3GPP TSG CN Plenary Meeting #19 **NP-030051**
12th - 14th March 2003. Birmingham, U.K.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.229,- pack 3**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **9** CRs, **Rel-5 to** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #19 for approval.

Spec	CR	Rev	Cat	Phase	Subject	Version-Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.229	311	1	F	Rel-5	P-CSCF handling of established dialogs upon registration-lifetime expiration	5.3.0	5.4.0	N1-28	N1-030235
24.229	312	1	F	Rel-5	Correction of Authentication procedure	5.3.0	5.4.0	N1-28	N1-030240
24.229	313		F	Rel-5	Mixed Path header and Service-Route operation	5.3.0	5.4.0	N1-28	N1-030127
24.229	315	2	F	Rel-5	Clarifications on updating the authorization token	5.3.0	5.4.0	N1-28	N1-030255
24.229	318	2	F	Rel-5	Consideration of P-CSCF/PDF	5.3.0	5.4.0	N1-28	N1-030307
24.229	319	2	F	Rel-5	Clarification on GPRS charging information	5.3.0	5.4.0	N1-28	N1-030308
24.229	323	1	F	Rel-5	P-Access-Network-Info procedure corrections for the UE	5.3.0	5.4.0	N1-28	N1-030250
24.229	324	1	F	Rel-5	P-Access-Network-Info procedure corrections for the S-CSCF	5.3.0	5.4.0	N1-28	N1-030251
24.229	326	1	F	Rel-5	Updating user agent related profile tables	5.3.0	5.4.0	N1-28	N1-030260

3GPP TSG-CN1 Meeting #28 ***Tdoc N1-030235***
Dublin, Ireland, 10 – 14 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **CR 311** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*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-CSCF handling of established dialogs upon registration-lifetime expiration
Source:	⌘	Lucent
Work item code:	⌘	**IMS-CCR**
Date:	⌘	***10/02/2003***
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:	⌘	Currently the document 24.229 does not specify the action that the P-CSCF should take when all public user identities have been deregistered and there are still active dialogs associated with the user.
Summary of change:	⌘	Relevant text added.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	propose 5.2.2

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

Other comments:	⌘	Revision 1 incorporates all modifications requested by the CN1 WG.

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.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

1) insert a Path header in the request including an entry containing:

   - the SIP URL identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) are expected to be treated as for the mobile-terminating case. This indication may e.g. be in a parameter in the URL, a character string in the user part of the URL, or be a port number in the URL;

2) insert a Require header containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header (see subclause 7.2.5);

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was received integrity protected, otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the ‘sec-agree’ item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

   - check the security association which protected the request. If that has a temporary lifetime, then the request shall contain a Security-Verify header. If there is no such header, then the P-CSCF shall return a suitable 4xx error code. If there is such header, then compare the content of the Security-Verify header with the local static list. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify header, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;

   - if the security association the REGISTER request came is an established one, then a Security-Verify header is not expected to be included. If the Security-Verify header is present, then the P-CSCF shall remove that header together with the 'Require: sec-agree' header; and

   - check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

7) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security association. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

2) insert the Security-Server header in the response, containing the P-CSCF static security list. For further information see 3GPP TS 33.203 [19]; and

3) set up the security association with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and draft-sip-sec-agree [48]. The P-CSCF shall set the SIP level lifetime of the security association to be long enough to permit the UE to finalize the registration procedure (bigger than 64*T1). The P-CSCF shall set the IPSec level lifetime of the security association to the maximum.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

4) store the default public user identity for use with procedures for the P-Asserted-Identity. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 1: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) update the SIP level lifetime of the security association with the value found in the Expires header;

7) protect the response within the same security association to that in which the associated requestwas protected;

8) delete all earlier security associations and related keys it may have towards the UE, when a message protected within the newly set up security association is received; and

9) delete the new security associations that it was trying to establish with the UE, in case the P-CSCF receives a message from the UE protected with the old security association.

NOTE 2: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPSec database when their SIP level lifetime expires. If there are still active dialogs associated with the user –after the security associations were deleted,– the P-CSCF shall ~~silently~~ discard all information pertaining to these dialogs without performing any further SIP transactions with the peer entities of the P-CSCF.

