3GPP TSG-CN Meeting #25 **NP-040385**
8th – 10th September 2004. Palm Springs, USA.

Source: **TSG CN WG1**

Title: **CR on Rel-5 WI IMS-CCR towards TS 24.228 and TS 24.229**

Agenda item: **8.1**

Document for: **APPROVAL**

This document contains **9 CRs on Rel-5 Work Item "IMS-CCR"**, that have been agreed by TSG CN WG1 CN#35 meeting and forwarded to TSG CN Plenary meeting #25 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	Current version	WI	Rel
N1-041432	P-Charging-Vector header error correction	24.228	133		F	5.9.0	IMS-CCR	Rel-5
N1-041537	Syntax correction for the P-Charging-Vector header	24.229	672	1	F	5.9.0	IMS-CCR	Rel-5
N1-041434	Syntax correction for the P-Charging-Vector header	24.229	673		A	6.3.0	IMS-CCR	Rel-6
N1-041541	Missing value for the event attribute within the <contact> element of NOTIFY body	24.229	679	1	F	5.9.0	IMS-CCR	Rel-5
N1-041540	Missing value for the event attribute within the <contact> element of NOTIFY body	24.229	697		A	6.3.0	IMS-CCR	Rel-6
N1-041549	HSS initiated deregistration	24.229	698		F	6.3.0	IMS-CCR	Rel-6
N1-041552	Correction to condition for removal of the P- Access- Network-Info Header	24.229	694	1	F	5.9.0	IMS-CCR	Rel-5
N1-041628	Network initiated deregistration upon UE roaming and registration to a new network	24.229	681	2	F	5.9.0	IMS-CCR	Rel-5
N1-041629	Network initiated deregistration upon UE roaming and registration to a new network	24.229	699	1	F	6.3.0	IMS-CCR	Rel-6

3GPP TSG-CN1 Meeting #35 **Tdoc N1-041432**
Sophia Antipolis, France, 16-20 August 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.228** **CR** **133** ⌘ **rev** **-** ⌘ Current version: **5.9.0** ⌘

*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:	⌘	P-Charging-Vector header error correction
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	07/08/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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:	⌘	P-Charging-Vector header syntax has changed, the syntax left unchanged in one example.
Summary of change:	⌘	P-Charging-Vector header updated in that example
Consequences if not approved:	⌘	An erroneous example left in the specs.
Clauses affected:	⌘	7.2.3.1 – only part of the subclause is shown

	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.

Table 7.2.3.1-20: UPDATE (P-CSCF to S-CSCF)

```
UPDATE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.home1.net;branch=z9hG4bK431h23.1, SIP/2.0/UDP
     [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024";
   ggsn=[5555::4b4:3c3:2d2:1e1]; pdp-sig=no; gcid=723084371; auth-token=43876559; flow-id=3
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024";
   ggsn=[5555::4b4:3c3:2d2:1e1]; auth-token=2A96B3AF30D1; pdp-info="pdp-item=1; pdp-sig=no;
   gcid=A93D238CAF; flow-id=({1,1},{1,2}), pdp-item=2; pdp-sig=no; gcid=F312D5E3BC; flow-
   id=({2,1},{2,2})"
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Type:
Content-Length:

v=
o=
s=
c=
t=
m=
b=
a=
a=
a=
a=
a=
a=
m=
b=
a=
a=
a=
a=
a=
a=
a=
```

3GPP TSG-CN1 Meeting #35 **Tdoc N1-041434**
Sophia Antipolis, France, 16-20 August 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **673** ⌘ **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:	⌘	P-Charging-Vector header error correction
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	07/08/2004
Category:	⌘	**A**
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:	⌘	P-Charging-Vector header syntax limits the number of media to 9, the same restriction for number of flows within a media desciption.
Summary of change:	⌘	Restriction removed, multiple digits allowed
Consequences if not approved:	⌘	Parsers implemented strictly according to specs will introduce unnecessary restrictions.

Clauses affected:	⌘	B.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.

