3GPP TSG CN Plenary Meeting #16 **NP-020230**
5th - 7th June 2002. Marco Island, USA.

Source: **TSG CN WG 1**

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

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **10** CRs on **Rel-5 on** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #16 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.229	004	1	Rel-5	S-CSCF Actions on Authentication Failure	C	5.0.0	5.1.0	N1-23	N1-020903
24.229	005	2	Rel-5	Disallow Parallel Registrations	C	5.0.0	5.1.0	N1-23	N1-020959
24.229	007	1	Rel-5	Hiding	F	5.0.0	5.1.0	N1-23	N1-020910
24.229	008	7	Rel-5	Support for services for unregistered users	B	5.0.0	5.1.0	N1-24	N1-021506
24.229	009	1	Rel-5	Editorials for GPRS Charging ID	F	5.0.0	5.1.0	N1-23	N1-020921
24.229	010	1	Rel-5	Passing GCID to AS	F	5.0.0	5.1.0	N1-23	N1-020922
24.229	011	1	Rel-5	Passing registration ICID	F	5.0.0	5.1.0	N1-23	N1-020907
24.229	012	2	Rel-5	Passing IOI	F	5.0.0	5.1.0	N1-23	N1-020967
24.229	013	1	Rel-5	Passing charging function addresses	F	5.0.0	5.1.0	N1-23	N1-020924
24.229	018		Rel-5	Corrections to original-dialog-id	F	5.0.0	5.1.0	N1-23	N1-020787

3GPP TSG-CN1 Meeting #23
Fort Lauderdale, Florida, USA 08. - 12. April 2002

Tdoc N1-020903

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **004** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	S-CSCF Actions on Authentication Failure
Source:	⌘	Hutchison 3G
Work item code:	⌘	IMS-CCR
Date:	⌘	26-03-2002
Category:	⌘	**C**
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)

Reason for change:	⌘	The current text in 24.229 states that the S-CSCF will deregister a user who has performed a register but failed the authentication cycle, see section 5.4.1.2.2 Abnormal Cases of 24.229. The currently defined action is open to an attack that would cause a valid user to be deregistered and sessions lost i.e. an attacker could send an unprotected REGISTER (i.e. not using the integrity key IK) knowing that it will fail as they do not have the correct security parameters. This would result in the real user being deregistered, and is clearly not a desirable outcome.
Summary of change:	⌘	S-CSCF actions are modified to allow it to perform a Network Initiated Authenication procedure or simply discard the failed authentication. It is also added that the users valid registration period is shortened when sending the NOTIFY.
Consequences if not approved:	⌘	A valid user will be de-registered from the IMS due to a malicious attacker sending false registrations.

Clauses affected:	⌘	5.4.1.2.2. 5.4.1.6
Other specs affected:	⌘	☐ 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/3G_Specs/CRs.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.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Normal procedures

When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.

The S-CSCF shall:

- check the existence of a Path header in the request;

Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.

- when a Path header exists in the request, insert its own FQDN, or IP address, in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;

- save the Contact header value for the entire duration of the registration;

- construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;

- include an expiration time in the 200 OK response, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE;

- save the list of preloaded Route headers for the entire duration of the registration;

NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);

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

- bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;

- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;

- check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and

Editor's Note: The method by which the P-CSCF indicates this is FFS.

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

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 Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:

- the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).

5.4.1.2.2 Abnormal cases

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by an initial registration or a UE initiated reauthentication, the S-CSCF shall either:

- start a network initiated re-authentication procedure as defined in subclause 5.4.1.6; or

- send a further challenge 401 (Unauthorized) to the UE.

In the case that the authentication response (RES) from the UE ~~is incorrect~~does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), ~~-~~ or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by a network initiated reauthentication the S-CSCF shall either:

- attempt a further authentication challenge; or

- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

~~In the case that the response from the UE is incorrect for three consecutive attempts then the S-CSCF shall deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.~~

~~In the case that the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), the S-CSCF shall either:~~

- ~~attempt a further authentication challenge; or~~

- ~~deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.~~

In the case that the response from the UE indicates that the authentication challenge was invalid with no RES or AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- respond with the relevant 4xx response (e.g. 401 Unauthorized to initiate a further authentication attempt, or 403 Forbidden if the authentication attempt is to be abandoned).

