3GPP TSG CN Plenary Meeting #21 **NP-030394**
17th – 19th September 2003 Frankfurt, GERMANY.

Source: TSG CN WG4

Title: Corrections on CX and Sh interfaces

Agenda item: 9.1

Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
29.228	052		N4-030831	Rel-6	Sharing public identities across multiple UEs	B	5.4.0
23.003	073	2	N4-031060	Rel-6	PSI definition	C	5.6.0

3GPP TSG-SA WG2 Meeting #34
Brussels, Belgium, 18-22 August 2003

Tdoc ⌘N4-031060

CR-Form-v7

CHANGE REQUEST

⌘	**23.003**	**CR**	**073**	⌘ **rev**	**2**	⌘	Current version:	**5.6.0**	⌘

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: ⌘	PSI definition		
Source: ⌘	CN4		
Work item code: ⌘	IMS-2	***Date:*** ⌘	25/08/2003
Category: ⌘	**C**	***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)*

Reason for change: ⌘	The Public Service Identity (PSI) format is not defined anywhere in the specification.
Summary of change: ⌘	Define the PSI format
Consequences if not approved: ⌘	interoperatbility problems due to different understandings of a PSI

Clauses affected: ⌘	13				
	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.

13 Numbering, addressing and identification within the IP multimedia core network subsystem

13.1 Introduction

This clause describes the format of the parameters needed to access the IP multimedia core network subsystem. For further information on the use of the parameters see 3GPP TS 23.228 [24].

13.2 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in RFC 1035 [19].

If there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps:

1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [27]) and separate them into MCC and MNC with ".";
2. reverse the order of the MCC and MNC. Append to the result: ".IMSI.3gppnetwork.org"

An example of a home network domain name is:

IMSI in use: 234150999999999;

Where:

MCC = 234;

MNC = 15;

MSIN = 0999999999, which gives

home domain name: 15.234.IMSI.3gppnetwork.org.

13.3 Private user identity

The private user identity shall take the form of an NAI, and shall have the form username@realm as specified in clause 3 of RFC 2486 [25].

NOTE: It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

If there is no ISIM application, the private user identity is not known. In this case, the private user identity is derived from the IMSI.

The following steps show how to build the private user identity out of the IMSI:

1. use the whole string of digits as the username part of the private user identity;
2. convert the leading digits of the IMSI, i.e. MNC and MCC, into a domain name, as described in subclause 13.2.

The result will be a private user identity of the form imsi@mnc.mcc."IMSI.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the private user identity then takes the form 234150999999999@15.234.IMSI.3gppnetwork.org

13.4 Public user identity

The public user identity shall take the form of either a SIP URI (see RFC 3261 [26]) or a tel URL (see RFC 2806 [45]). A SIP URI shall take the form "sip:user@domain".

If there is no ISIM application to host the public user identity, a temporary public user identity shall be derived, based on the IMSI. The temporary public user identity shall be of the form "user@domain" and shall therefore be equal to the private user identity. The private user identity is derived as described in subclause 13.2. That is, the private user identity will be appended to the string "sip:"

EXAMPLE: "sip:234150999999999@15.234.IMSI.3gppnetwork.org".

13.5 Public service identity (PSI)

The public service identity shall take the form of either a SIP URI (see RFC 3261 [26]) or a tel URL (see RFC 2806 [45]).

A public service identity defines a service, or a specific resource created for a service.

The domain part is pre-defined by the IMS operators and the IMS system provides the flexibility to dynamically create the user part of the PSIs.

The SIP URI shall take the form of a distinct PSI "sip:service@domain", where “service” identifies a service (EXAMPLE: sip:conference@examplenetwork.com).

In order to facilitate the operation and maintenance of the nodes, it is possible to represent a collection of SIP URIs as an escaped SIP URI (see RFC 3261) that contains a wildcard “*”. The asterisk matches any string of 0 or more characters. Example: sip:chatlist%2A@examplenetwork.com matches sip:chatlist1@examplenetwork.com, sip:chatlist2@examplenetwork.com, etc.

NOTE: SIP URIs cannot contain wildcards, as such; the asterisk is represented as character %2A.

