3GPP TSG CN Plenary Meeting #27 **NP-050037**
9th – 11th March 2005 Tokyo, JAPAN.

Source: TSG CN WG4

Title: Corrections on IMS2 Cx/Dx-interface

Agenda item: 9.1

Document for: APPROVAL

Doc-2nd-Level	Spec	CR	Rev	Phase	Subject	Cat	Ver_C
N4-050154	29.229	079		Rel-6	TEL-URI reference update	F	6.3.0
N4-050197	29.228	172		Rel-6	Distribution of Cipher key and integrity Key	F	6.5.0
N4-050338	23.008	143	1	Rel-6	Add reference to implicitlyregistered public user identities set definition	F	6.4.0
N4-050460	29.228	170	3	Rel-6	Clarification of Behaviour of Shared Public User Identities	F	6.5.0

3GPP TSG-CN WG4 Meeting #26 **N4-050154**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.229** **CR** **079** ⌘ **rev** **-** ⌘ Current version: **6.3.0** ⌘

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

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

Title:	⌘	TEL-URI reference update
Source:	⌘	CN4
Work item code:	⌘	IMS2-CCR
Date:	⌘	02/02/2005
Category:	⌘	**F**
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)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change:	⌘	IETF RFC 2806 has been obsoleted by IETF RFC 3966. SA2 and CN1 have decided to update Rel-6 specs regarding this change, see 23.228 V6.8.0 and 24.229 V6.5.1.
Summary of change:	⌘	IETF RFC 3966 is referenced for TEL-URI.
Consequences if not approved:	⌘	Rel-6 29.229 refers to an obsoleted RFC.

Clauses affected:	⌘	2, 6.3.2			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

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

2 References

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

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

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

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

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

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

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

[6] IETF RFC 3588 “Diameter Base Protocol”

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

[8] IETF RFC 2806 "URLs for Telephone Calls"3966 "The tel URI for Telephone Numbers"

***** Next modified section *****

6.3.2 Public-Identity AVP

The Public-Identity AVP is of type UTF8String. This AVP contains the public identity of a user in the IMS. The syntax of this AVP corresponds either to a SIP URL (with the format defined in IETF RFC 3261 [3] and IETF RFC 2396 [4]) or a TEL URL (with the format defined in IETF RFC ~~2806~~3966 [8]).

3GPP TSG-CN WG4 Meeting #26 **N4-050197**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **172** ⌘ **rev** **-** ⌘ Current version: **6.5.0** ⌘

*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 ☒

Title:	⌘	Distribution of Cipher Key and Integrity Key
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR2
Date:	⌘	31/01/2005
Category:	⌘	**F**
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)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	There is a mismatch between 29.228 and 33.203 regarding the distribution of Cipher Key and Integrity Key from the S-CSCF to the P-CSCF during registration. 33.203 states that the Cipher Key and the Integrity Key are sent to the P-CSCF along with the random number RAND and the authentication token AUTN. However, 29.228 shows in Appendix A.4.1 that the Cipher key and the Integrity key are sent to the P-CSCF from the S-CSCF after authentication has taken place.
Summary of change:	⌘	Modify Figure A.4.1.1 to show that the Cipher Key and the Integrity Key are sent to the P-CSCF with RAND||AUTN when the user is unauthorised.
Consequences if not approved:	⌘	Misalignment between specifications leading to interoperability issues.

Clauses affected:	⌘	A.4.1

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

Other comments: ⌘

How to create CRs using this form:

