## 3GPP TSG CN Plenary Meeting #22 10<sup>th</sup> – 12<sup>th</sup> December 2003 Maui, USA.

Source: TSG CN WG4

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

Agenda item: 8.1

**Document for:** APPROVAL

Spec	CR	CR Rev Doc-2nd-Level Phase Subject		Cat	Ver_C		
29.229	021	1	N4-031220	Rel-5	The S-CSCF name needs to be checked always in MAR and SAR	F	5.5.0
29.228	054	3	N4-031280	Rel-5	The S-CSCF name needs to be checked always in MAR	F	5.5.0
29.228	061	1	N4-031281	Rel-6	The S-CSCF name needs to be checked always in MAR	Α	6.0.0
29.228	062		N4-031222	Rel-5	Conditional AVPs in answer commands	F	5.5.0
29.228	063		N4-031223	Rel-6	Conditional AVPs in answer commands	Α	6.0.0
29.229	027		N4-031241	Rel-5	User-Authorization-Type	F	5.5.0
29.228	066		N4-031237	Rel-5	Determination of User-Authorization-Type AVP based on registration expiration		5.5.0
29.228	067		N4-031238	Rel-6	Rel-6 Determination of User-Authorization-Type AVP based on registration expiration		6.0.0
29.228	064	1	N4-031283	Rel-5	el-5 Server-Assignment-Request		5.5.0
29.228	065	1	N4-031284	Rel-6	S Server-Assignment-Request		6.0.0
29.228	068	2	N4-031304	Rel-5	Not registered state after deregistration with S-CSCF deleted at the HSS	F	5.5.0
29.228	069	2	N4-031305	Rel-6	Not registered state after deregistration with S-CSCF deleted at the HSS		6.0.0
29.228	059	1	N4-031310	Rel-5	MAR in synchronisation failure case	F	5.5.0
29.228	060	1	N4-031311	Rel-6	MAR in synchronisation failure case		6.0.0
29.228	070		N4-031357	Rel-5	The extensibility of the XML schema	F	5.5.0
29.228	071		N4-031358	Rel-6	The extensibility of the XML schema	Α	6.0.0

				С	HAN	GE	REQ	UE	ST	•					CR-Form-v7
*		29.	228	CR 0	54	8	≋rev	3	æ	Curre	ent ver	sion:	5.5.	0	*
For <u>HEL</u>	_P on u	sing th	nis for	m, see k	oottom o	of this p	page or	look	at th	e pop	-up tex	t over	the <b>%</b>	syn	nbols.
Proposed o	change a	affects	s: L	JICC ap	ps <b>#</b>		ME	Rad	dio A	ccess	Netwo	ork	] Core	e Ne	twork X
Title:	ж	The	S-CS	CF nam	e needs	to be	checke	ed alv	vays	in MA	R				
Source:	*	CN4	,												
Work item	code: ₩	IMS	-CCR							L	Date: 3	23/	10/200	)3	
Category:	ж	F								Rele	ease: #	Re	l-5		
		F A B C Detail	(corr (corr (add (fund (edit ed exp	rection) responds lition of fe ctional m orial mod	odification dification) s of the a	rection n of fea bove c	in an ea ature)			Us e)	e <u>one</u> o 2 R96 R97 R98 R99 Rel-4 Rel-5 Rel-6	f the fo (GSN (Rele (Rele (Rele (Rele (Rele		96) 96) 97) 98)	ases:
Γ				_			_					,	,		
Reason for	change	e: #	The H	HSS nee	ssential eds to ve the user	erify th		//AR	comr	mand	comes	from	the S-C	csc	F that is
Summary o	of chang	је: Ж		HSS che	ecks the	S-CS	CF nam	ne als	o in	the re	sycroni	sation	case	of th	ne MAR
Consequent not approve		*	CSCI S-CS	F than w CF to th	onisation what is as ne HSS when the HSS whe	ssigne will be	ed for the differe	e use nt fro	er, so m the	the Re RAN	RAND p ID sent	aram	eter se	nt fr	om the
Clauses aff	fected:	æ	631	and 8.1											
Other spec affected:	s	*	YN	Other o	core spe pecificati specifica	ons	ions	ж	29.2	229 (C	R 021)	)			
Other comi	ments:	$\mathbf{z}$													

#### **How to create CRs using this form:**

- 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  $\underline{\text{ftp://ftp.3gpp.org/specs/}}$  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.

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.

**Table 6.3.1: Authentication request** 

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	This information element contains the public identity of the user
(See 7.2)  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	С	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 binary encoded.

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	М	Number of authentication vectors delivered in the Authentication Data information element
Authentication Data (See 7.9)	SIP-Auth- Data-Item	С	If the SIP-Number-Auth-Items AVP is equal to zero then this AVP shall not be present.  See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Experimental- Result	M	Result of the operation.  Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.  Experimental-Result AVP shall be used for Cx/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	С	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP- Authentication -Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".

Authentication Information (See 7.9.3)	SIP- Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP- Authorization	M	It shall containbinary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentialit y Key (See 7.9.5)	Confidentialit y-Key	О	- This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	- This information element shall contain the integrity key. It shall be binary encoded.

#### 6.3.1 Detailed behaviour

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

- 1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2. The HSS may check that the private and public identities belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_IDENTITIES\_DONT\_MATCH.
- 3. Check that the authentication scheme indicated in the request is supported. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_AUTH\_SCHEME\_UNSUPPORTED.
- 4. 4. If the request indicates there is a synchronization failure, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
  - <u>If they are identical</u> the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER\_SUCCESS.
- 5. Check the registration status of the public identity received in the request:
  - If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
    - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER\_SUCCESS.
  - If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored), the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
    - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this

public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER\_SUCCESS.

- If 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 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.

## 8.1 Registration error cases

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

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

			CHAN	GE REQ	UE	ST			CR-Form-v7
*	29.2	228 CF	<b>059</b>	жrev	1	<b>*</b>	Current vers	5.5.	<b>0</b> #
For <u>HELP</u> on the second secon	-		ee bottom o	of this page or	_		pop-up text		symbols.  Network X
				-11					
Title:		•	ronisation f	allure case					
Source:	CN4								
Work item code: #	IMS-	CCR					Date: #	17/10/200	3
Category: #	F A B C D Detaile	(correction (corresponding) (addition (function (editorial) (ed explana	onds to a cor of feature), al modification modification	rection in an ea on of feature) ) above categorie			2	Rel-5 the following (GSM Phase (Release 19: (Release 19: (Release 19: (Release 4): (Release 4) (Release 5) (Release 6)	e 2) 96) 97) 98)
Reason for chang		ensure th	at in the sy	The LS from nchronisation E and stored i	failure	case	the S-CSC	F shall send	the CN4 to
Summary of chan	ge: #	The usag	ge of SIP-Au	uthorization A	/P is p	ropo	sed to be sp	ecified more	e accurate.
Consequences if not approved:	æ	Incorrect	behaviour	of S-CSCF ma	ay caus	se a ı	replay of syr	nchronisation	n failure.
Clauses affected:	¥	6.3							
Other specs affected:	*	/ N X Oth X Tes	ner core spe st specificat M Specifica	ions	ж				
Other comments:	ж	Tdoc N4	-031211 cor	ntains the mirr	or CR	060 f	for Rel-6		

#### How to create CRs using this form:

- 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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)	<ol> <li>With "track changes" disabled, paste the clause containing the first piece the change request.</li> </ol>	e the entire CR fo of changed text.	orm (use CTRL-A to Delete those parts	select it) into the specif of the specification whic	ication just in front of th are not relevant to

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.