B.4.1 P-Charging-Vector header

The access network charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. Table B.1 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

Table B.1: Syntax of extensions to P-Charging-Vector header

```
   access-network-charging-info = (gprs-charging-info / generic-param)
   gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
   ggsn = "ggsn" EQUAL gen-value
   pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
   pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
   pdp-item = "pdp-item" EQUAL DIGIT
   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
   gcid = "gcid" 1*HEXDIG
   auth-token = "auth-token" EQUAL 1*HEXDIG
   flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
"}")")"
   extension-param = token [EQUAL token]
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks.

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameters that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid and flow-id parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface (see 3GPP TS 29.209 [13A]).

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.

For a dedicated PDP context for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go and Gq interfaces. Since there are no GCID, media authorization token or flow identifiers in this case, the GCID and media authorization token are set to zero and no flow identifier parameters are constructed by the PDF.

3GPP TSG-CN1 Meeting #35 **Tdoc N1-041537**
Sophia Antipolis, France, 16-20 August 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **672** ⌘ **rev** **1** ⌘ Current version: **5.9.0** ⌘

*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:	⌘	P-Charging-Vector header error correction
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	16/08/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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:	⌘	P-Charging-Vector header syntax limits the number of media to 9, the same restriction for number of flows within a media desciption.
Summary of change:	⌘	Restriction removed, multiple digits allowed
Consequences if not approved:	⌘	Message parsers will not remain compatible between Rel5 and Rel6 (the corresponding change for Rel6 is already agreed).
Clauses affected:	⌘	7.2A.5.2

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.

7.2A.5.2 Syntax

The P-Charging-Vector header field has the syntax described in RFC 3455 [52]. Table 7.3 describes extensions required for 3GPP to that syntax.

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
   access-network-charging-info = (gprs-charging-info / generic-param)
   gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
   ggsn = "ggsn" EQUAL gen-value
   pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
   pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
   pdp-item = "pdp-item" EQUAL DIGIT
   pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
   gcid = "gcid" EQUAL 1*HEXDIG
   auth-token = "auth-token" EQUAL 1*HEXDIG
   flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
"}")")"
   extension-param = token [EQUAL token]
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks.

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameters that contains the information for one or more PDP contexts. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a flow identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.207 [12] Annex C. The gcid and flow-id parameters are transferred from the GGSN to the P-CSCF (PDF) over the Go interface, see 3GPP TS 29.207 [12].

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before including it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.

For a dedicated PDP context for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go interface. Since there are no GCID, media authorization token or flow identifiers in this case, the GCID and media authorization token are set to zero and no flow identifier parameters are constructed by the P-CSCF/PDF.

3GPP TSG–CN1 Meeting #35
Sophia Antipolis, France, 16th to 20th August 2004

***Tdoc* ⌘N1-041540**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **697** ⌘**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: ⌘	Missing value for the event attribute within the <contact> element of NOTIFY body	
Source: ⌘	Orange	
Work item code: ⌘	IMS-CCR	***Date:*** ⌘ 16/08/2004
Category: ⌘	**A**	***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: ⌘	In RFC 3680, the rejected event occurs when an active contact is removed by the administrator not wishing the client to attempt to re-register the contact, e.g. if a user does not pay his bills. In TS 24.229, it is stated in section 5.4.1.5: "When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package." In TS 24.229 section 5.4.1.5, for each NOTIFY, if the public user identity has been deregistered, the S-CSCF shall "set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister". However, in section 5.4.2.1.2 dealing with general rules for notifications sent by the S-CSCF (initial and subsequent notifications), it is not possible to mark as "rejected" the event attribute in the <contact> element of the NOTIFY request.
Summary of change: ⌘	In section 5.4.2.1.2, the event attribute within the <contact> element may be set to "rejected" if a public user identity has been deregistered in accordance with RFC 3680 and section 5.4.1.5.
Consequences if not approved: ⌘	With the existing specification, implementation may assume that the rejected value is not used however the intention was to comply with the RFC 3680 which includes the value. Interoperability problem will result between the two

	interpretations.

Clauses affected:	⌘	5.4.2.1.2			
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 co

*** FIRST MODIFICATION ***

5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE; and

   b) if the public user identity:

      I) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according RFC 3680 [43]; or

      II) has been registered then:

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "registered"; or

      III) has been automatically registered:

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "created"; and

5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
               state="active">
    <contact id="76" state="active" event="registered">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
               state="active">
    <contact id="86" state="active" event="created">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #35