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

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

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

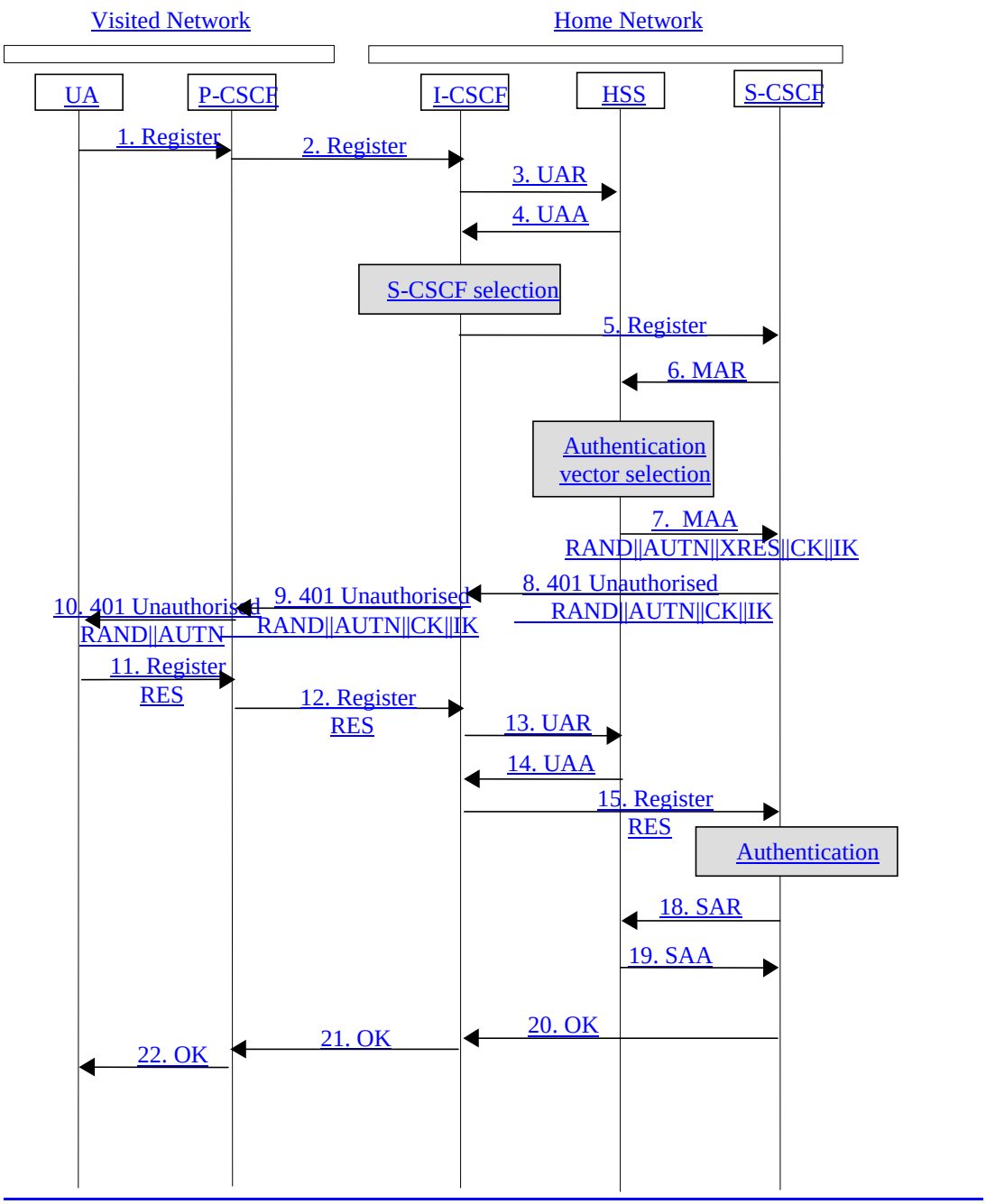
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

*** First Modification ***

A.4 Message flows

The following message flows give examples regarding which Diameter messages shall be sent in scenarios described in 3GPP TS 23.228 [1].

