

3GPP TSG CN Plenary Meeting #26
8th – 10th December 2004 Athens, Greece.

NP-040530

Source: TSG CN WG4
Title: Corrections on IMS2 Cx-/Dx-interface
Agenda item: 9.1
Document for: APPROVAL

Spec	CR	Rev	Doc-2nd-Level N4-040	Phase	Subject	Cat	Ver_C
29.228	146	1	1458	Rel-6	Clarification of R6 authentication scheme	F	6.4.0
29.228	155		1549	Rel-6	Correction to XML Root Element	F	6.4.0
29.228	156	1	1550	Rel-6	Modification of User-Data-Already-Available in SAR command.	F	6.4.0
29.228	140	1	1563	Rel-6	HSS initiated deregistration with user profile removal for permanent termination	F	6.4.0

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST⌘ **29.228 CR 155** ⌘ rev **-** ⌘ 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:	⌘ Correction to XML Root Element		
Source:	⌘ CN4		
Work item code:	⌘ IMS2-CCR	Date:	⌘ 21/10/2004
Category:	⌘ F	Release:	⌘ Rel-6
	Use <i>one</i> of the following categories:		Use <i>one</i> of the following releases:
	F (correction)	Ph2 (GSM Phase 2)	
	A (corresponds to a correction in an earlier release)	R96 (Release 1996)	
	B (addition of feature),	R97 (Release 1997)	
	C (functional modification of feature)	R98 (Release 1998)	
	D (editorial modification)	R99 (Release 1999)	
	Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)
			Rel-7 (Release 7)

Reason for change:	⌘ The XML representation of the trigger in Annex C states that testDatatype is the root element. However this element is unknown and not defined in the XML Schema. The root element for the user profile should be IMSSubscription.
Summary of change:	⌘ Modify the XML representations in Annex C to refer to IMSSubscription as the root element of the user profile.
Consequences if not approved:	⌘ Incorrect representation of user profile in Informative Annex may lead to interoperability issues when messaging contains user profile between HSS and S-CSCF.

Clauses affected:	⌘ Annex C							
Other specs affected:	⌘	<table border="1"><tr><td>Y</td><td>N</td></tr><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr></table>	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
	Y	N						
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>						
		<table border="1"><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr></table>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Test specifications			
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							
	<table border="1"><tr><td><input checked="" type="checkbox"/></td><td><input checked="" type="checkbox"/></td></tr></table>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	O&M Specifications				
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>							
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 *****

Annex C (informative): Conjunctive and Disjunctive Normal Form

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

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

Taking as an example the following trigger:

Method = "INVITE" OR Method = "MESSAGE" OR (Method="SUBSCRIBE" AND NOT Header = "from" Content = "joe")

The trigger can be split into the following atomic expressions:

Method="INVITE"

Method="MESSAGE"

Method="SUBSCRIBE"

NOT header="from" Content = "joe"

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

(Method="INVITE" OR Method = "MESSAGE" OR Method="SUBSCRIBE") AND (Method="INVITE" OR Method = "MESSAGE" OR (NOT Header = "from" Content = "joe"))

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

(Method="INVITE" OR Method = "MESSAGE" OR Method="SUBSCRIBE")

(Method="INVITE" OR Method = "MESSAGE" OR (NOT Header = "from" Content = "joe"))

The XML representation of the trigger is:

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

```

        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
    </SPT>
    <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>MESSAGE</Method>
    </SPT>
    <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>SUBSCRIBE</Method>
    </SPT>
    <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>1</Group>
        <Method>INVITE</Method>
    </SPT>
    <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>1</Group>
        <Method>MESSAGE</Method>
    </SPT>

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

```

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

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

Method="INVITE"

Method="MESSAGE"

Method="SUBSCRIBE" AND (NOT header="from" Content ="joe")

The XML representation of the trigger is:

```

<?xml version="1.0" encoding="UTF-8"?>
<testDatatype IMSSubscription xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="D:\ CxDataType.xsd">
    <IMSSubscription>
        <PrivateID>IMPI1@homedomain.com</PrivateID>
    </IMSSubscription>
</testDatatype>

```

```

<ServiceProfile>
  <PublicIdentity>
    <BarringIndication>1</BarringIndication>
    <Identity> sip:IMPU1@homedomain.com </Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity> sip:IMPU2@homedomain.com </Identity>
  </PublicIdentity>
  <InitialFilterCriteria>
    <Priority>0</Priority>
    <TriggerPoint>
      <ConditionTypeCNF>0</ConditionTypeCNF>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
      </SPT>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>1</Group>
        <Method>MESSAGE</Method>
      </SPT>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>2</Group>
        <Method>SUBSCRIBE</Method>
      </SPT>
      <SPT>
        <ConditionNegated>1</ConditionNegated>
        <Group>2</Group>
        <SIPHeader>
          <Header>From</Header>
          <Content>"joe"</Content>
        </SIPHeader>
      </SPT>
    </TriggerPoint>
    <ApplicationServer>
      <ServerName>sip:AS1@homedomain.com</ServerName>
      <DefaultHandling index="0">0</DefaultHandling>
    </ApplicationServer>
  </InitialFilterCriteria>
</ServiceProfile>
</IMSSubscription>
</testDatatype>

```

Seoul, KOREA. 15th to 19th November 2004.