Sophia Antipolis, France, 16th to 20th August 2004

***Tdoc* ⌘N1-041541**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **679** ⌘**rev** **1** ⌘ Current version: **5.9.0** ⌘

*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:	⌘	Missing value for the event attribute within the <contact> element of NOTIFY body
Source:	⌘	Orange
Work item code:	⌘	IMS-CCR
Date:	⌘	16/08/2004
Category:	⌘	**F**
Release:	⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	In RFC 3680, the rejected event occurs when an active contact is removed by the administrator not wishing the client to attempt to re-register the contact, e.g. if a user does not pay his bills. In TS 24.229, it is stated in section 5.4.1.5: "When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package." In TS 24.229 section 5.4.1.5, for each NOTIFY, if the public user identity has been deregistered, the S-CSCF shall "set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister". However, in section 5.4.2.1.2 dealing with general rules for notifications sent by the S-CSCF (initial and subsequent notifications), it is not possible to mark as "rejected" the event attribute in the <contact> element of the NOTIFY request.
Summary of change:	⌘	In section 5.4.2.1.2, the event attribute within the <contact> element may be set to "rejected" if a public user identity has been deregistered in accordance with RFC 3680 and section 5.4.1.5.
Consequences if not approved:	⌘	With the existing specification, implementation may assume that the rejected value is not used however the intention was to comply with the RFC 3680 which includes the value. Interoperability problem will result between the two

	interpretations.

Clauses affected:	⌘	5.4.2.1.2			
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 co

*** FIRST MODIFICATION ***

5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE; and

   b) if the public user identity:

      I) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according RFC 3680 [43]; or

      II) has been registered then:

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "registered"; or

      III) has been automatically registered:

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "created"; and

5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
               state="active">
    <contact id="76" state="active" event="registered">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
               state="active">
    <contact id="86" state="active" event="created">
          <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #35
Sophia Antipolis, France, 16th to 20th August 2004

***Tdoc* ⌘N1-041549**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **698** ⌘**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:	⌘	HSS initiated deregistration
Source:	⌘	Orange
Work item code:	⌘	IMS-CCR
Date:	⌘	16/08/2004
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)

Reason for change: ⌘

In TS 23.228 section 5.3.2.2, it is required that the HSS can initiate the network de-registration.

"For different reasons (e.g., subscription termination, lost terminal, etc.) a home network administrative function may determine a need to clear a user's SIP registration. This function initiates the de-registration procedure and may reside in various elements depending on the exact reason for initiating the de-registration.

One such home network element is the HSS, which already knows the S-CSCF serving the user and that for this purpose makes use of the Cx-Deregister."

In TS 24.229 section 5.4.1.5, the network initiated deregistration applies to the case when a "deregistration event occurs" at the S-CSCF.

It is clear that this procedure can apply if an internal de-registration event occurs at the S-CSCF (e.g. expiration of the registration timer at the S-CSCF). However, it is not clearly stated that the network initiated deregistration can be triggered by the S-CSCF due to a request from the HSS.

Summary of change: ⌘

The network initiated deregistration includes the HSS initiated deregistration.

This procedure shall be triggered when the S-CSCF receives from the HSS an indication of deregistration (for administrative reason e.g. subscription expiration, lost terminal).

Consequences if not approved: ⌘

Clarification that the network initiated deregistration can be originated by the HSS.

	Misalignment with TS 23.228

Clauses affected:	⌘	5.4.1.5			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	
			Test specifications		
			O&M Specifications		
Other comments:	⌘				

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

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

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

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

*** FIRST MODIFICATION ***

5.4.1.5 Network-initiated deregistration

Note: a network-initiated deregistration event that occurs at the S-CSCF may be received from the HSS or may be an internal event in the S-CSCF.

Prior to initiating the network-initiated deregistration for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) while there are still active multimedia sessions belonging to this UE, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity that were registered by this UE, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF may release all remaining dialogs related to the public user identity being deregistered and shall generate a NOTIFY request on all remaining dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) if the public user identity:

      i) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

         I) set the state attribute within the <registration> element to "active";

         II) set the state attribute within the <contact> element to:

            - for the contact address to be removed set the state attribute within the <contact> element to "terminated", and event attribute element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

            - for the contact address which remain unchanged, if any, leave the <contact> element unmodified; and

NOTE 1: There might be more then one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user identitity, if registered by another UE using different private user identities remain unchanged.

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event.

On completion of the above procedures for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

*** END OF MODIFICATION ***

3GPP TSG-CN1 Meeting #35 **Tdoc N1-041552**
