020853

CR-Form-v7

CHANGE REQUEST

⌘ **29.229 CR 001** ⌘ **rev -** ⌘ Current version: **5.0.0** ⌘

*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:	⌘	CR to 29.229 to add a reference to the new IETF RFC on SCTP checksum
Source:	⌘	CN4

Work item code: ⌘ IMS-CCR ***Date:*** ⌘ 11/07/2002

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:	⌘	To provide the new reference to the IETF RFC 3309 which gives the newly devised error free checksum algorithm for SCTP.
Summary of change:	⌘	A new RFC reference is provided and stipulated to be used for SCTP.
Consequences if not approved:	⌘	An error prone checksum algorithm for SCTP will be used.

Clauses affected: ⌘ 2, 5.4

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.

***** First 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.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”

***** Next Modified Section *****

5.4 Transport protocol

Diameter messages over the Cx interface shall make use of SCTP [5] and shall utilise the new SCTP checksum method specified in RFC 3309 [10].

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-020896

CR-Form-v7

CHANGE REQUEST

⌘ **29.229**	**CR**	**003**	⌘ **rev**	**-**	⌘ Current version:	**5.0.0** ⌘

*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:	⌘	Wrong format of Charging Function Addresses		
Source:	⌘	CN4		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	08/07/2002
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:	⌘	The format of the charging function addresses is wrong in table 6.3.1. It should be DiameterURI instead of OctetString. Essential correction
Summary of change:	⌘	Format of charging function addresses changed in table 6.3.1 from OctetString to DiameterURI
Consequences if not approved:	⌘	Inconsistency between the data type in table 6.3.1 and in chapters 6.3.20 to 6.3.23.

Clauses affected:	⌘	6.3				
		Y	**N**			
Other specs affected:	⌘	□	□	Other core specifications	⌘	
		□	□	Test specifications		
		□	□	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 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	~~OctetString~~DiameterURI	M, V				No
Secondary-Event-Charging-Function-Name	21	6.3.21	~~OctetString~~DiameterURI	M, V				No
Primary-Charging-Collection-Function-Name	22	6.3.22	DiameterURI~~OctetString~~	M, V				No
Secondary-Charging-Collection-Function-Name	23	6.3.23	DiameterURI~~OctetString~~	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
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.								

…

3GPP TSG CN WG4 Meeting #15
Helsinki, Finland, 29th July – 2nd August 2002

N4-021027

CR-Form-v7

CHANGE REQUEST

⌘	**29.229**	**CR**	**005**	⌘**rev**	**-**	⌘	Current version:	**5.0.0**	⌘

*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: ⌘	Editorial mistake in the definition of command MAA			
Source: ⌘	CN4			
Work item code: ⌘	IMS CCR		***Date:*** ⌘	30/07/2002
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: ⌘	The name of Authentication-Data-Item AVP of MAA command has to be changed to SIP-Auth-Data-Item.
Summary of change: ⌘	The name of Authentication-Data-Item AVP of MAA command is changed to SIP-Auth-Data-Item
Consequences if not approved: ⌘	Internal inconsistency in the specification. Authentication-Data-Item AVP is not defined.

Clauses affected: ⌘	6.1.8				
	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.

6.1.8 Multimedia-Auth-Answer (MAA) Command

The Multimedia-Auth-Answer (MAA) command, indicated by the Command-Code field set to 4 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-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 >
                               < Session-Id >
                               { Vendor-Specific-Application-Id }
                               [ Result-Code ]
                               [ Vendor-Specific-Result ]
                               { Auth-Session-State }
                               { Origin-Host }
                               { Origin-Realm }
                               [ User-Name ]
                               [ Public-Identity ]
                                [ SIP-Number-Auth-Items ]
                               * [ SIP-Auth~~entication~~-Data-Item ]
                               * [ AVP ]
                               * [ Proxy-Info ]
                               * [ Route-Record ]
```