NOTE 3: At the same time, the P-CSCF will also indicate via the Go interface that the all resources associated with these dialogs should be released..

3GPP TSG-CN1 Meeting #28
Dublin, Ireland, 10 – 14 February 2003

Tdoc N1-030240
(rev of Tdoc N1-030105)

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **312** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction of Authentication procedure
Source:	⌘	Siemens
Work item code:	⌘	IMS-CCR
Date:	⌘	22/01/2003
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:	⌘	Description of Authentication procedure is incorrect
Summary of change:	⌘	During Authentication procedure first AUTN and RAND have to be extracted, then validation of the AUTN is performed and thereafter the parameters CK, IK and RES are derived
Consequences if not approved:	⌘	Authentication procedure in 24.229 described incorrectly

Clauses affected:	⌘	5.1.1.5.1

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

Other comments: ⌘

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

********** First Modified Section **********

Abbreviations

For the purposes of the present document, the following abbreviations apply:

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
APN	Access Point Name
AUTN	Authentication TokeN
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional
CCF	Charging Collection Function
CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTD	Document Type Definition
ECF	Event Charging Function
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
i	irrelevant
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia core network Subsystem
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP multimedia Subsystem Service Control
ISIM	IMS Suscriber Identity Module
m	mandatory
MAC	Message Authentication Code
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Media Gateway
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
n/a	not applicable
NAI	Netework Access Identifier
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF

SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Universal Resource Identifier
URL	Universal Resource Locator
USIM	UMTS Subscriber Identity Module
x	prohibited
XMAC	expected MAC
XML	eXtensible Markup Language

********** **Next Modified Section** **********

Authentication

5.1.1.5.1 General

Authentication is achieved via the registration and re-registration procedures. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

- extract the RAND and AUTN parameters

- check the validity of a received authentication challenge, as described in 3GPP TS 33.102 [18] i.e. the locally calculated MAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

- check the existence of the Security-Server header as described in draft-sip-sec-agree [48]. If the header is not present, the UE shall send a new REGISTER request.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

- ~~extract the RAND and AUTN parameters, and derive~~ calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203[19];

- set up the security association based on the static list it received in the 401 (Unauthorized) and its capabilities sent in the Security-Client header in the REGISTER request. The UE shall set up the security association using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using CK and IK as shared keys; and

- send another REGISTER request using the derived IK to integrity protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter). Instead of the Security-Client header the UE shall insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) for the integrity protected REGISTER request, the UE shall start using the security association the 200 (OK) was protected with.

Whenever the 200 (OK) response is not received after a time-out, the UE shall consider the registration to have failed. The UE shall delete the new security associations it was trying to establish, and use the old security association.

In the case that the 401 (Unauthorized) response is deemed to be invalid then the UE shall behave as defined in subclause 5.1.1.5.3.

3GPP TSG-CN1 Meeting #28 ***Tdoc N1-030127***
Dublin, Ireland, 10 – 14 February 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **313** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

*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 **X**

Title:	⌘	Mixed Path header and Service-Route operation
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	31/01/03
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 UE builds a preloaded Route header upon the contents received in the Service-Route (at registration). The Service-Route header shall contain the indication of mobile originating or mobile terminating side. Currently the text refers to the Path header instead of the Service-Route. This comes from long time ago when the Path header was bidirectional. But now the Path header is unidirectional only. The Service-Route is used to convey information from the registrar to the UE instead.
Summary of change:	⌘	Path is replaced by Service-Route
Consequences if not approved:	⌘	Wrong operation according to the relevant IETF standards. Incongruent text according to the text written in 5.4.1.2

Clauses affected:	⌘	5.4.3.1

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.