**Table 6.3.1: Authentication request** 

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	This information element contains the public identity of the user
(See 7.2)  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	С	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, as sent to the terminal, and auts, as received from the terminal. Nonce and auts shall both be binary encoded.

**Table 6.3.4: Authentication answer** 

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	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	С	If the SIP-Number-Auth-Items AVP is equal to zero then this AVP shall not be present.  See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Experimental- Result	M	Result of the operation.  Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.  Experimental-Result AVP shall be used for Cx/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	С	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP- Authentication -Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".

Authentication Information (See 7.9.3)	SIP- Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP- Authorization	M	It shall containbinary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentialit y Key (See 7.9.5)	Confidentialit y-Key	О	- This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	- This information element shall contain the integrity key. It shall be binary encoded.

CHANGE REQUEST											
*		29.22	CR (	060	<b>≋rev</b>	1	ж (	Current vers	ion: <b>6.</b>	0.0	*
For <u>HELP</u>	on us	sing this fo	orm, see l	bottom of th	is page or	look a	at the	pop-up text	over the	<b>₩</b> syn	nbols.
Proposed cha	nge a	iffects:	UICC ap	ps <b>%</b>	ME	Rad	lio Aco	cess Networ	·k C	ore Ne	twork X
Title:	Ж	MAR in	synchroni	isation failu	re case						
Source:	æ	Nokia									
Work item cod	de: #	IMS-CC	R					Date: ₩	17/10/2	2003	
Category:		F (cd A (cd B (ad C (fu D (ed	orrection) orresponds odition of for onctional moditiorial mod xplanation	odification of dification) s of the abov	ion in an ea ffeature)		-	Release: <b>%</b> Use <u>one</u> of 2 R96 R97 R98 R99 Rel-4 Rel-5 Rel-6		ase 2) 1996) 1997) 1998) 1999) 4)	ases:
Reason for ch	nange	syn	chronisat		ase the S-	CSCF	shall	ks the CN4 to send the no			
Summary of c	hang	e:	e usage o	f SIP-Autho	rization A\	/P is p	oropos	sed to be sp	ecified m	ore ac	ccurate.
Consequence not approved:		# Inc	orrect beh	naviour of S	-CSCF ma	ıy cau	se a r	eplay of syr	chronisa	tion fa	ilure.
Clauses affec	ted:	₩ 6.3									
Other specs affected:		)	Other of Test sp	core specific pecifications Specification	3	ж					
Other comme	nts:	<b>₩</b> Tdd	c N4-031	210 contair	ns the corr	espon	ding (	CR 059 for F	Rel-5		

#### How to create CRs using this form:

- 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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)	<ol> <li>With "track changes" disabled, paste the clause containing the first piece the change request.</li> </ol>	e the entire CR fo of changed text.	orm (use CTRL-A to Delete those parts	select it) into the specif of the specification whic	ication just in front of th are not relevant to

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.

**Table 6.3.1: Authentication request** 

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	This information element contains the public identity of the user
(See 7.2)  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	С	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, as sent to the terminal, and auts, as received from the terminal. Nonce and auts shall both be binary encoded.

Table 6.3.4: Authentication answer

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity (See 7.2)	Public-Identity	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	С	If the SIP-Number-Auth-Items AVP is equal to zero then this AVP shall not be present.  See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Experimental- Result	M	Result of the operation.  Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.  Experimental-Result AVP shall be used for Cx/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	С	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP- Authentication -Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".

Authentication Information (See 7.9.3)	SIP- Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP- Authorization	M	It shall containbinary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentialit y Key (See 7.9.5)	Confidentialit y-Key	О	- This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	- This information element shall contain the integrity key. It shall be binary encoded.

			CHAN	GE REC	UE	ST				CR-Form-v7
*	29.2	28 CR	061	жrev	1	æ	Current vers	sion: 6.	0.0	*
For <u>HELP</u> on u	sing thi	s form, se	ee bottom o	of this page o	r look	at the	e pop-up text	over the	<b>Ж</b> syn	nbols.
Proposed change a	affects	: UICC	apps <b></b>	] ME	Rad	dio A	ccess Netwo	rk Co	ore Ne	twork X
Title: 第	The S	S-CSCF r	ame needs	s to be check	ed alw	<i>ı</i> ays i	n MAR			
Source: #	CN4									
Work item code: 第	IMS-0	CCR					Date: #	23/10/2	2003	
Category: #	F A B C D	(correction (correspo (addition (functiona (editorial) d explanat	nds to a con of feature), Il modification modification,	rection in an e on of feature) ) above categori		elease	Release: <b>%</b> Use <u>one</u> of 2 e) R96 R97 R98 R99 Rel-4 Rel-5 Rel-6		ase 2) 1996) 1997) 1998) 1999) 4)	ases:
Reason for change			needs to vo	erify that the r.	MAR	comm	nand comes f	from the S	S-CSC	F that is
Summary of chang		The HSS command		S-CSCF nar	ne als	o in tl	he resycronis	sation cas	se of th	ne MAR
Consequences if not approved:	(	CSCF that S-CSCF t	n what is a the HSS	n case the M ssigned for t will be differe roved S3-030	ne use ent fror	er, so m the	the RAND part RAND sent	arameter	sent fr	om the
Clauses affected:	<b></b>	6.3.1 and	8.1							
Other specs affected:	¥ X	X Tes X O&I	er core spe t specificat M Specifica	ions itions		29.2	29			
Other comments:	₩ -	This is the	e rel-6 mirro	or of the CR (	)54.					

### How to create CRs using this form:

- 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  $\underline{\text{ftp://ftp.3gpp.org/specs/}}$  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.

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.

**Table 6.3.1: Authentication request** 

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	This information element contains the public identity of the user
(See 7.2)  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	С	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 binary encoded.

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	М	Number of authentication vectors delivered in the Authentication Data information element
Authentication Data (See 7.9)	SIP-Auth- Data-Item	С	If the SIP-Number-Auth-Items AVP is equal to zero then this AVP shall not be present.  See Table 6.3.5 for the contents of this information element.
Result (See 7.6)	Result-Code / Experimental- Result	M	Result of the operation.  Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.  Experimental-Result AVP shall be used for Cx/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	С	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP- Authentication -Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".

Authentication Information (See 7.9.3)	SIP- Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP- Authorization	M	It shall containbinary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentialit y Key (See 7.9.5)	Confidentialit y-Key	О	- This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	- This information element shall contain the integrity key. It shall be binary encoded.