A.4.1 Registration– user not registered


Visited Network
Home Network
UA
P-CSCF
I-CSCF
HSS
S-CSCF
1. Register
2. Register
3. UAR
4. UAA
S-CSCF selection
5. Register
6. MAR
Authentication vector selection
7. MAA
RAND||AUTN||XRES||CK||IK
8. 401 Unauthorised
RAND||AUTN||CK||IK
9. 401 Unauthorised
RAND||AUTN||CK||IK
10. 401 Unauthorised
RAND||AUTN
11. Register
RES
12. Register
RES
13. UAR
14. UAA
15. Register
RES
Authentication
18. SAR
19. SAA
20. OK
21. OK
22. OK

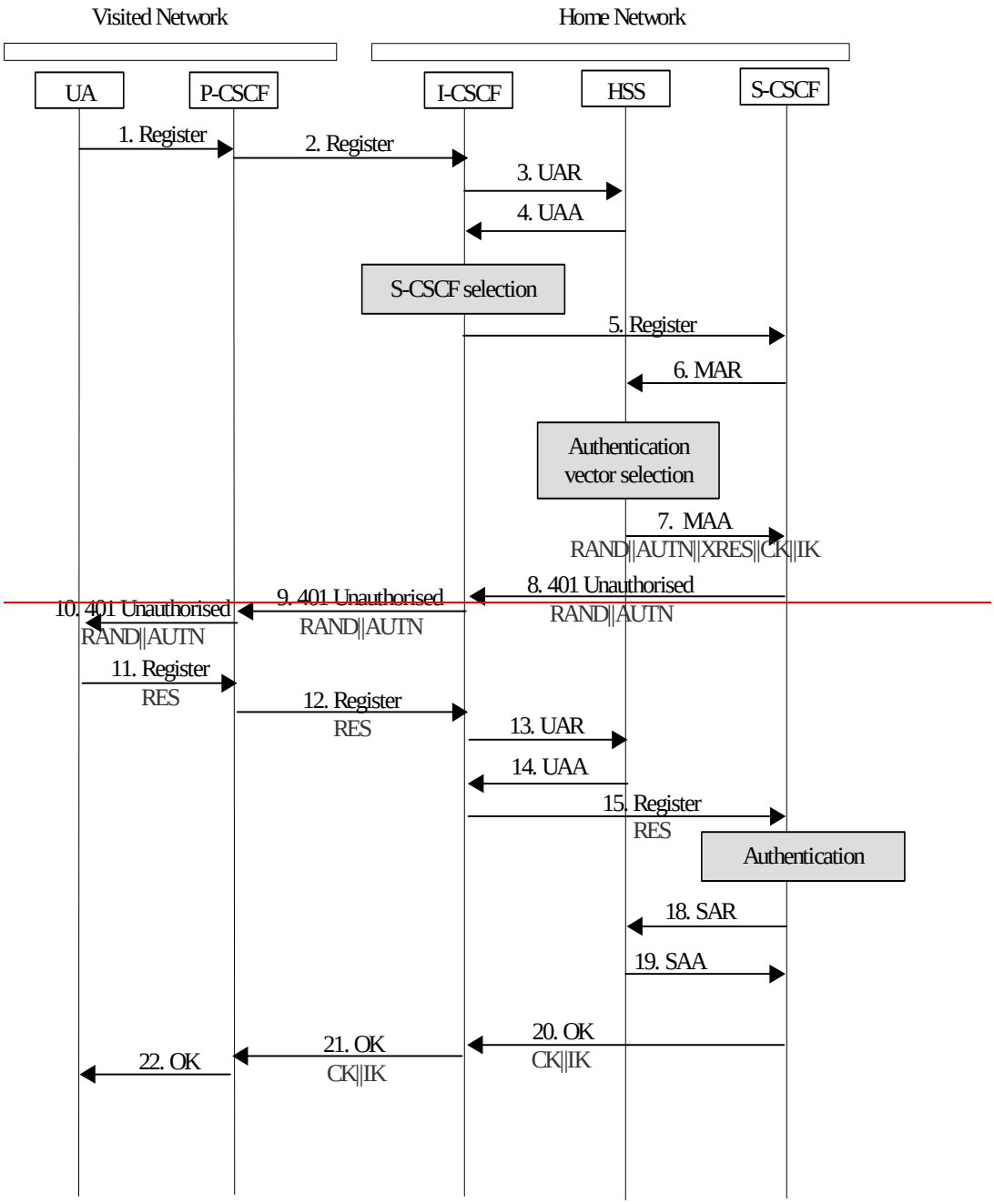


Figure A.4.1.1: Registration – user not registered

3GPP TSG–CN4 Meeting #26
Sydney, Australia, 14th to 18th February 2005

***Tdoc* ⌘N4-050338**

CR-Form-v7

CHANGE REQUEST

⌘ **23.008** **CR** **143** ⌘**rev** **1** ⌘ Current version: **6.4.0** ⌘

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

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

Title:	⌘	Add reference to Implicitly registered Public User Identities set definition
Source:	⌘	CN4
Work item code:	⌘	IMS-CCR2
Date:	⌘	04/02/2004
Category:	⌘	**F**
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)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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

Summary of change: ⌘	In TS 29.228 section 6.5.1.1 about implicit registration, it is stated: The user information downloaded in the response contains the Public User Identities of the Implicitly registered Public Identity set with the associated Service Profiles. However, in TS 23.008 no information element is currently present in the Service Profile to identify the Public User Identities which are part of a same Implicitly registered Public User Identity set. In addition, services related to Unregistered State are absent in the table of IMS data storage in section 5.3.
Summary of change: ⌘	A new section is added for Implicitly registered Public User Identity sets in section 3.1 about data related to subscription, identification and numbering. The Implicitly registered Public User Identity sets are added in the table of IMS data storage in section 5.3. In addition, Services related to Unregistered State is added in this table.
Consequences if not approved:	Inconsistency between TS 29.228, TS 23.228 and TS 23.008.

Clauses affected:	⌘	3.1, 5.3

☒ Y ☐ N

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

How to create CRs using this form:

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

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

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

3)With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause co