Sophia Antipolis, France, 16-20 August 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **694** ⌘ **rev** **1** ⌘ Current version: **5.9.0** ⌘

*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 condition for removal of the P- Access- Network-Info Header
Source:	⌘	Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	12/07/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	The conditions under which the P-Access-Network-Info header are removed are not clearly defined. The current condition described in sec 5.4.3.2, step 13 does not make it clear if the removal of the P-Access-Network-Info header depends upon the destination user, or that the forwarding of the message depends upon the destination user.
Summary of change:	⌘	The text in 5.4.3.2 is modified to clearly identify the true intention of step 13.
Consequences if not approved:	⌘	Ambiguity in the text remains which could lead to incorrect implementation and behaviour. This in turn could lead to secure information (such as about the network topology) being exposed to entities beyond the trust domain of the S-CSCF.

Clauses affected:	⌘	5.4.3.2

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.

5.4.3.2 Requests initiated by the served user

When the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399. Otherwise, continue with the rest of the steps;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

2) remove its own SIP URI from the topmost Route header;

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;

4) check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header, and if it does, forward this request to that AS, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted AS as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI. In case of contacting one or more AS(s) the S-CSCF shall:

   a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and

   b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values in the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values in the request that is forwarded to the AS;

5) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

6) insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;

7) insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

8) in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI;

11) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

12) in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URI;

13) if the destination user (Request-URI) lies outside of the trust domain of the S-CSCF, remove the P-Access-Network-Info header, prior to forwarding the message~~remove the P-Access-Network-Info header prior to forwarding the message based on the destination user (Request-URI)~~;

14) route the request based on SIP routeing procedures; and

15) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives any response to the above request, the S-CSCF may:

1) apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header.

NOTE 2: This header would normally only be expected in 1xx or 2xx responses.

NOTE 3: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) create a Record-Route header containing its own SIP URI;

3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

4) in case the request is routed towards the destination user (Request-URI)or is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

5) route the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

1) remove its own URI from the topmost Route header;

2) in case the request is routed towards the destination user (Request-URI)or is routed to an AS located outside the trust domain, remove the P-access-network-info header; and

3) route the request based on the topmost Route header.

3GPP TSG–CN1 Meeting #35
Sophia Antipolis, France, 16th to 20th August 2004

***Tdoc* ⌘N1-041628**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **681** ⌘**rev** **2** ⌘ Current version: **5.9.0** ⌘

*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:	⌘	Network initiated deregistration upon UE roaming and registration to a new network
Source:	⌘	Orange
Work item code:	⌘	IMS-CCR
Date:	⌘	20/08/2004
Category:	⌘	**F**
Release:	⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

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

Reason for change: ⌘ In TS 23.228 section 5.3.2, it is required that the network can initiate the user deregistration in case the UE registers in a new network without deregistering in the old network.

Network/traffic determined reason:
"The IM CN subsystem must support a mechanism to avoid duplicate registrations or inconsistent information storage. This case will occur when a user roams to a different network without de-registering the previous one. This case may occur at the change of the roaming agreement parameters between two operators, imposing new service conditions to roamers."

TS 24.228 contains such a flow example (section 6.7.3).

"When the UE starts registration in via the new visited access network and P-CSCF, the home S-CSCF in the home IMS network initiates the deregistration to the P-CSCF in the previous visited network. It is assumed that the old P-CSCF has subscribed the event package to the S-CSCF and the subscription has not expired."

However, it is not clearly stated in TS 24.229 that the S-CSCF shall perform the network initiated de-registration procedure for the previous contact information.

Summary of change: ⌘ In section 5.4.1.2.1, the handling at the S-CSCF when the S-CSCF receives a new unprotected registration request for an already registered public user identity linked to the same private user identity but with a new contact information is added.

In section 5.4.1.5, an editor note is added to indicate that the procedure shall be

		improved for the case when the UE is roaming, registration is done in a new network and the previous registration has not expired.
Consequences if not approved:	⌘	Misalignment with TS 23.228 Inconsistency with TS 24.228 Registration information still present for the previous contact information.

Clauses affected:	⌘	5.4.1.2.1, 5.4.1.5			
Other specs affected:	⌘	Y / N	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 ***

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected by the UE is considered to be an initial registration. A 200 (OK) final response to such a request will only be sent back after the S-CSCF receives a correct authentication challenge response in a REGISTER request that is sent integrity protected.

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