#### 6.3.1 Detailed behaviour

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

- 1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2. The HSS may check that the private and public identities belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_IDENTITIES\_DONT\_MATCH.
- 3. Check that the authentication scheme indicated in the request is supported. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_AUTH\_SCHEME\_UNSUPPORTED.
- 4. 4. If the request indicates there is a synchronization failure, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
  - If they are identical the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER\_SUCCESS.
- 5. Check the registration status of the public identity received in the request:
  - If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
    - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication—Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The HSS shall set the public identity's authentication pending flag which is specific to the private identity which was received in the request. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The 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. The HSS shall set the public identity's authentication pending flag which is specific to the private identity which was received in the request. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The HSS shall set the

public identity's authentication pending flag which is specific to the private identity that was received in the request. 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. The HSS shall set the public identity's authentication pending flag which is specific to the private identity that was received in the request. The Result-Code shall be set to DIAMETER\_SUCCESS.

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

## 8.1 Registration error cases

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

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

	(	CHANGE	REQ	UES <sup>-</sup>	Τ		CR-Form-v7			
* TS 29.228	CR	062	жrev	<b>-</b> #	Current vers	5.5.0	) #			
For <u>HELP</u> on using t	For <u>HELP</u> on using this form, see bottom of this page or look at the pop-up text over the <b>%</b> symbols.									
Proposed change affects: UICC apps# ME Radio Access Network Core Network X										
Title: 第 Co	nditional AVF	's in answer co	ommands							
Source: # CN	14									
Work item code: 第 IMS	S-CCR				Date: #	17/10/2003				
Deta	F (correction) A (correspond B (addition of C (functional of D (editorial m	modification of to odification) ns of the above	on in an ear feature)		2	Rel-5 the following re (GSM Phase 2 (Release 1996 (Release 1996 (Release 1998 (Release 4) (Release 5) (Release 6)	2) 5) 7) 3)			
Reason for change: 第										
Summary of change: %	Items AVPs		n MAA cor		, User-Name a They shall be					
Consequences if % not approved:	Misalignme	nt between TS	S 29.228 a	nd 29.2	29.					
Clauses affected: #	6.3									
Other specs % affected:	Y N Other	core specifica specifications Specifications		¥						
Other comments: #										

#### **How to create CRs using this form:**

- 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  $\underline{\text{ftp://ftp.3gpp.org/specs/}}$  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.

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.

**Table 6.3.1: Authentication request** 

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	This information element contains the public identity of the user
(See 7.2)  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	С	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 binary encoded.

Table 6.3.4: Authentication answer

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

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item- Number	С	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP- Authentication -Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".

Authentication Information (See 7.9.3)	SIP- Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP- Authorization	M	It shall containbinary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentialit y Key (See 7.9.5)	Confidentialit y-Key	О	- This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	- This information element shall contain the integrity key. It shall be binary encoded.

### 6.3.1 Detailed behaviour

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

- 1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2. The HSS may check that the private and public identities belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_IDENTITIES\_DONT\_MATCH.
- 3. Check that the authentication scheme indicated in the request is supported. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_AUTH\_SCHEME\_UNSUPPORTED.
- 4. If the request indicates there is a synchronization failure, the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER\_SUCCESS.
- 5. Check the registration status of the public identity received in the request:
  - If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
    - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER\_SUCCESS.
  - If it is unregistered (i.e. registered as a consequence of a terminating call to unregistered user or there is an S-CSCF keeping the user profile stored), the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:
    - If they are different, the HSS shall store the S-CSCF name. The HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. It shall also set for this public identity the flag that indicates the identity is pending of the confirmation of the authentication. The Result-Code shall be set to DIAMETER\_SUCCESS.

- If 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 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.

CHANGE REQUEST								
* TS 29.228	CR <mark>063</mark>	жrev	<b>-</b> #	Current vers	6.0.0	*		
For <u>HELP</u> on using	this form, see bottom of the	his page or l	ook at th	ne pop-up text	over the <b>%</b> syr	mbols.		
Proposed change affect	cts: UICC apps <b>Ж</b> ☐	ME	Radio A	Access Netwo	rk Core Ne	etwork X		
Title: # Co	onditional AVPs in answer	commands						
Source: # CN	N4							
Work item code: 器 IM	IS-CCR			Date: %	17/10/2003			
Deta	e one of the following categories  F (correction)  A (corresponds to a correction)  B (addition of feature),  C (functional modification of the december of the above ound in 3GPP TR 21.900.	tion in an earl		2	Rel-6 the following rele (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5) (Release 6)	eases:		
Reason for change: #	AVPs are mandatory in where the AVPs are option.  It is proposed to change	MAA commutional in the	and. It is ABNF o	s not aligned with the second of the second	vith the TS 29.2 and. and SIP-Numbe	229 r-Auth-		
Consequences if #	Items AVPs conditional Code is DIAMETER_SU  Misalignment between	JCCESS.			present ii the K	esuit-		
not approved:								
Clauses affected: #	6.3							
Other specs # affected:	X Test specification X O&M Specificatio	S	*					
Other comments: #	8							

### How to create CRs using this form:

- 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  $\underline{\text{ftp://ftp.3gpp.org/specs/}}$  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.

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.

**Table 6.3.1: Authentication request** 

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity	Public-Identity	M	This information element contains the public identity of the user
(See 7.2)  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	С	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 binary encoded.

Table 6.3.4: Authentication answer

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

Table 6.3.5: Authentication Data content – response

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item- Number	С	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP- Authentication -Scheme	M	Authentication scheme. For 3GPP R5 it shall contain "Digest-AKAv1-MD5".

Authentication Information (See 7.9.3)	SIP- Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN.
Authorization Information (See 7.9.4)	SIP- Authorization	M	It shall containbinary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentialit y Key (See 7.9.5)	Confidentialit y-Key	О	- This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	- This information element shall contain the integrity key. It shall be binary encoded.

### 6.3.1 Detailed behaviour

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

- 1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2. The HSS may check that the private and public identities belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_IDENTITIES\_DONT\_MATCH.
- 3. Check that the authentication scheme indicated in the request is supported. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_AUTH\_SCHEME\_UNSUPPORTED.
- 4. If the request indicates there is a synchronization failure, the HSS shall 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. The HSS shall set the public identity's authentication pending flag which is specific to the private identity which was received in the request. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The 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. The HSS shall set the public identity's authentication pending flag which is specific to the private identity which was received in the request. The Result-Code shall be set to DIAMETER SUCCESS.
    - If they are identical, the HSS shall download Authentication-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The HSS shall set the public identity's authentication pending flag which is specific to the private identity that was received in the request. 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. The HSS shall set the public identity's authentication pending flag which is specific to the private identity that was received in the request. The Result-Code shall be set to DIAMETER\_SUCCESS.

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

CR-Form-v7

### 3GPP TSG-CN4 Meeting #21 Bangkok, Thailand, 27<sup>th</sup> to 31<sup>th</sup> October 2003

Tdoc #N4-031283

### CHANGE REQUEST

æ

29,228 CR 064

**#rev** 

Current version: **5.5.0** 

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:

Server-Assignment-Request

Source:

₩ CN4

Work item code: 第 IMS-CCR

R98

R99

Date: # 19/09/2003

Category:

F

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.

Release: # REL-5

Use one of the following releases:

(GSM Phase 2)

2 R96 (Release 1996)

(Release 1997) R97

(Release 1998)

(Release 1999)

(Release 4) Rel-4

Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change: **\* Essential correction:** 

In case of REGISTRATION or RE\_REGISTRATION, the registration state should be set to registered for the public user identity and associated identities in case of implicit registration.