*** FIRST MODIFICATION ***

3.1 Data related to subscription, identification and numbering

3.1.1 Private User Identity

The Private User Identity is in the form of a Network Access Identifier (NAI), which is defined in RFC 2486 [48].

If the GAA bootstrapping is based on authentication data from the IM domain, the corresponding Private User Identity from the IM d omain (IMPI) is used as it is. If the GAA bootstrapping is based on the authentication data from the CS/PS domain, a Private User Identity is derived from user's IMSI according 3GPP TS 23.003 [5] is used.

The Private User Identity is permanent subscriber data and is stored in HSS ,and in S-CSCF.

3.1.2 Public User Identities

The Public User Identities contain one or several instances of Public User Identity, which is defined in 3GPP TS 23.003 [5].

The Public User Identities are permanent subscriber data and are stored in HSS S-CSCF and BSF.

3.1.3 Barring indication

Flag associated to each public identity to indicate that the identity is barred from any IMS communication (except registrations and re-registrations).

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

3.1.4 List of authorized visited network identifiers

The list of authorized visited network identifiers is associated with the public user identity of IMS subscribers to indicate which visited network identifiers are allowed for roaming.

The list of visited network identifiers is permanent subscriber data and is stored in the HSS. This list can be a linear list of visited network identifiers or a compound list of network identifier types e.g. home PLMN or home country; however the exact structure of the list is an implementation option.

3.1.5 Services related to ~~unregistered~~ Unregistered ~~s~~State

The Services related to ~~unregistered~~ Unregistered ~~state~~ State is a parameter associated to each public identity and it indicates whether the identity has services related to unregistered state or not.

The Services related to U~~u~~nregistered S~~s~~tate is permanent subscriber data stored in the HSS.

3.1.x~~6~~ Implicitly Registered Public User Identity Sets

The Implicitly Registered Public User Identity Set contains one or several instances of Public User Identity, and is defined in 3GPP TS 29~~3~~.228~~003~~ [5~~4~~3] following the described concept in 3GPP TS 23.228 [42]. Several Implicitly Registered Public User Identity Sets can be configured for a given user.

The Implicitly Registered Public User Identity Sets are permanent subscriber data and are stored in HSS and in S-CSCF.