In the case that the response from the UE indicates that the authentication challenge was invalid with the AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation; and

- on receipt of the new vectors send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

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 with a 423 Registration Too Brief, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

-

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs (i.e. the dialog between S-CSCF and the UE and additionally between S-CSCF and P-CSCF) which have been established due to subscription to the registration-state event package of that user. The S-CSCF shall populate the content of the NOTIFY request and additionally shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value; and
- indicate a public user identity of the user for which the private user identity needs to be re-authenticated in the body of the NOTIFY request with registration state "re-authenticate".

Afterwards the S-CSCF shall:

- wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication might be requested from the HSS or may occur due to internal processing within the S-CSCF.

In case S-CSCF receives no data it can authenticate the subscriber from, the S-CSCF may as an implementation option try to request the UE by other means to re-authenticate, e.g. by sending a REFER method in order to request a REGISTER message.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of subscriber's registration timer to an operator defined value that will allow the user to be re-authenticated. If user fails to reauthenticate while its registration is still valid, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.

~~If UE does not re-authenticate within a certain period of time, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.~~

3GPP TSG-CN1 Meeting #23 ***Tdoc N1-020959***
Fort Lauderdale, Florida, USA 08. - 12. April 2002

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **005** ⌘ **rev** **2** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [ ] ME/UE [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Disallow Parallel Registrations
Source:	⌘	Hutchison 3G, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	29-03-2002
Category:	⌘	**C**
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)*

Reason for change:	⌘	There is a need to restrict the possibility of a UE to perform multiple registrations to ensure that the number of security associations stored in P-CSCF is restricted.
Summary of change:	⌘	P-CSCF and S-CSCF bahaviour are clarified when receiving multiple parallel registrations (e.g. due to an attacker) and the UE is restricted to a single REGISTER.
Consequences if not approved:	⌘	Denial of service attack is possible

Clauses affected:	⌘	5.1.1.2, 5.4.1.2.2
Other specs affected:	⌘	[ ] 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/3G_Specs/CRs.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 Procedures at the UE

5.1.1 Registration and authentication

5.1.1.1 General

The UE shall register public user identities (see table A.3/1 and dependencies on that major capability).

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [14], received in an earlier registration.

The public user identity to be registered can be extracted either from the USIM or may be input from the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration.

NOTE: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 response.

The use of the Path header shall not be supported by the UE.

On receiving the 200 OK response to the REGISTER request, the UE shall store the expiration time of the registration.

When a 401 Unauthorized response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 Registration too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 response.

5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the users registration-state event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). Therefore the UE shall generate a SUBSCRIBE request with the following elements:

- a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URL that contains the public user identity that was previously registered;

- a From header set to a SIP URL that contains the public user identity that was previously registered;

- a To header, set to a SIP URL that contains the public user identity that was previously registered;

- an Event header set to the "registration-state" event package;

- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

Afterwards it shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE message, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

The UE shall automatically resubscribe to the registration-state event package for a previously registered public user identity if the expiration time, as indicated in the Expires header of the 2xx response to the SUBSCRIBE message, has run out and the public user identity is still registered.

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

The UE shall reregister the public user identity 600 seconds before the expiration time of a previous registration, unless either the user or the application within the UE has determined that a continued registration is not required. If the registration period indicated from the S-CSCF is less than 600 seconds, the UE shall reregister when half of the registration period has expired.

The REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [14], received in an earlier registration.

On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, should contain the same expiration timer as the expiration timer returned in the 200 OK response to the initial.

NOTE: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 response.

On receiving the 200 OK response to the REGISTER request, the UE shall store the new expiration time of the registration for this public user identity.

The use of the Path header shall not be supported by the UE.

When a 401 Unauthorized response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 Registration Too Brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 response.

5.4 Procedures at the S-CSCF

Editor's note: The text on routeing needs to be enhanced to ensure interworking with RFC 2543 and RFC 2543bis networks.