Summary of change: \* After successful registration or re-registration, the registration state shall be set to registered (if not already registered).

Consequences if not approved:

# The registration state will be unchanged although it must change from not registered to registered after a first registration. If the registration state of the public identity is not changed and has no services related no unregistered state, the interrogation at the HSS will fail with a

DIAMETER\_ERROR\_IDENTITY\_NOT\_REGISTERED response for an incoming session.

Clauses affected:

第 6.1.2

YN

Other specs affected:	*	2	X	Other core specifications Test specifications O&M Specifications	€	TS 24.229 (§ 5.4.1.4)
Other comments:	ж					

#### How to create CRs using this form:

- 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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 MODIFICATION \*\*\*

# 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
Public User Identity (See 7.2)	Public-Identity	С	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	С	User private identity.  It shall be present if it is available when the S-CSCF issues the request.  It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER.  In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server- Assignment- Type	M	Type of update the S-CSCF requests in the HSS (e.g. de-registration). See 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	Destination- Host	С	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command.
(See 7.13)			This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.
			This information may not be available if the command is sent as a consequence of a session termination for an unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	С	User private identity.  It shall be present if it is available when the HSS sends the response.  It may be absent in the following error case: when the Server-Assignment-Type of the request is UNREGISTERED_USER and the received public user identity is not known by the HSS.
Registration result (See 7.6)	Result-Code / Experimental- Result	M	Result of registration.  Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.  Experimental-Result AVP shall be used for Cx/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	С	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 shall trigger the selection of a new S-CSCF by the I-CSCF, as specified in 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging- Information	О	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 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 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 and the HSS shall set the registration state of the public user identity and associated public user identities as registered (if not already registered).

Only one <u>public</u> identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and no user information shall be returned.

- If it indicates UNREGISTERED\_USER, the HSS shall store the S-CSCF name, set the registration state of the public 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 <u>public</u> identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and the modifications specified in the previous paragraph shall not be performed.

- If it indicates TIMEOUT\_DEREGISTRATION, USER\_DEREGISTRATION, DEREGISTRATION\_TOO\_MUCH\_DATA or ADMINISTRATIVE\_DEREGISTRATION, the HSS shall clear the S-CSCF name for all the public 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 Experimental-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.

Only one public identity shall be present in the request. If more than one public identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and no user information shall be returned.

 If it indicates AUTHENTICATION\_FAILURE or AUTHENTICATION\_TIMEOUT, the HSS shall clear the S-CSCF name for the public 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 <u>public</u> identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and the modifications specified in the previous paragraph shall not be performed.

See chapter 8.1.2 and 8.1.3 for the description of the handling of the error situations: reception of an S-CSCF name different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible with the registration state of the user.

\*\*\* END OF MODIFICATION \*\*\*

# 3GPP TSG-CN4 Meeting #21 Bangkok, Thailand, 27<sup>th</sup> to 31<sup>th</sup> October 2003

*Tdoc* **≋N4-031284** 

		CHAN	IGE REQ	UE	ST	-		CR-Form-v7
ж	29.228	CR <mark>065</mark>	<b>≋rev</b>	1	ж	Current version:	6.0.0	¥
- 455								

For <u>HELP</u> or	า นร	ing this form, see	e bottom of this	s pag	e or look at the	pop-up tex	t over the <b>%</b> sym	bols.
Proposed chang	je a	ffects: UICC a	apps <b>%</b>	М	E Radio Ad	ccess Netwo	ork Core Net	work X
Title:	Ж	Server-Assign	ment-Reques	st				
Source:	æ	CN4						
Work item code:	<b>:</b> #	IMS-CCR				Date: 8	19/09/2003	
Category:	#	Use <u>one</u> of the folk <b>F</b> (correction, <b>A</b> (correspon <b>B</b> (addition o	ds to a correction feature), modification of the constitution of the constitution of the above	n in a featur		2	REL-6 f the following relea (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5) (Release 6)	ases:
Reason for chan	100	φ <sub>1</sub>	ECICTD ATIO	NT	DE DECICED		,	

Reason for change.	should be set to registered for the public user identity and associated identities in case of implicit registration.
Summary of change: #	After successful registration or re-registration, the registration state shall be set to registered (if not already registered).
Consequences if	The registration state will be unchanged although it must change from not registered to registered after a first registration. If the registration state of the public identity is not changed and has no services related no unregistered state, the interrogation at the HSS will fail with a DIAMETER_ERROR_IDENTITY_NOT_REGISTERED response for an incoming session.

Clauses affected:	ж	6	.1.2			
	_					
		Υ	Ν			
Other specs	ж		X	Other core specifications 3	¥	TS 24.229 (§ 5.4.1.4)
affected:			X	Test specifications		

	ſ	X O&M Specifications	
	· <u>-</u>	<del></del>	
Other comments:	$\mathfrak{R}$		

### **How to create CRs using this form:**

- 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a>. 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 MODIFICATION \*\*\*

# 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
Public User Identity (See 7.2)	Public-Identity	С	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	С	User private identity.  It shall be present if it is available when the S-CSCF issues the request.  It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER.  In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server- Assignment- Type	M	Type of update the S-CSCF requests in the HSS (e.g. de-registration). See 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	Destination- Host	С	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command.
(See 7.13)			This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.
			This information may not be available if the command is sent as a consequence of a session termination for an unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	С	User private identity.  It shall be present if it is available when the HSS sends the response.
			It may be absent in the following error case: when the Server-Assignment- Type of the request is UNREGISTERED_USER and the received public user identity is not known by the HSS.
Registration	Result-Code /	M	Result of registration.
result (See 7.6)	Experimental- Result		Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.
			Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile	User-Data	С	Relevant user profile.
(See 7.7)			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 shall trigger the selection of a new S-CSCF by the I-CSCF, as specified in 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging- Information	О	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 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 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 the public identity's authentication pending flag which is specific for the private
    identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER\_SUCCESS\_and the HSS
    shall set the registration state of the public identity and associated public identities as registered (if not
    already registered).

Only one <u>public</u> identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and no user information shall be returned.

- If it indicates UNREGISTERED\_USER, the HSS shall store the S-CSCF name, set the registration state of the public identity as unregistered, i.e. registered as a consequence of a terminating call and download the relevant user public identity information. If there are multiple private identities associated to the public identity in the HSS, the HSS shall arbitrarily select one of the private identities and put it into the response message. The Result-Code shall be set to DIAMETER\_SUCCESS.

Only one <u>public</u> identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and the modifications specified in the previous paragraph shall not be performed.

- If it indicates TIMEOUT\_DEREGISTRATION, USER\_DEREGISTRATION, DEREGISTRATION\_TOO\_MUCH\_DATA or ADMINISTRATIVE\_DEREGISTRATION, the HSS shall clear the S-CSCF name associated to the private identity 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 public identities associated to the private identity 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 associated to the private identity 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 decides to keep the S-CSCF name stored the HSS shall keeps the S-CSCF name stored for all the public identities associated to the private identity 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 Experimental-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.