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the S-CSCF shall:

- perf`orm the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the ~~Path~~ Service-Route header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

3GPP TSG-CN1 Meeting #28 ***Tdoc N1-030255***
Dublin, Ireland, 10-14 February, 2003 **rev. of N1-030131 and N1-030215**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **315** ⌘ **rev** **2** ⌘ Current version: **5.3.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Clarifications on using Authorization token
Source:	⌘	NEC Corporation
Work item code:	⌘	IMS-CCR
Date:	⌘	05/02/2003
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 current text is not described clearly the same authorization token is used when the additional QoS authorization is necessary after the initial decision of authorization token.
Summary of change:	⌘	It is clarified that the media authorization token is always the same when any subsequent SDP is received at P-CSCF and need to be authorized during offer/answer session.
Consequences if not approved:	⌘	Wrong implementation.

Clauses affected:	⌘	5.2.7

		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.

Start of change

5.2.7 Initial INVITE

5.2.7.1 Introduction

In addition to following the procedures for initial requests defined in subclause 5.2.6, initial INVITE requests also follow the procedures of this subclause.

5.2.7.2 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response (e.g. 183 (Session Progress), 200 (OK)) to the initial INVITE request, the P-CSCF:

- if a media authorization token is generated by the PDF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated.

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the URL of the UE in the Request-URI, and a single preloaded Route header. The received initial INVITE request will also have a list of Record-Route headers. Prior to forwarding the initial INVITE to the URL found in the Request-URI, the P-CSCF shall:

- if a media authorization token is generated by the PDF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. . The same media authorization token is used until the session is terminated.

In addition, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

When the P-CSCF sends 180 (Ringing) or 200 (OK) (to INVITE) towards the S-CSCF, the P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

End of change

3GPP TSG-CN1 Meeting #28 ***Tdoc N1-030307***
Dublin, Ireland, 10-14 February, 2003 **rev. of N1-030134 and 264**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **318** ⌘ **rev** **2** ⌘ Current version: **5.3.0** ⌘

*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:	⌘	Consideration of P-CSCF/PDF
Source:	⌘	NEC Corporation
Work item code:	⌘	IMS-CCR
Date:	⌘	05/02/2003
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 Rel5, several sentences are ambiguous regarding procedure of policy control information or gprs charging information due to the requirement of the colocation of PDF and P-CSCF. However, Rel 5 29. 207 is already taken into account the separation of P-CSCF/PDF. Thus, from Rel 5, it is neccesary to change the several sentences as shown below because of the alignment with 29.207 and readability of users. (1) In 4.5.1 overview, it is modified to explain this requirement. (2) In 4.5.3, it needs to modify the several sentences, by reflecting the above requirement. (3) In 7.2.6.2, it is also necessary to change the several sentences, being aligned with the above requirements.
Summary of change:	⌘	It is added the above modifications shown in the column of reason for change.
Consequences if not approved:	⌘	24.229 remains misalighed with 29.207 and may be wrongly implemented.

Clauses affected:	⌘	4.5.1, 4.5.3, 4.5.3.3, 7.2.6.2

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.

Start of first Change

4.5 Charging correlation principles for IM CN subsystems

4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in clause 5. See 3GPP TS 32.200 [16] and 3GPP TS 32.225 [17] for further information on charging. The interface between the PDF and P-CSCF is not defined in this release.
The IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IM CN subsystem Charging Identifier (ICID);
2. Access network information:
   a. ~~a.~~ GPRS Charging Information;
3. Inter Operator Identifier (IOI);
4. Charging function addresses:
   a. Charging Collection Function (CCF);
   b. Event Charging Function (ECF).

How to use and where to generate the parameters in IM CN subsystems are described further in the subclauses that follow. The charging correlation information is encoded in the P-Charging-Vector header as defined in subclause 7.2. The P-Charging-Vector header contains the following parameters: icid, access network information and ioi.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in subclause 7.2. The P-Charging-Function-Addresses header contains the following parameters: CCF and ECF.

4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems.

The first IM CN subsystem entity involved in a dialog (session) or standalone (non-session) method will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. See 3GPP TS 32.225 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for mobile-originated calls. The I-CSCF will generate an ICID for mobile-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header. This ICID is valid for the duration of the registration and is associated with the signalling PDP context.

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF/PDF to the GGSN, but the ICID is not passed to the SGSN. The interface supporting this operation is outside the scope of this document.