When the S-CSCF receives a new unprotected registration request for an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

1) perform the procedure for 'receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated de-registration procedure only for the previous contact information as described in subclause 5.4.1.4.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3 select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE 3: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) store the icid parameter received in the P-Charging-Vector header;

5) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:

- the home network identification in the realm field;
- the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
- the security mechanism, which is AKAv1-MD5, in the algorithm field;
- the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and
- the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);

6) store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

7) send the so generated 401 (Unauthorized) response towards the UE; and,

8) start timer reg-await-auth which guards the receipt of the next REGISTER request.

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

1) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2) stop timer reg-await-auth;

3) check whether an Authorization header is included, containing:

   a) the private user identity of the user in the username field;

   b) the algorithm which is AKAv1-MD5 in the algorithm field; and

   c) the authentication challenge response needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

   a) the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

9) store the icid parameter received in the P-Charging-Vector header;

10) create a 200 (OK) response for the REGISTER request, including:

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that the user is authorized to use. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

- the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,

- if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry; and

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

11) send the so created 200 (OK) response to the UE;

12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

13) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.3 Abnormal cases

In the case that the authentication challenge response from the UE does not match with the expected authentication challenge response and the request has the "integrity-protected" parameter in the Authentication header set to "yes", the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration time of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no authentication challenge response and no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration time of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an authentication challenge response indicates that the authentication challenge was invalid (contains the AUTS parameter indicating this), the S-CSCF will fetch new authentication vectors from the HSS. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS received from the UE and the stored RAND when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or

- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned.

NOTE 3: Since the UE responds only to two consecutive challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

NOTE 4: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in 3GPP TS 33.203 [19]. The operator's policy will specify when will, upon authentication failure, the currently registered public user identity or the user be de-registered by the S-CSCF.

*** END OF FIRST MODIFICATION ***

*** SECOND MODIFICATION ***

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) while there are still active multimedia sessions belonging to this user, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF shall release all remaining dialogs related to the public user identity being deregistered and shall generate a NOTIFY request on all remaining

dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) if the public user identity:

      i) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

         - set the state attribute within the <registration> element to "active"; and

         - set the state attribute within the <contact> element to "active"; and

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event.

On completion of the above procedures in this subclause for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

Editor's note: this procedure shall be improved for the case of de-registration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired.

*** END OF SECOND MODIFICATION ***

3GPP TSG–CN1 Meeting #35
Sophia Antipolis, France, 16th to 20th August 2004

***Tdoc* ⌘N1-041629**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **699** ⌘**rev** **1** ⌘ 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:	⌘	Network initiated deregistration upon UE roaming and registration to a new network
Source:	⌘	Orange
Work item code:	⌘	IMS-CCR
Date:	⌘	20/08/2004
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)*

Reason for change: ⌘ In TS 23.228 section 5.3.2, it is required that the network can initiate the user deregistration in case the UE registers in a new network without deregistering in the old network.

Network/traffic determined reason:
"The IM CN subsystem must support a mechanism to avoid duplicate registrations or inconsistent information storage. This case will occur when a user roams to a different network without de-registering the previous one. This case may occur at the change of the roaming agreement parameters between two operators, imposing new service conditions to roamers."

TS 24.228 contains such a flow example (section 6.7.3).

"When the UE starts registration in via the new visited access network and P-CSCF, the home S-CSCF in the home IMS network initiates the deregistration to the P-CSCF in the previous visited network. It is assumed that the old P-CSCF has subscribed the event package to the S-CSCF and the subscription has not expired."

However, it is not clearly stated in TS 24.229 that the S-CSCF shall perform the network initiated de-registration procedure for the previous contact information.

Summary of change: ⌘ In section 5.4.1.2.1, the handling at the S-CSCF when the S-CSCF receives a new unprotected registration request for an already registered public user identity linked to the same private user identity but with a new contact information is added.