Only one public <u>user</u> identity shall be present in the request. If more than one public identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and no user information shall be returned.

 If it indicates AUTHENTICATION\_FAILURE or AUTHENTICATION\_TIMEOUT, the HSS shall clear the S-CSCF name for the public identity associated to the private identity that the S-CSCF indicated in the request and set the registration state of the identity as not registered. If the public identity's authentication pending flag which is specific for the private identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER\_SUCCESS. Only one <u>public</u> identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and the modifications specified in the previous paragraph shall not be performed.

See chapter 8.1.2 and 8.1.3 for the description of the handling of the error situations: reception of an S-CSCF name different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible with the registration state of the user.

\*\*\* END OF MODIFICATION \*\*\*

Other comments:

ж

# 3GPP TSG-CN4 Meeting #21

*Tdoc* **≋N4-031237** 

		CHA	NGE	REQ	JE	ST				CR-Form-v7
*	29.228	CR <mark>066</mark>		⊭rev	-	æ	Current vers	sion:	5.5.0	ж
For <u>HELP</u> on us	sing this for	m, see botto	n of this <sub>l</sub>	page or I	ook i	at the	e pop-up text	over	the <b>%</b> syr	nbols.
Proposed change a	offects: \	JICC apps <b></b>		ME	Rac	dio A	ccess Netwo	rk	Core Ne	etwork X
Title: #	Determir expiratio		er-Autho	rization-	Тур	e A\	/P based or	regi	stration	
Source: #	CN4									
Work item code: ₩	IMS						Date: %	19/	09/2003	
	Use one of F (cor A (cor B (add C (fun D (edi Detailed ex	the following of rection) responds to a dition of feature ctional modificatorial modificatol lanations of tl 3GPP TR 21.9	correction e), ation of fe ion) ne above c	ature)		elease	<b>Release: 光</b> Use <u>one</u> of 2 e) R96 R97 R98 R99 Rel-4 Rel-5 Rel-6	the fo (GSM (Rele (Rele (Rele (Rele (Rele	-	eases:
Reason for change	The d	etermination	of the Us				Type is based ld be based o			
Summary of change	e: # Expir	es field is rep	laced by	Expires 1	field	or ex	xpires parame	eter in	1 Contact	field.
Consequences if not approved:							the registrat pires header.	ion co	ontains an	expires
Clauses affected:	<b>₩</b> 6.1.1									
Other specs affected:	χ X X	Other core Test specifi O&M Speci	cations	ions	æ	TS 2	29.229-027			

#### How to create CRs using this form:

- 1) Fill out the above form. The symbols above marked \( \mathbb{H} \) 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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 MODIFICATION \*\*\*

# 6.1.1 User registration status query

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

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

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

Table 6.1.1.1 : User registration status query

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

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

Table 6.1.1.2 : User registration status response

#### 6.1.1.1 Detailed behaviour

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

- 1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2. Check that the private and public identities received in the request belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER ERROR IDENTITIES DONT MATCH.
- 3. Check whether the public identity received in the request is barred for the establishment of multimedia sessions.
  - If it is, the HSS shall check whether there are other non-barred public identities to be implicitly registered with that one.
    - If so, continue to step 4.
    - If not, Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED.
- 4. Check the User-Authorization-Type received in the request:
  - If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED). Continue to step 5.
  - If it is DE\_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.
  - If it is REGISTRATION\_AND\_CAPABILITIES, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER\_ERROR \_ROAMING\_NOT\_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED). The HSS shall return the 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 S-CSCF capabilities shall be present in the response. If User-Authorization-Type is equal to REGISTRATION, Experimental-Result-Code shall be set to DIAMETER\_SUBSEQUENT\_REGISTRATION. If User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER\_SUCCESS.

- If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored) and User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER\_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION, then:
  - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER\_SUBSEQUENT\_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
  - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to DIAMETER\_SERVER\_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
  - If the value of User-Authorization-Type is DE\_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Experimental-Result-Code to DIAMETER\_ERROR\_IDENTITY\_NOT\_REGISTERED in the response.
  - If the value of User-Authorization-Type is REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
    - If there is at least one identity of the user that is registered the HSS shall return the S-CSCF name assigned for the user and Experimental-Result-Code set to DIAMETER\_SUBSEQUENT\_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
    - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored), then:
      - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER\_SUBSEQUENT\_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
      - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to
        DIAMETER\_SERVER\_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
    - If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the 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. 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.

\*\*\* END OF MODIFICATION \*\*\*

# 3GPP TSG-CN4 Meeting #21 Bangkok, Thailand, 27<sup>th</sup> to 31<sup>th</sup> October 2003

Use one of the following categories:

**C** (functional modification of feature)

Detailed explanations of the above categories can

**B** (addition of feature),

**D** (editorial modification)

be found in 3GPP TR 21.900.

**F** (correction)

Tdoc \*\*N4-031238

Use one of the following releases:

(GSM Phase 2)

(Release 1996)

(Release 1997)

(Release 1998)

(Release 1999)

(Release 4)

(Release 5)

(Release 6)

2

R96

R97

R98

R99

Rel-4

Rel-5

Rel-6

	CHANGE REQUEST									CK-FOIIII-VI	
*		29.228	CR	067	<b>≋rev</b>	-	¥	Current versi	on:	6.0.0	ж
For <u>HELP</u> o	on us	ing this for	m, see	e bottom of this	s page o	or look a	at th	e pop-up text	over	the <b>%</b> syn	nbols.
Proposed chan	ge a	ffects: L	JICC a	apps <b></b>	ME	Rac	lio A	ccess Networl	k	Core Ne	etwork X
Title:	Ж	Determin expiration		of User-Auth	orizatio	n-Typ	e A\	/P based on	regi	stration	
Source:	æ	CN4									
Work item code	e: #	IMS						Date: ℜ	19/0	09/2003	
Category:	æ	Α						Release: %	REI	L-6	

A (corresponds to a correction in an earlier release)

Reason for change: %	The determination of the User-Authorization-Type is based on the value of Expires header in REGISTER although it could be based on expires parameter in Contact too.
C	
Summary of change: ж	Expires field is replaced by Expires field or expires parameter in Contact field.
Consequences if #	
not approved:	Impossible registration or deregistration when the registration contains an expires
	parameter in Contact header instead of an Expires header.

Clauses affected:	第 6.1.1
Other specs affected:	Y N  X Other core specifications
Other comments:	<b>₩</b>

# How to create CRs using this form:

- 1) Fill out the above form. The symbols above marked \( \mathcal{H} \) 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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 MODIFICATION \*\*\*

# 6.1.1 User registration status query

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

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

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

Table 6.1.1.1: User registration status query

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

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

Table 6.1.1.2: User registration status response

#### 6.1.1.1 Detailed behaviour

(See 7.4)

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

- 1. Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_USER\_UNKNOWN.
- 2. Check that the private and public identities received in the request belong to the same user. If not Experimental-Result-Code shall be set to DIAMETER ERROR IDENTITIES DONT MATCH.
- 3. Check whether the public identity received in the request is barred for the establishment of multimedia sessions.
  - If it is, the HSS shall check whether there are other non-barred public identities to be implicitly registered with that one.
    - If so, continue to step 4.
    - If not, Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED.
- 4. Check the User-Authorization-Type received in the request:
  - If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER\_ERROR\_ROAMING\_NOT\_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED). Continue to step 5.
  - If it is DE\_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 5.
  - If it is REGISTRATION\_AND\_CAPABILITIES, the HSS shall check that the user is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER\_ERROR \_ROAMING\_NOT\_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER\_AUTHORIZATION\_REJECTED). The HSS shall return the 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 S-CSCF capabilities shall be present in the response. If User-Authorization-Type is equal to REGISTRATION, Experimental-Result-Code shall be set to DIAMETER\_SUBSEQUENT\_REGISTRATION. If User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER\_SUCCESS.