~~riessriessriessriess~~*** NEXT MODIFICATION ***

5.3 IP Multimedia Service Data Storage

Table 5.3: Overview of data used for IP Multimedia services

PARAMETER	Subclause	HSS	S-CSCF	IM-SSF	AS	TYPE
Private User Identity	3.1.1	M	M		-	P
Public Identity	3.1.2	M	M		-	P
Barring Indication	3.1.3	M	M		-	P
List of authorized visited network identifiers	3.1.4	M	-		-	P
Services related to U~~u~~nregistered S~~s~~tate	3.1.5	M	-~~M~~		-	P
Implicitly registered Public User Identity~~ies~~ sets~~—~~	3.1.6	C	C	-	-	P
Registration Status	3.2.1	M	-		-	T
S-CSCF Name	3.2.2	M	-		-	T
Diameter Client Address of S-CSCF	3.2.3	M	-		-	T
Diameter Server Address of HSS	3.2.4	-	M	-	C	T
RAND, XRES, CK, IK and AUTN	3.3.1	M	C		-	T
Server Capabilities	3.4.1	C	C		-	P
Subscribed Media Profile Identifier	3.6.1	C	C		-	P
Initial Filter Criteria	3.5.2	C	C		-	P
Application Server Information	3.5.3	C	C	-	-	P
Service Indication	3.5.4	M	-		M	P
Shared iFC Set Identifier	3.5.5	C	C			P
Primary Event Charging Function Name	3.7.1	C	C	-	-	P
Secondary Event Charging Function Name	3.7.2	C	C	-	-	P
Primary Charging Collection Function Name	3.7.3	M	M	-	-	P
Secondary Charging Collection Function Name	3.7.4	C	C	-	-	P
GsmSCF address for IM CSI	3.8.4	C	-		-	P
IM-SSF address for IM CSI	3.8.5	C	-		-	T
O-IM-CSI	3.8.1	C	-	C	-	P
VT-IM-CSI	3.8.2	C	-	C	-	P
D-IM-CSI	3.8.3	C	-	C	-	P
GsmSCF address for IM CSI	3.8.4	C	-	-	-	P
IM-SSF address for IM CSI	3.8.5	C	-	-	-	T

*** END OF MODIFICATION ***

3GPP TSG-CN WG4 Meeting #26 **N4-050460**
Sydney, AUSTRALIA. 14th to 18th February 2005.

CR-Form-v7.1

CHANGE REQUEST

⌘ **29.228** **CR** **170** ⌘ **rev** **3** ⌘ Current version: **6.5.0** ⌘

*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 ☒

Title:	⌘	Clarification of behaviour for Shared Public User Identities
Source:	⌘	CN4
Work item code:	⌘	IMS2-CCR
Date:	⌘	28/01/2005
Category:	⌘	**F**
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)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(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)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Release 6 introduced the ability for multiple Private User Identities to register a single Public User Identity. With this association the behaviour of altering the registration state for the Public User Identity stored in the HSS and S-CSCF should be clarified for the case of Registration and Deregistration.
Summary of change:	⌘	- Clarification is made that an SAR/SAA should always be sent to the HSS on all registration/deregistration procedures (i.e. S-CSCF cannot filter based on registration state of Public user identity). - Behaviour is defined for registration state of a Shared Public User Identity in the SAR/SAA for cases of Deregistration and Authentication Failure. - Behaviour is defined for regisration state of a Shared Public user Identity in the RTR/RTA.
Consequences if not approved:	⌘	Incorrect the behaviour for Shared Public User Identities. Registrations and Deregistrations for Private User Identites using a Shared Public User Identity may be filitered out at the S-CSCF leading to mismatch of Registration states between the HSS and the S-CSCF. Users may be deregistered prematurely when using a Shared Public user Identity. Loss of Service.