In section 5.4.1.5, an editor note is added to indicate that the procedure shall be improved for the case when the UE is roaming, registration is done in a new

		network and the previous registration has not expired.
Consequences if not approved:	⌘	Misalignment with TS 23.228 Inconsistency with TS 24.228 Registration information still present for the previous contact information.

Clauses affected:	⌘	5.4.1.2.1, 5.4.1.5			
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 co

*** FIRST MODIFICATION ***

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected by the UE is considered to be an initial registration. A 200 (OK) final response to such a request will only be sent back after the S-CSCF receives a correct authentication challenge response in a REGISTER request that is sent integrity protected.

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

When the S-CSCF receives a new unprotected registration request for an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

1) perform the procedure for 'receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated de-registration procedure only for the previous contact information as described in subclause 5.4.1.4.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE 3: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

4) store the icid parameter received in the P-Charging-Vector header;

5) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:

   - the home network identification in the realm field;
   - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
   - the security mechanism, which is AKAv1-MD5, in the algorithm field;
   - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and
   - the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);

6) store the RAND parameter used in the 401 (Unathorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

7) send the so generated 401 (Unauthorized) response towards the UE; and,

8) start timer reg-await-auth which guards the receipt of the next REGISTER request.

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

1) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2) stop timer reg-await-auth;

3) check whether an Authorization header is included, containing:

   a) the private user identity of the user in the username field;

   b) the algorithm which is AKAv1-MD5 in the algorithm field; and

   c) the authentication challenge response needed for the authentication procedure in the response field.

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

   a) the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

9) store the icid parameter received in the P-Charging-Vector header;

10) create a 200 (OK) response for the REGISTER request, including:

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that the user is authorized to use. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

- the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,

- if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry; and

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;

11) send the so created 200 (OK) response to the UE;

12) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

13) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.3 Abnormal cases

In the case that the authentication challenge response from the UE does not match with the expected authentication challenge response and the request has the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration state of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no authentication challenge response and no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration state of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an authentication challenge response indicates that the authentication challenge was invalid (contains the AUTS parameter indicating this), the S-CSCF will fetch new authentication vectors from the HSS. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS received from the UE and the stored RAND, when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or

- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned. The S-CSCF shall not update the registration state of the subscriber.

NOTE 3: If the UE was registered before, it stays registered until the registration expiration time expires.

NOTE 4: Since the UE responds only to two consecutive invalid challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

NOTE 5: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in 3GPP TS 33.203 [19].

*** END OF FIRST MODIFICATION ***

*** SECOND MODIFICATION ***

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) while there are still active multimedia sessions belonging to this UE, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity that were registered by this UE, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the reg event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF may release all remaining dialogs related to the public user identity being deregistered and shall generate a

NOTIFY request on all remaining dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) if the public user identity:

      i) has been deregistered then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within the <contact> element to "terminated"; and

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

         I) set the state attribute within the <registration> element to "active";

         II) set the state attribute within the <contact> element to:

            - for the contact address to be removed set the state attribute within the <contact> element to "terminated", and event attribute element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

            - for the contact address which remain unchanged, if any, leave the <contact> element unmodified; and

NOTE 1: There might be more then one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user identitity, if registered by another UE using different private user identities remain unchanged.

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS for the REGISTER event.

On completion of the above procedures for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

Editor's note: this procedure shall be improved for the case of de-registration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired and the case of de-registration of a contact information when multiple UEs are using the same public user identity and one of these UEs is de-registered.

*** END OF SECOND MODIFICATION ***