- If it is unregistered (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored) and User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER\_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION, then:
  - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER\_SUBSEQUENT\_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
  - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to DIAMETER\_SERVER\_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
  - If the value of User-Authorization-Type is DE\_REGISTRATION, then the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Experimental-Result-Code to DIAMETER\_ERROR\_IDENTITY\_NOT\_REGISTERED in the response.
  - If the value of User-Authorization-Type is REGISTRATION, then the HSS shall check if there is at least one identity of the user with an S-CSCF name assigned.
    - If there is at least one identity of the user that is registered the HSS shall return the S-CSCF name assigned for the user and Experimental-Result-Code set to DIAMETER\_SUBSEQUENT\_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
    - If there is at least one identity of the user that is unregistered (i.e registered as a consequence of a terminating call or there is an S-CSCF keeping the user profile stored), then:
      - If the selection of a new S-CSCF is not necessary, the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER\_SUBSEQUENT\_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
      - Otherwise, the HSS shall return the name of the S-CSCF assigned to the unregistered user, the S-CSCF capabilities and the Experimental-Result-Code set to
        DIAMETER\_SERVER\_SELECTION. Considering the information received from the HSS, the I-CSCF shall determine whether or not it has to select a new S-CSCF.
    - If there is not any identity of the user with an S-CSCF name assigned, then the HSS shall return the 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. 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.

\*\*\* END OF MODIFICATION \*\*\*

Proposed change affects:

# 3GPP TSG-CN4 Meeting #21 Bangkok, Thailand, 27<sup>th</sup> to 31<sup>th</sup> October 2003

UICC apps#

Tdoc #N4-031305

ME Radio Access Network Core Network X

		CHAN	GE REQ	UES1	-		CR-Form-v7	
*	29.228	CR <mark>068</mark>	жrev	2 *	Current version:	5.5.0	¥	
For <u>HELP</u>	For <u>HELP</u> on using this form, see bottom of this page or look at the pop-up text over the <b>%</b> symbols.							

					•		•	
Title:	ж	Not r	egistered state	after deregist	ration with S-CS0	CF deleted a	at the HSS	
Source:	Ж	CN4						
Work item code:	<b>:</b> #	IMS				Date: X	15/10/2003	
Category:	Ж	F			1	Release: X	REL-5	
		Use <u>or</u>	<u>ne</u> of the following	categories:		Use <u>one</u> of	the following releas	ses:
		F	(correction)			2	(GSM Phase 2)	
		Α	(corresponds to	a correction in	an earlier release)	R96	(Release 1996)	
		В	(addition of feat	ure),		R97	(Release 1997)	
			(functional modi		ıre)	R98	(Release 1998)	
			(editorial modific			R99	(Release 1999)	
			ed explanations of		egories can	Rel-4	(Release 4)	
		be four	nd in 3GPP <u>TR 2</u>	<u>1.900</u> .		Rel-5	(Release 5)	
						Rel-6	(Release 6)	

Reason for change: 
# Essential correction:
The registration status should be set to "not registered" after a Server-Assignment-Request for all kinds of deregistrations where the HSS decides to clear the S-CSCF address.

\*\*Summary of change: #\* The registration status is changed to "not registered" for these cases

\*\*Consequences if not approved: 
#\*At session establishment, the I-CSCF will request the user location to the HSS and the HSS will not be able to provide the S-CSCF name as specified in § 6.1.4.1 for an "unregistered state".

Clauses affected:	æ	6. Y	1.2 N	.1		
Other specs affected:	Ж		X	Other core specifications Test specifications O&M Specifications	æ	
Other comments:	æ					

## **How to create CRs using this form:**

- 1) Fill out the above form. The symbols above marked \( \mathcal{H} \) 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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 MODIFICATION \*\*\*

# 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
Public User Identity (See 7.2)	Public-Identity	С	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	С	User private identity.  It shall be present if it is available when the S-CSCF issues the request.  It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER.  In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server- Assignment- Type	M	Type of update the S-CSCF requests in the HSS (e.g. de-registration). See 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	Destination- Host	С	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command.
(See 7.13)		regist stored AVP	This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.
			This information may not be available if the command is sent as a consequence of a session termination for an unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	С	User private identity.  It shall be present if it is available when the HSS sends the response.  It may be absent in the following error case: when the Server-Assignment-Type of the request is UNREGISTERED_USER and the received public user identity is not known by the HSS.
Registration result (See 7.6)	Result-Code / Experimental- Result	M	Result of registration.  Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.  Experimental-Result AVP shall be used for Cx/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	С	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 shall trigger the selection of a new S-CSCF by the I-CSCF, as specified in 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging- Information	О	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 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 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 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 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 Experimental-Result-Code shall be set to DIAMETER\_SUCCESS\_SERVER\_NAME\_NOT\_STORED. If the HSS received public identities in the request, the HSS shall set the registration state to not registered for the public identity(ies) that the S-CSCF indicated in the request. If the HSS received a private identity in the request, the HSS shall set the registration state of all public identites related to the private identity to not registered.

- If it indicates NO\_ASSIGNMENT, the HSS checks whether the user is assigned for the S-CSCF requesting the data and download the 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.

Only one public identity shall be present in the request. If more than one public identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and no user information shall be returned.

 If it indicates AUTHENTICATION\_FAILURE or AUTHENTICATION\_TIMEOUT, the HSS shall clear the S-CSCF name for the public 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 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 8.1.2 and 8.1.3 for the description of the handling of the error situations: reception of an S-CSCF name different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible with the registration state of the user.