CR-Form-v7.1

CHANGE REQUEST⌘ **29.228 CR 146** ⌘ 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:	⌘ Clarification of R6 authentication scheme		
Source:	⌘ CN4		
Work item code:	⌘ IMS-CCR2	Date:	⌘ 01/11/2004
Category:	⌘ F	Release:	⌘ Rel-6
	Use <i>one</i> 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 <i>one</i> 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:	⌘ Currently in the spec there is an explicit identification of the authentication scheme that is used in 3GPP R5, but no mention is made of R6.
Summary of change:	⌘ A clear statement of the authentication scheme used in R6 is added.
Consequences if not approved:	⌘ The inclusion of only a statement on R5 authentication leaves the question open as to what R6 authentication is (the same or different?)

Clauses affected:	⌘ 6.3, 7.9.2										
Other specs affected:	<table border="1"> <thead> <tr> <th>Y</th> <th>N</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Y	N	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N										
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>										
		Test specifications									
		O&M Specifications									
Other comments:	⌘										

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

Below is a brief summary:

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

- 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.

- Authentication procedures

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

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

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

Table 6.3.1: Authentication request

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

Table 6.3.2: Authentication Data content – request

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	This information element indicates the authentication scheme. For 3GPP R5 and 3GPP R6 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	C	User public identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity (See 7.3)	User-Name	C	User private identity. It shall be present when the result is DIAMETER_SUCCESS.
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	C	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	C	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	C	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 and 3GPP R6 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 contain binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentiality Key (See 7.9.5)	Confidentiality-Key	O	- 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.

- 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]):

- Check that the user exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.
- 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_I_MATCH.
- 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 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.
 - 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.

***** *Next Changed Section* *****

7.9.2 Authentication Scheme

This information element contains the authentication scheme, which is used to encode the authentication parameters.

~~For 3GPP Release 5 and 3GPP Release 6~~ The scheme is "Digest-AKA_{v1}-MD5".

CHANGE REQUEST

⌘ **29.228 CR 156** ⌘ 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:	⌘ Modification of User-Data-Already-Available in SAR command.		
Source:	⌘ CN4		
Work item code:	⌘ IMS2-CCR	Date:	⌘ 19/10/2004
Category:	⌘ F	Release:	⌘ Rel-6
	<i>Use one of the following categories:</i> 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 .		<i>Use one of the following releases:</i> 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:	⌘ The User-Data-Already-Available is only used by the HSS when there is potential for a User Profile download to the S-CSCF. For cases of de-registration, this AVP is not used and should not be included in the SAR command when this is reflected in the Server Assignment Type. Therefore the AVP should be defined as Conditional in the SAR command description.
Summary of change:	⌘ Change User-Data-Already-Available AVP to conditional in the SAR command. It shall be present when the User Profile may be downloaded as a result of the Server-Assignment-Type being NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER.
Consequences if not approved:	⌘ Unused AVP included in the SAR command when assignment type is other than being NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER.

Clauses affected:	⌘ 6.1.2										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="padding: 2px;">Y</td> <td style="padding: 2px;">N</td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> <tr> <td style="padding: 2px;"><input type="checkbox"/></td> <td style="padding: 2px;"><input checked="" type="checkbox"/></td> </tr> </table>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications Test specifications O&M Specifications	⌘
Y	N										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
<input type="checkbox"/>	<input checked="" type="checkbox"/>										
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	<p>If the S-CSCF knows the HSS name, the Destination-Host AVP shall be present in the command.</p> <p>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.</p> <p>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.</p>
-----------------------------------	------------------	---	--

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	<p>Private User Identity.</p> <p>It shall be present if it is available when the HSS sends the response.</p> <p>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.</p>
Registration result (See 7.6)	Result-Code / Experimental-Result	M	<p>Result of registration.</p> <p>Result-Code AVP shall be used for errors defined in the Diameter Base Protocol.</p> <p>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.</p>
User Profile (See 7.7)	User-Data	C	<p>Relevant user profile.</p> <p>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.</p> <p>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].</p>
Charging Information (See 7.12)	Charging-Information	C	<p>Addresses of the charging functions.</p> <p>It shall be present when the User-Data AVP is sent to the S-CSCF.</p> <p>When this parameter is included, the Primary Charging Collection Function address shall be included. All other elements shall be included if they are available.</p>

CR-Form-v7	
CHANGE REQUEST	
# 29.228 CR 140	# 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:	#	HSS initiated deregistration with user profile removal for permanent termination	
Source:	#	CN4	
Work item code:	#	IMS-CCR	Date: # 21/09/2004
Category:	#	F	Release: # REL-6
		Use <u>one</u> 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 <u>one</u> 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:	#	It is an essential correction.
		Currently, in TS 29.228, the HSS initiated deregistration does not mention that the user profile is deleted at the end of the procedure due to the subscription closing.
Summary of change:	#	In section 6.1.3.1 detailing the process for HSS initiated deregistration for "PERMANENT_TERMINATION" reason code, it is added that the user is no longer available for registration or terminating calls.
Consequences if not approved:	#	The user may be reachable or use his subscription while the IMS subscription is closed.

Clauses affected:	#	6.1.3								
Other specs affected:	#	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">#</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications # Test specifications # O&M Specifications #	Y	N	#	X	#	X	#	X
Y	N									
#	X									
#	X									
#	X									
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 ***

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 the user (only one public identity, one or more public identities or all the public identities registered) has to be de-registered.

The HSS may de-register:

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

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

- PERMANENT_TERMINATION: The IMS subscription or service profile(s) has been permanently terminated. The S-CSCF should start the network initiated de-registration towards the user. [The user is no longer available for registration or terminating calls in the HSS.](#) ~~The HSS shall delete the user profile for this 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.

*** END OF MODIFICATION ***