Clauses affected:	⌘	6.1.2.1, 6.1.3.1

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

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

*** First 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 User Identity, or to clear the name of the S-CSCF assigned to one or more Public User Identities.
- To download from HSS the relevant user 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	C	Public User Identity or list of Public User Identities. One and only one Public User Identity shall be present if the Server-Assignment-Type is any value other than TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION or ADMINISTRATIVE_DEREGISTRATION. If Server-Assignment-Type indicates deregistration of some type and Private User Identity is not present in the request, at least one Public User Identity shall be present.
S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity (See 7.3)	User-Name	C	Private User 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 User Identity AVPs are present then Private User Identity 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 Already Available (See 7.16)	User-Data-Already-Available	M	This indicates if the user profile is already available in the S-CSCF. In the case where Server-Assignment-Type is not equal to NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER, the HSS shall not use User Data Already Available when processing the request.

Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name, the Destination-Host AVP shall be present in the command. This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent as a consequence of a session termination for an unregistered 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	C	Private User 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	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER according to the rules defined in section 6.6. If the S-CSCF receives more data than it is prepared to accept, it shall perform the de-registration of the 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	C	Addresses of the charging functions. It shall be present when the User-Data AVP is sent to the S-CSCF. When this parameter is included, the Primary Charging Collection Function address shall be included. All other elements shall be included if they are available.

6.1.2.1 Detailed behaviour

On registering/deregistering a Public User Identity the S-CSCF shall inform the HSS. The same procedure is used by the S-CSCF to get the user information which contains the user profile and the charging information. The relevant user profile downloaded is described in more detailed in sections 6.5.1 and 6.6. The HSS holds information about the state of registration of all the identities of the user. The S-CSCF uses this procedure to update such states. For Shared Public User Identities, the S-CSCF shall initiate this procedure towards the HSS for each Private User Identity undergoing a Registration or Deregistration related to the Shared Public User Identity. For implicitly registered identities, the rules

defined in Section 6.5.1 shall apply. The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 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. If there is neither a Public User Identity nor a Private User Identity included, the Experimental-Result-Code shall be set to DIAMETER_MISSING_USER_ID.

2. The HSS may check whether the Private and Public User 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 information. . If the Public User Identity's authentication pending flag which is specific for the Private User Identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER_SUCCESS and the HSS shall set the registration state of the Public User Identity as registered (if not already registered).

  Only one Public User 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 there is no Public User Identity present, the Experimental-Result-Code shall be set to DIAMETER_MISSING_USER_ID.

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

  Only one Public User 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 there is no Public User Identity present, the Experimental-Result-Code shall be set to DIAMETER_MISSING_USER_ID.

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

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

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

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

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

  The Result-Code shall be set to DIAMETER_SUCCESS.~~the HSS shall clear the S-CSCF name associated to the Private User Identity for all the Public User Identities that the S-CSCF indicated in the request and set the registration state of the identities as not registered. If no Public User Identity is present in the request, the Private User Identity shall be present; in this case the HSS shall clear the S-CSCF name for all the Public User Identities associated to the Private User 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 User Identity stored or not for all the Public User Identities that the S-CSCF

indicated in the request. If no Public User Identity is present in the request, the Private User Identity shall be present.

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

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

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

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

  ~~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.

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

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

  - If more than one Private User Identity that shares that Public User Identity is currently registered with the Public User Identity the HSS shall keep the registration state of the Public User Identity as Registered.~~If the HSS received Public User Identities in the request, the HSS shall set the registration state to not registered for the Public User Identity (ies) that the S-CSCF indicated in the request~~

~~. If the HSS received a Private User Identity in the request, the HSS shall set the registration state of all Public User Identities 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 relevant user information. The Result-Code shall be set to DIAMETER_SUCCESS. If the requesting S-CSCF is not the same as the assigned S-CSCF, the Result-Code shall be set to DIAMETER_UNABLE_TO COMPLY.

  Only one Public User Identity shall be present in the request. If more than one Public User Identity is present the Result-Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and no user information shall be returned. If there is no Public User Identity present, the Experimental-Result-Code shall be set to DIAMETER_MISSING_USER_ID.