\*\*\* END OF MODIFICATION \*\*\*

# 3GPP TSG-CN4 Meeting #21 Bangkok, Thailand, 27<sup>th</sup> to 31<sup>th</sup> October 2003

Tdoc \*\*N4-031305

CHANGE REQUEST						CR-Form-v7	
*	29.228 CR	069	жrev	<b>2</b> *	Current version	on: <b>6.0.0</b>	*
For <u>HELP</u> on u	sing this form, se	e bottom of thi	is page or l	ook at the	e pop-up text o	over the <b>%</b> syn	nbols.
Proposed change affects: UICC apps ** ME Radio Access Network Core Network X							
Title: %	Not registered	d state after d	l <mark>eregistrat</mark>	ion with	S-CSCF dele	eted at the HS	SS
Source: #	CN4						
Work item code: ₩	IMS				Date: %	15/10/2003	
Reason for change	B (addition of C (functional D (editorial national nation	n) nds to a correction feature), I modification of modification) ions of the above TR 21.900.	on in an ear feature) e categories	can to "not re	2 ( R96 ( R97 ( R98 ( R99 ( Rel-4 ( Rel-5 ( Rel-6 (	he following rele (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 4) (Release 5) (Release 6)	gnment-
Summary of chang	Je:   The registra						HSS and
not approved:	the HSS wi	ll not be able t tered state".		_			

# Other specs affected: \*\*X\*\* Other core specifications X\*\* Test specifications O&M Specifications

# Other comments: #

Clauses affected:

### How to create CRs using this form:

**第 6.1.2.1** 

- 1) Fill out the above form. The symbols above marked \( \mathcal{H} \) 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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 MODIFICATION \*\*\*

# 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
Public User Identity (See 7.2)	Public-Identity	С	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	С	User private identity.  It shall be present if it is available when the S-CSCF issues the request.  It may be absent during the initiation of a session to an unregistered user. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER.  In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION, if no Public-Identity AVPs are present then User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server- Assignment- Type	M	Type of update the S-CSCF requests in the HSS (e.g. de-registration). See 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	Destination- Host	С	If the S-CSCF knows HSS name Destination-Host AVP shall be present in the command.
(See 7.13)			This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command.
			This information may not be available if the command is sent as a consequence of a session termination for an unregistered user. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity (See 7.3)	User-Name	С	User private identity.  It shall be present if it is available when the HSS sends the response.
			It may be absent in the following error case: when the Server-Assignment- Type of the request is UNREGISTERED_USER and the received public user identity is not known by the HSS.
Registration	Result-Code /	M	Result of registration.
result (See 7.6)	Experimental- Result		Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.
			Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile	User-Data	С	Relevant user profile.
(See 7.7)			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 shall trigger the selection of a new S-CSCF by the I-CSCF, as specified in 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging- Information	О	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 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 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 the public identity's authentication pending flag which is specific for the private identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER\_SUCCESS.
    - Only one identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER AVP OCCURS TOO MANY TIMES and no user information shall be returned.
  - If it indicates UNREGISTERED\_USER, the HSS shall store the S-CSCF name, set the registration state of the public identity as unregistered, i.e. registered as a consequence of a terminating call and download the relevant user public identity information. If there are multiple private identities associated to the public identity in the HSS, the HSS shall arbitrarily select one of the private identities and put it into the response message. The Result-Code shall be set to DIAMETER SUCCESS.
    - Only one identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and the modifications specified in the previous paragraph shall not be performed.
  - If it indicates TIMEOUT\_DEREGISTRATION, USER\_DEREGISTRATION, DEREGISTRATION\_TOO\_MUCH\_DATA or ADMINISTRATIVE\_DEREGISTRATION, the HSS shall clear the S-CSCF name associated to the private identity 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 public identities associated to the private identity 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 associated to the private identity 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 decides to keep the S-CSCF name stored the HSS shall keeps the S-CSCF name stored for all the public identities associated to the private identity 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 Experimental-Result-Code shall be set to DIAMETER\_SUCCESS\_SERVER\_NAME\_NOT\_STORED. If the HSS received public identities in the request, the HSS shall set the registration state to not registered for the public identity(ies) that the S-CSCF indicated in the request. If the HSS received a private identity in the request, the HSS shall set the registration state of all public identites related to the private identity to not registered.

- If it indicates NO\_ASSIGNMENT, the HSS checks whether the user is assigned for the S-CSCF requesting the data and download the 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.

Only one public identity shall be present in the request. If more than one public identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and no user information shall be returned.

- If it indicates AUTHENTICATION\_FAILURE or AUTHENTICATION\_TIMEOUT, the HSS shall clear the S-CSCF name for the public identity associated to the private identity that the S-CSCF indicated in the request and set the registration state of the identity as not registered. If the public identity's authentication pending flag which is specific for the private identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER\_SUCCESS.

Only one identity shall be present in the request. If more than one identity is present the Result-Code shall be set to DIAMETER\_AVP\_OCCURS\_TOO\_MANY\_TIMES and the modifications specified in the previous paragraph shall not be performed.

See chapter 8.1.2 and 8.1.3 for the description of the handling of the error situations: reception of an S-CSCF name different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible with the registration state of the user.

\*\*\* END OF MODIFICATION \*\*\*

# 3GPP TSG CN WG4 Meeting #21 Bangkok, THAILAND, 27<sup>th</sup> – 31<sup>st</sup> October 2003

CHANGE REQUEST								
æ	29.228 CR 070	Current version: 5.5.0 **						
For <u>HELP</u> on u	sing this form, see bottom of this page or look at the	e pop-up text over the <b>%</b> symbols.						
Proposed change	affects: UICC apps業 ME Radio Ad	ccess Network Core Network X						
Title: #	The extensibility of the XML schema							
Source: #	CN4							
Work item code: 第	IMS-CCR	Date: ₩ 30/10/2003						
Reason for change	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.  Essential correction.  The current Cx user profile XML schema definences the correction of the correction.  The current Cx user profile XML schema definences the correction of the correction.	R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)  ines several complex types to be						
Summary of abone	namespace="##other" processContents="lax maxOccurs="unbounded"/> The value "##other" of the attribute namespace check that the extensions are from a different namespace of the schema.  To avoid the definition of separate namespace Rel-6) the namespace attribute shall have the	"minOccurs="0" ace means that the validator shall at namespace than the default ces for the future extensions (e.g. e value "##any".						
Summary of chang	It is proposed to remove the attribute names comlex types in XML schema. This causes the for the namespace attribute.							
Consequences if not approved:	# Interoperability problems.							
Clauses affected:								
Other specs affected:	Y N  X Other core specifications   Test specifications   O&M Specifications							
Other comments:	Similar correction is proposed to Sh XML sch	nema too.						

How to create CRs using this form:

- 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"</pre>
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"</p>
minOccurs="0"/>
         <xs:element name="InitialFilterCriteria" type="tInitialFilterCriteria" minOccurs="0"</p>
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="SPT" type="tSePoTri" maxOccurs="unbounded"/>
         <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </r></rs:complexType>
   <xs:complexType name="tSePoTri">
      <xs:sequence>
         <xs:element name="ConditionNegated" type="tBool" default="0" minOccurs="0"/>
         <xs:element name="Group" type="tGroupID" maxOccurs="unbounded"/>
         <xs:choice>
             <xs:element name="RequestURI" type="tString"/>
             <xs:element name="Method" type="tString"/>
             <xs:element name="SIPHeader" type="tHeader"/>
```