4.5.3 Access network information

4.5.3.1 General

The access network information are the media component level data shared among the IM CN subsystem entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and PDP context information) is an example of access network information.

4.5.3.2 GPRS charging information

The GGSN provides the GPRS charging information to the IM CN subsystem, which is the common information used to correlate GGSN CDRs with IM CN subsystem CDRs.

The GPRS charging information is generated at the first opportunity after the resources are allocated at the GGSN. The GPRS charging ingormation is passed from GGSN to P-CSCF/PDF. GPRS charging information will be updated with new information during the session as media streams are added or removed. The P-CSCF provides the GPRS charging information to the S-CSCF. The S-CSCF may also pass the information to an AS, which may be needed for online pre-pay applications. The GPRS charging information for the originating network is used only within that network, and similarly the GPRS charging information for the terminating network is used only within that network. Thus the GPRS charging information are not shared between the calling and called networks. The GPRS charging information is not passed towards the external ASs from its own network.

The GPRS charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. The details of the gprs-charging-info parameter is described in subclause 7.2.6.

4.5.4 Inter operator identifier (IOI)

The Inter Operator Identifier (IOI) is a globally unique identifier to share between operator networks/service providers/content providers. There are two possible instances of an IOI to be exchanged between networks/service providers/content providers: one for the originating side, orig-ioi, and one for the terminating side, term-ioi.

The S-CSCF in the originating network populates the orig-ioi parameter of the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. Also in the initial request, the term-ioi parameter is left out of the P-Charging-Vector parameter. The S-CSCF in the originating network retrieves the term-ioi parameter from the P-Charging-Vector header within the message sent in response to the initial request, which identifies the operator network from which the response was sent.

The S-CSCF in the terminating network retrieves the orig-ioi parameter from the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. The S-CSCF in the terminating network populates the term-ioi parameter of the P-Charging-Vector header in the response to the initial request, which identifies the operator network from which the response was sent.

The MGCF takes responsibility for populating the orig-ioi parameter when a call/session is originated from the PSTN/PLMN. The MGCF takes responsibility for populating the term-ioi parameter when a call/session is terminated at the PSTN/PLMN.

IOIs will not be passed along within the network, except when proxied by BGCF and I-CSCF to get to MGCF and S-CSCF. However, IOIs will be sent to the AS for accounting purposes.

4.5.5 Charging function addresses

Charging function addresses are distributed to each of the IM CN subsystem entities in the home network for one side of the session (either the calling or called side) and are to provide a common location for each entity to send charging information. Charging Collection Function (CCF) addresses are used for offline billing. Event Charging Function (ECF) addresses are used for online billing.

There may be multiple addresses for CCF and ECF addresses populated into the P-Charging-Function-Addresses header of the SIP request or response. The parameters are ccf and ecf. Only one instance of ccf is required. Additional ccf addresses may be included by each network for redundancy purposes, but the first instance of ccf is the primary address. If ecf address is included for online charging, then additional instances may also be included for redundancy.

The CCF addresses and ECF addresses are retrieved from an HSS via the Cx interface and passed by the S-CSCF to subsequent entities. The charging function addresses are passed from the S-CSCF to the IM CN subsystem entities in its home network, but are not passed to the visited network or the UE. When the P-CSCF is allocated in the visited network, then the charging function addresses are obtained by means outside the scope of this document. The AS receives the charging function addresses from the S-CSCF via the ISC interface. CCF and/or ECF addresses may be allocated as locally preconfigured addresses. The AS may also retrieve the charging function address from the HSS via Sh interface.