- If it indicates AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, the HSS shall check the registration state for the Public User Identity in the request. For the Public User Identity;-

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

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

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

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

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

~~the HSS shall clear the S-CSCF name for the Public User Identity associated to the Private User Identity that the S-CSCF indicated in the request and set the registration state of the identity as not registered. If the Public User Identity's authentication pending flag which is specific for the Private User Identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER_SUCCESS.~~

Only one Public User 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 there is no Public User Identity present, the Experimental-Result-Code shall be set to DIAMETER_MISSING_USER_ID.

If the HSS cannot fulfil the received request, e.g. due to database error, it shall set the Result-Code to DIAMETER_UNABLE_TO_COMPLY. The HSS shall not modify any user state nor download any user Public User Identity information to the S-CSCF.

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.

*** Second Modification ***

6.1.3 Network initiated de-registration by the HSS, administrative

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

HSS may decide to de-register:

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

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

Table 6.1.3.1 : Network Initiated Deregistration by HSS request

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	O	It contains the list of public user identities that are de-registered, in the form of SIP URL or TEL URL.
Private User Identity (See 7.3)	User-Name	M	It contains the private user identity in the form of a NAI.

Reason for de-registration (See 7.11)	Deregistration -Reason	M	The HSS shall send to the S-CSCF a reason for the de-registration. The de-registration reason is composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [5]) that determines the behaviour of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given multimedia user. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

Table 6.1.3.2 : Network Initiated Deregistration by HSS response

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

6.1.3.1 Detailed behaviour

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

The HSS may de-register:

- Only one public identity or a list of public identities. In this case the S-CSCF shall remove all the information that is related to the private identity received in the request and stored in the S-CSCF for those public identities.
- The private identity with all related public identities (no public identity sent in the Cx-Deregister request). In this case the S-CSCF shall remove all the information stored for that private identity.

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

- PERMANENT_TERMINATION: The HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to the Public User Identity and associated implicitly registered Public User Identities for a given ~~user~~ Private User Indentity (e.g. due IMS subscription ~~cancellation~~modification).

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

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

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

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

associated with the Public User Identity. The S-CSCF initiates the de-registration of the Public User Identity.

- if the registration state of the Public User Identity is Unregistered, the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name associated with the Public User Identity. ~~In this case, the S-CSCF initiates the de-registration of the user's Public User Identities. The user is no longer available for registration or terminating calls in the HSS.~~

- NEW_SERVER_ASSIGNED: The HSS indicates to the S-CSCF that a new S-CSCF has been allocated to the user (e.g. because the previous assigned S-CSCF was unavailable during a registration procedure). ~~In this case, t~~The S-CSCF ~~initiates the de-registration~~shall remove all information for all of the Public User Identities~~y and the associated implicitly registered Public User Identities for that user~~within the IMS Subscription.

- SERVER_CHANGE: The HSS indicates to the S-CSCF that the de-registration is requested to force the selection of new S-CSCF to assign to the user (e.g. when the user's S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for the updated User Profile). ~~In this case, the S-CSCF initiates the de-registration of the registered Public User Identity and the associated implicitly registered Public User Identities. Then, the HSS shall set the registration state to "Not Registered" for the de-registered and implicitly de-registered Public User Identity(ies).~~ The HSS shall set the registration state to "Not Registered" and clear the S-CSCF name for all Public User Identities within the IMS Subscription. The S-CSCF should start the network initiated de-registration towards the user, i.e. all registrations within the IMS Subscription are de-registered and the user is asked to re-register to all existing registrations.

- REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to an unregistered Public User Identity(ies) (i.e registered as a consequence of a terminating call or there is a S-CSCF keeping the user profile stored) for a given user. For each Public User Identity contained within the request the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name associated with the Public User Identity. ~~In this case, t~~The S-CSCF shall remove all information related to the Public User Identity contained ~~initiates the de-registration of this user's Public User Identity(ies)~~within the request. ~~Then, the HSS shall set the registration state to "Not Registered" for the de-registered and implicitly de-registered Public User Identity(ies).~~

The detailed de-registration procedures performed by the S-CSCF for each reason code are described in the 3GPP TS 24.229 [8].