```
<xs:element name="SessionCase" type="tDirectionOfRequest"/>
             <xs:element name="SessionDescription" type="tSessionDescription"/>
         </xs:choice>
         <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="tHeader">
      <xs:sequence>
         <xs:element name="Header" type="tString"/>
         <xs:element name="Content" type="tString" minOccurs="0"/>
      </xs:sequence>
   </r></rs:complexType>
   <xs:complexType name="tSessionDescription">
      <xs:sequence>
         <xs:element name="Line" type="tString"/>
         <xs:element name="Content" type="tString" minOccurs="0"/>
      </xs:sequence>
   </r></rs: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>
   </r></rs:complexType>
   <xs:complexType name="tPublicIdentity">
      <xs:sequence>
         <xs:element name="BarringIndication" type="tBool" default="0" minOccurs="0"/>
         <xs:element name="Identity" type="tIdentity"/>
         <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>
   <xs:element name="IMSSubscription" type="tIMSSubscription"/>
</xs:schema>
```

## 3GPP TSG CN WG4 Meeting #21 Bangkok, THAILAND, 27<sup>th</sup> – 31<sup>st</sup> October 2003

CHANGE REQUEST									
*	29.228 CR 071								
For <u>HELP</u> on us	ng this form, see bottom of this page or look at the pop-up text over the <b>%</b> symbols.								
Proposed change affects: UICC apps# ME Radio Access Network Core Network X									
Title: #	The extensibility of the XML schema								
Source: #	CN4								
Work item code: 第	IMS-CCR Date: # 30/10/2003								
ı	Release: # Rel-6  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)  Petailed explanations of the above categories can release is efound in 3GPP TR 21.900.  Release: # Rel-6  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:   Essential correction.  The current Cx user profile XML schema defines several complex types to be extensible. However the extensibility is defined in the form of <xs:any maxoccurs="unbounded" minoccurs="0" namespace="##other" processcontents="lax"></xs:any> The value "##other" of the attribute namespace means that the validator shall check that the extensions are from a different namespace than the default namespace of the schema.  To avoid the definition of separate namespaces for the future extensions (e.g. Rel-6) the namespace attribute shall have the value "##any".  Summary of change:   It is proposed to remove the attribute namespace from the any elements of comlex types in XML schema. This causes the default value "##any" to be used for the namespace attribute.									
Consequences if not approved:	** Interoperability problems.								
Clauses affected: Other specs affected:	** CxDataType.xsd file  Y N  X Other core specifications Test specifications O&M Specifications								
Other comments:	Similar correction is proposed to Sh XML schema too.								

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <a href="http://www.3gpp.org/specs/CR.htm">http://www.3gpp.org/specs/CR.htm</a>. 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"</p>
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"</p>
minOccurs="0"/>
```

```
<xs:element name="InitialFilterCriteria" type="tInitialFilterCriteria" minOccurs="0"</p>
maxOccurs="unbounded"/>
         <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </r></rs: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>
   </r></rs: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="SPT" type="tSePoTri" maxOccurs="unbounded"/>
         <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="tSePoTri">
      <xs:sequence>
         <xs:element name="ConditionNegated" type="tBool" default="0" minOccurs="0"/>
         <xs:element name="Group" type="tGroupID" maxOccurs="unbounded"/>
         <xs:choice>
             <xs:element name="RequestURI" type="tString"/>
             <xs:element name="Method" type="tString"/>
             <xs:element name="SIPHeader" type="tHeader"/>
             <xs:element name="SessionCase" type="tDirectionOfRequest"/>
```

```
<xs:element name="SessionDescription" type="tSessionDescription"/>
         </xs:choice>
         <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </r></rs: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>
   </r></rs: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:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>
   <xs:element name="IMSSubscription" type="tIMSSubscription"/>
</xs:schema>
```

## 3GPP TSG CN WG4 Meeting #21 Bangkok, THAILAND, 27<sup>th</sup> – 31<sup>st</sup> October 2003

CR-Form-v7  CHANGE REQUEST						
æ	29.229 CR <mark>021                                   </mark>	Current version: 5.5.0 **				
For <u>HELP</u> on usi	ng this form, see bottom of this page or look at the	e pop-up text over the <b>%</b> symbols.  ccess Network Core Network X				
Title:	The S-CSCF name needs to be checked always	in MAR and SAR				
Source: #	CN4					
Work item code: 第	IMS-CCR	Date: ₩ 17/10/2003				
	Ise 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)  retailed explanations of the above categories can  e found in 3GPP TR 21.900.	Release: # Rel-5 Use one of the following releases: 2 (GSM Phase 2) e) 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:  This is an essential correction. The HSS needs to check the S-CSCF name against the S-CSCF name received in the MAR and SAR commands. Currently the S-CSCF name is mandatory in both commands in 29.228.  Summary of change:  The S-CSCF name is defined mandatory in MAR and SAR.						
Consequences if not approved:	# Misalignment between 29.228 and 29.229.					
Clauses affected:	<b>%</b> 6.1.3, 6.1.7					
Other specs affected:	Y N  X Other core specifications	228				
Other comments:	<b>%</b> -					

#### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <a href="http://www.3gpp.org/specs/CR.htm">http://www.3gpp.org/specs/CR.htm</a>. 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a> 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)	<ol> <li>With "track changes" disabled, paste the the clause containing the first piece of containing the change request.</li> </ol>	e entire CR for hanged text. I	rm (use CTRL-A to Delete those parts	select it) into the spe of the specification w	ecification just in front of hich are not relevant to

### 6.1.3 Server-Assignment-Request (SAR) Command

The Server-Assignment-Request (SAR) command, indicated by the Command-Code field set to 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: 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 ]
```

### 6.1.7 Multimedia-Auth-Request (MAR) Command

The Multimedia-Auth-Request (MAR) command, indicated by the Command-Code field set to 4 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: 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 ]
```

# 3GPP TSG-CN4 Meeting #21 Bangkok, Thailand, 27<sup>th</sup> to 31<sup>th</sup> October 2003

*Tdoc* **≋N4-031241** 

CHANGE REQUEST								
æ	29.229 CR 027							
For <u>HELP</u> on u	ng 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: #	User-Authorization-Type							
Source: #	Orange							
Work item code: ₩	IMS Date:   # 19/09/2003							
Category: #	Release:  REL-5  Ise 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)  Release 1998)  Petailed explanations of the above categories can effound in 3GPP TR 21.900.  REL-5  Use one of the following releases:  2 (GSM Phase 2)  Release 1996)  R97 (Release 1997)  R98 (Release 1998)  R99 (Release 1999)  Rel-6 (Release 5)  Rel-6 (Release 6)							
Reason for change	** Essential correction:  The determination of the User-Authorization-Type is based on the value of Expires header in REGISTER although it could be based on expires parameter Contact too.	in						
Summary of chan	Expires field is replaced by Expires field or expires parameter in Contact field.							
Consequences if not approved:	Impossible registration or deregistration when the registration contains an expir parameter in Contact header instead of an Expires header.	res						
Clauses affected:	₩ 6.3.24							
Other specs affected:	Y N  X Other core specifications Test specifications O&M Specifications							
Other comments:	<b>x</b>							

How to create CRs using this form:

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

- 1) Fill out the above form. The symbols above marked \$\mathbb{X}\$ 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 <a href="ftp://ftp.3gpp.org/specs/">ftp://ftp.3gpp.org/specs/</a>. 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 MODIFICATION \*\*\*

## 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 or expires parameter in Contact 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 <u>or expires</u> parameter in Contact field in the SIP REGISTER method if it is equal to zero.

#### REGISTRATION\_AND\_CAPABILITIES (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

\*\*\* END OF MODIFICATION \*\*\*