End of first Change

Start of second Change

7.2.6.2 Syntax

The P-Charging-Vector header field has the syntax described in draft-garcia-sipping-3gpp-p-headers [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 pdp-info) [SEMI extension-param]
ggsn = "ggsn" EQUAL gen-value
pdp-info = pdp-sig SEMI gcid SEMI auth-token *(SEMI flow-id)
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "gcid" EQUAL gen-value
auth-token = "auth-token" EQUAL gen-value
flow-id = "flow-id" EQUAL gen-value
extension-param = token [EQUAL (token | quoted-string)]
```

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) and one or more PDP contexts (pdp-info parameter). 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), a media authorization token (auth-token parameter) and one or more flow identifiers (flow-id parameter) that identify associated m-lines within the SDP from the SIP signalling. These parameters are transferred from the GGSN to the P-CSCF (PDF) over the Go interface, see 3GPP TS 29.207[12].

For a PDP context that is only used for SIP signalling, i.e. no media stream requested ~~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.

7.2.6.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

7.2.7 Void

7.2.8 Void

7.2.9 P-Asserted-Identity header

7.2.9.1 Introduction

The P-Asserted-Identity header is the mechanism whereby the first element in the trust domain (see subclause 4.4) may assert a public user identity identifying the user. The P-Asserted-Identity header can also be used as a hint to the first element in the trust domain when it selects the asserted public user identity.

The header is inserted at the first opportunity when initialising dialogs and with standalone transactions. The header may be included in requests and responses.

End of second Change

3GPP TSG-CN1 Meeting #28 ***Tdoc N1-030308***
Dublin, Ireland, 10-14 February, 2003 **rev. of N1-030135 and 265**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **319** ⌘ **rev** **2** ⌘ Current version: **5.3.0** ⌘

*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 **X**

Title:	⌘	Clarification on GPRS charging information
Source:	⌘	NEC Corporation
Work item code:	⌘	IMS-CCR
Date:	⌘	05/02/2003
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:	⌘	1. In 4.5, there is misalignment on the terminology of access network charging with other subclause. 2. GPRS charging information is only used for correlation between bearer (PDP context) and session. Correlation between IP flow and session is not supported in this version of the document. 3. Other minor changes are proposed.
Summary of change:	⌘	The above changes are proposed.
Consequences if not approved:	⌘	For IMS charging mechanism, it may not work properly.

Clauses affected:	⌘	4.5.3, 7.2.6

		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.

Start of first change

4.5 Charging correlation principles for IM CN subsystems

4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in clause 5. See 3GPP TS 32.200 [16] and 3GPP TS 32.225 [17] for further information on charging.

The IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IM CN subsystem Charging Identifier (ICID);
2. Access network information:
   a. GPRS Charging Information;
3. Inter Operator Identifier (IOI);
4. Charging function addresses:
   a. Charging Collection Function (CCF);
   b. Event Charging Function (ECF).

How to use and where to generate the parameters in IM CN subsystems are described further in the subclauses that follow. The charging correlation information is encoded in the P-Charging-Vector header as defined in subclause 7.2. The P-Charging-Vector header contains the following parameters: icid, access network information and ioi.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in subclause 7.2. The P-Charging-Function-Addresses header contains the following parameters: CCF and ECF.

4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems.

The first IM CN subsystem entity involved in a dialog (session) or standalone (non-session) method will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. See 3GPP TS 32.225 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for mobile-originated calls. The I-CSCF will generate an ICID for mobile-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header. This ICID is valid for the duration of the registration and is associated with the signalling PDP context.

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF/PDF to the GGSN, but the ICID is not passed to the SGSN. The interface supporting this operation is outside the scope of this document.

4.5.3 Access network charging information

4.5.3.1 General

The access network charging information are the media ~~component~~ flow level data shared among the IM CN subsystem entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and PDP context information) is an example of access network charging information.

4.5.3.2 GPRS charging information

The GGSN provides the GPRS charging information to the IM CN subsystem, which is the common information used to correlate GGSN CDRs with IM CN subsystem CDRs. The GPRS charging information is used to correlate the bearer level (i.e. PDP context) with session level.

The GPRS charging information is generated at the first opportunity after the resources are allocated at the GGSN. The GPRS charging ingormation is passed from GGSN to P-CSCF/PDF. GPRS charging information will be updated with new information during the session as media ~~streams~~ flows are added or removed. The P-CSCF provides the GPRS charging information to the S-CSCF. The S-CSCF may also pass the information to an AS, which may be needed for online pre-pay applications. The GPRS charging information for the originating network is used only within that network, and similarly the GPRS charging information for the terminating network is used only within that network. Thus the GPRS charging information are not shared between the calling and called networks. The GPRS charging information is not passed towards the external ASs from its own network.

The GPRS charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. The details of the gprs-charging-info parameter is described in subclause 7.2.6.

End of first change