3GPP TSG CN WG4 Meeting #20
Sophia Antipolis, FRANCE, 25th – 29th August 2003

N4-030831

CR-Form-v7

CHANGE REQUEST

⌘ **29.228 CR 052** ⌘**rev** **-** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Sharing public identities across multiple UEs		
Source:	⌘	CN4		
Work item code:	⌘	IMS2-CCR	***Date:*** ⌘	29/08/2003
Category:	⌘	**B**	***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)*

Reason for change:	⌘	23.228 requires that different UEs may share the same public identities.
Summary of change:	⌘	To enable simultaneous registrations of the same public identity and different private identities, the public identities are defined to have private identity specific registration states and authentication pending flags. Term “authentication pending flag” is introduced and taken into use.
Consequences if not approved:	⌘	Misalignment with 23.228.

Clauses affected:	⌘	3.1, 6.1.2.1, 6.1.3.1, 6.2.2.1, 6.3.1, 6.5.1			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	The public identity needs to have private identity specific registration states and authentication pending flags because 23.228 states the following: “Registration and de-registration always relates to a particular contact address. A Public user identitity that has been registered (including when implicitly registered) with different contact addresses remains registered in relation to those contact addreses that have not been de-registered.”. The term authentication pending flag is introduced to replace texts that hint that such paramter exists e.g. “the flag that indicates that the identity is pending of the confirmation of the authentication”.			

How to create CRs using this form:

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

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

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

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

************** First modified clause ***************************************

3.1 Definitions

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

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

Authentication pending flag: A flag that indicates that the authentication of a public identity - private identity pair is pending and waiting for confirmation.

************** Next modified clause (SAR) ***************************************

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. ~~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. 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 ~~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 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~~d~~ to keep the S-CSCF name stored the HSS shall keep~~s~~ the S-CSCF name stored for all the public identities associated to the private identity ~~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 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 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 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.

************** Next modified clause (RTR) **

6.1.3.1 Detailed behaviour

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

The HSS may de-register:

- Only one public identity or a list of public identities. In this case the S-CSCF shall remove all the information that is related to the private identity received in the request and stored in the S-CSCF for those public identities.
- The ~~user~~ private identity with all ~~his/her~~ 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 ~~user~~.

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

- PERMANENT_TERMINATION: The IMS subscription or service profile(s) has been permanently terminated. The S-CSCF should start the network initiated de-registration towards the user.

- NEW_SERVER_ASSIGNED: A new S-CSCF has been allocated to the user due to some reason, e.g. an error case, where the SIP registration is terminated in a new S-CSCF. The S-CSCF shall not start the network initiated de-registration towards the user but only clears its registration state and information regarding the user, i.e. all service profiles are cleared.

- SERVER_CHANGE: A new S-CSCF shall be allocated to the user when the user's S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for the updated User Profile. The S-CSCF should start the network initiated de-registration towards the user, i.e. all registrations are de-registered and the user is asked to re-register to all existing registrations.

- REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF should no longer be used for a given user. The S-CSCF shall not start the network initiated de-registration towards the user when the user is not currently registered but clears all information regarding the user and responds to the HSS. The HSS then removes the S-CSCF for that user.

************** Next modified clause (PPR) ***************************************

6.2.2.1 Detailed behaviour

The HSS shall make use of this procedure to update relevant user profile information in the S-CSCF. See chapter 6.6.1 for the rules of user profile updating. If there are multiple registered private identities associated to the public identity in the HSS, the HSS shall send only single request and select arbitrarily one of the private identities and put it into the request.

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

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

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

Table 6.2.2.1.1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_ERROR_NOT SUPPORTED_USER_DATA	The request failed.The S-CSCF informs the HSS that the received subscription data contained information, which was not recognised or supported, i.e. profile information which is not correctly encoded according to the XML schema or standardised profile information which cannot be interpreted by the S-CSCF due to unsupported S-CSCF capabilities.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the user is not found in S-CSCF.
DIAMETER_ERROR_TOO_MUCH_DATA	The request failed. The S-CSCF informs to the HSS that it tried to push too much data into the S-CSCF.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

************** Next modified clause (MAR) ***************************************

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. ~~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. The HSS shall set the public identity’s authentication pending flag which is specific to the private identity which was received in the 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 HSS shall set the public identity’s authentication pending flag which is specific to the private identity that was received in the 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. The HSS shall set the public identity’s authentication pending flag which is specific to the private identity that was received in the 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.

************** Next modified clause (implicit registration)*************************************

6.5.1 S-CSCF initiated procedures

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

6.5.1.1 Registration

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

6.5.1.2 De-registration

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

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

6.5.1.3 Authentication

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

6.5.1.4 Downloading the user profile

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