3GPP TSG-CN1 Meeting #28
Dublin, Ireland, 10 – 14 February 2003

Tdoc N1-030250

revision of ***Tdoc N1-030156***

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **323** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*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-Access-Network-Info procedure corrections for the UE
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	03/01/2003
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:	⌘	Currently clause 5.1.2A specifies that the P-Access-Network-Info header should be included in all requests and responses. RFC 3455 does not define it as applicable for ACK and CANCEL methods, and there is no benefit to 3GPP in using it on these methods.
Summary of change:	⌘	• The ACK and CANCEL methods are explicitly excluded from the requests and responses in which the P-Access-Network-Info header can be included. • The text in clause 7 is made descriptive, because clause 5 already contains these requirements fully detailed.
Consequences if not approved:	⌘	Inconsistency with IETF RFCs.

Clauses affected:	⌘	5.1.2A.1, 5.1.2A.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.

5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity stored in the USIM which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 2: The contents of the From header are modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is not explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in the USIM. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Preferred-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (learnt through the P-CSCF discovery procedures) and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

5.1.2A.2 Mobile-terminating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE can indicate privacy of the P-Preferred-Identity in accordance with RFC 3323 [33].

NOTE: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

3GPP TSG-CN1 Meeting #28
Dublin, Ireland, 10 – 14 February 2003

Tdoc N1-030251

revision of ***Tdoc N1-030157***

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **324** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*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-Access-Network procedure corrections for the S-CSCF
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	06/01/2003
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:	⌘	CR281 R1 (N1-022445) provided procedures for the use of the P-Access-Network-Info header at the S-CSCF based on whether the AS is within the trust domain or not. However the procedures currently within 5.4.3.2 specify that the P-Access-Network-Info header is forwarded to the AS when it is not in the trust domain, and not forwarded when it is. This is the opposite of what is intended according to the reason for change in the CR, and according to what is specified for the trust domain in RFC 3455. Further the requirement that relates to the removal of this header is step 13) duplicates the requirements with respect to the AS, and therefore the text is modified to remove the AS requirement. Further, the P-Access-Network-Info header should appear in all responses, and procedures relating to this header are missing for a response to a request for a standalone transaction (whether the user is registered or not), and for a response to a a subsequent request other than target refresh request for a dialog.
Summary of change:	⌘	The S-CSCF procedures relating to the retention and removal of the P-Access-Network-Info header are reversed. Further procedures are provided in regard to responses to requests.
Consequences if not approved:	⌘	Incorrect procedures for the handling of the P-Access-Network-Info header with regard to the trust domain.

Clauses affected:	⌘	5.4.3.2, 5.4.3.3
Other specs	⌘	Y ☐ N ☒ Other core specifications ⌘

affected:		
	X	Test specifications
	X	O&M Specifications
Other comments:	⌘	Revision 1 contains modified text to item 13 of 5.4.3.2.

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 or From header fields of the request or not. In case any of the said header fields 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;

2) remove its own SIP URL 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 Application Server 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, the S-CSCF shall forward this request to that application server, 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 application server 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 application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

   a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL 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 ~~retain~~ 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 ~~remove~~ 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 (see subclause 7.2.5) 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 URL 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 URL 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 URL 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 URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed;

13) in case the request is forwarded to the destination network (either via an I-CSCF(THIG) or directly) ~~or to an AS located outside the trust domain~~, remove the P-Access-Network-Info header; and

14) route the request based on SIP routeing procedures.

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

NOTE 2: 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 response to the initial request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog 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 URL from the topmost Route header;

2) create a Record-Route header containing its own SIP URL and save the Contact header from the request in order to release the dialog when needed;

3) in case the request is forwarded to the destination network or to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

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

When the S-CSCF receives a response to the target refresh request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog 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 URL from the topmost Route header;

2) in case the request is forwarded to the destination network or 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.

5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a registered 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 Request-URI of the request or not. In case the Request URI contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, continue with the rest of the steps;

2) remove its own URL 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 Application Server in response to a previously sent request;

4) check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI, the S-CSCF shall forward this request to that application server, 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 application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

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

5) insert a P-Charging-Function-Addresses header (see subclause 7.2.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) 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;

7) store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

8) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2;

9) build the Route header field with the values determined in the previous step;

10) determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;

11) build a Request-URI with the contents of the saved Contact URL determined in the previous step;

12) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

13) in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed; and

14) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and

NOTE: 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].

15) forward the request based on the topmost Route header.

When the S-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

1) execute the procedures described in the steps 1, 2 and 3 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

2) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];

3) keep the user registration status as unregistered for the duration of the dialog. When the dialog expires, the S-CSCF shall inform appropriately the HSS according to the procedures described in 3GPP TS 29.228 [14];

4) execute the procedure described in step 4 and 5 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures; and

5) execute the procedures described in the steps 6, 7, 12, 13, 14 and 15 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS.

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

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

2) create a Record-Route header containing its own SIP URL and save the Contact header from the target refresh request in order to release the dialog when needed; and

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

When the S-CSCF receives a response to the target refresh request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

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

1) remove its own URL from the topmost Route header; and

2) forward the request based on the topmost Route header.

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

3GPP TSG-CN1 Meeting #28
Dublin, Ireland, 10-14 February 2003

Tdoc ⌘N1-030260

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **326** ⌘ **rev** **1** ⌘ Current version: **5.3.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Updating user agent related profile tables.
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	13/02/2003
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:	⌘	24.229 mandates the UE to subscribe to the registration event package after a successful registration. This implies that the support of the SUBSCRIBE/NOTITY is mandatory for the UE.
Summary of change:	⌘	'o' has been changed to 'm' with condition in table A.4
Consequences if not approved:	⌘	24.229 will have contradictory requirements.

Clauses affected:	⌘	A.2.1.2

		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.

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[26] subclause 10.2	m	c3
2	registrar?	[26] subclause 10.3	o	c4
3	client behaviour for INVITE requests?	[26] subclause 13.2	m	o
4	server behaviour for INVITE requests?	[26] subclause 13.3	m	o
5	session release?	[26] subclause 15.1	m	c1
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o
7	authentication between UA and UA?	[26] subclause 22.2	o	o
8	authentication between UA and registrar?	[26] subclause 22.2	o	n/a
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	o
9	server handling of merged requests due to forking	[26] 8.2.2.2	m	m
10	client handling of multiple responses due to forking	[26] 13.2.2.4	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o
12	downloading of alerting information?	[26] subclause 20.4	o	o
	Extensions			
13	The SIP INFO method?	[25]	o	n/a
14	Reliability of provisional responses in SIP?	[27]	o	m
15	the REFER method?	[36]	o	o
16	Integration of resource management and SIP?	[30]	o	m
17	the SIP UPDATE method	[29]	c5	m
19	SIP extensions for media authorization?	[31]	o	m
20	SIP specific event notification	[28]	o	~~O~~c9
21	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
22	acting as the notifier of event information	[28]	c2	c2
23	acting as the recipient of event information	[28]	c2	c2
24	Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts	[35]	o	c6
25	private extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m
26	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
27	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	c7
28	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	m
29	Compressing the Session Initiation Protocol	[55]	o	c8

TypeUnitOrDepartmentHere
TypeYourNameHere TypeDateHere

c1:	IF A.4/3 OR A.4/4 THEN m ELSE o - - client behaviour or server behaviour for INVITE requests.
c2:	IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.
c3:	IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UA or S-CSCF functional entity.
c4:	IF A.3/4 OR A.3/7 THEN m ELSE n/a - - S-CSCF or AS functional entity.
c5:	IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.
c6:	IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7:	IF A.3/1 OR A.3/7B OR A.3/7D THEN m ELSE n/a - - UE or AS acting as originating UA, or AS performing 3rd party call control
c8:	IF A.3/1 THEN m ELSE n/a - - UE behaviour.
c9:	IF A.3/1 THEN m ELSE o - - UE behaviour.
o.1:	At least one of these capabilities is supported.