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities, (see table A.150/2 and other capabilities in annex A dependent on that major capability).

The S-CSCF shall support the use of the Path header. The S-CSCF must also support the Require and Proxy-Require headers. The Path header is only applicable to the REGISTER request and its 200-OK response.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Normal procedures

When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.

The S-CSCF shall:

- check the existence of a Path header in the request;

Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.

- when a Path header exists in the request, insert its own FQDN, or IP address, in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;

- save the Contact header value for the entire duration of the registration;

- construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;

- include an expiration time in the 200 OK response, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE;

- save the list of preloaded Route headers for the entire duration of the registration;

NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);

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

- bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;

- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;

- check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and

Editor's Note: The method by which the P-CSCF indicates this is FFS.

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

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 Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:

- the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).

5.4.1.2.2 Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response from the UE is incorrect the S-CSCF shall either:

- attempt a further authentication challenge; or

- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE is incorrect for three consecutive attempts then the S-CSCF shall deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), the S-CSCF shall either:

- attempt a further authentication challenge; or

- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE indicates that the authentication challenge was invalid with no RES or AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- respond with the relevant 4xx response (e.g. 401 Unauthorized to initiate a further authentication attempt, or 403 Forbidden if the authentication attempt is to be abandoned).

In the case that the response from the UE indicates that the authentication challenge was invalid with the AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation; and

- on receipt of the new vectors send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

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 with a 423 Registration Too Brief, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** 007 ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Hiding
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	11-04-2002
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)*

Reason for change:	⌘	After encryption the value is not a valid SIP URL
Summary of change:	⌘	The encrypted string is transformed into a SIP URL
Consequences if not approved:	⌘	Not in line with the standards

Clauses affected:	⌘	5.3.3
Other specs Affected:	⌘	☐ 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/3G_Specs/CRs.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.

5.3.3 THIG functionality in the I-CSCF(THIG)

5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

All headers which reveal topology information, such as Via, Route, Record-Route, Path, shall be subject to topology hiding. ~~The Refer-To header shall not be subject to topology hiding.~~
Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URL of an I-CSCF(THIG) to the top of the Path header.
Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URL to the top of the Record-Route header.

5.3.3.2 Encryption for topology hiding

Upon receiving an outgoing request/response from the hiding network the I-~~CSFC~~CSCF(THIG) shall perform the encryption for topology hiding purposes, i.e. the I-CSCF(THIG) shall:

1) use the whole header values which were added by one or more specific entity of the hiding network as input to encryption, besides the UE entry;

2) not change the order of the headers subject to encryption when performing encryption;

3) use for one encrypted string all received consecutive header entries subject to encryption, regardless if they appear in separate consecutive headers or if they are consecutive entries in a comma separated list in one header;

4) construct an NAI in the form of 'username@realm',where the username part is the encrypted string, and the realm is the name of the encrypting network.

5~~4~~) ~~add~~ append ~~after the encrypted string~~ a "tokenized-by=" tag and set it to the value of the encrypting network's name, after the constructed NAI~~, indicating the encrypting network as a parameter~~;

6~~5~~) form one valid entry for the specific header out of the resulting ~~string~~NAI, e.g. ~~add~~ prepend "SIP/2.0/UDP " for Via headers ~~and~~ or "sip:" for Route and Record-Route headers.

NOTE 1: Even if consecutive entries of the same network in a specific header are encrypted, they will result in only one encrypted header entry. For example:

```
Via: SIP/2.0/UDP icscf1_s.home1.net,
     SIP/2.0/UDP Token( SIP/2.0/UDP scscf1.home1.net,
                        SIP/2.0/UDP pcscf1.home1.net)@home1.net;tokenized-by=home1.net,
     SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
```

NOTE 2: If multiple entries of the same network are within the same type of headers, but they are not consecutive, then these entries will be tokenized to different strings. For example

```
Route:  sip:icscf1_s.home1.net,
        sip:Token(sip:scscf1.home1.net)@home1.net;tokenized-by=home1.net,
        sip:as1.foreign.net,
        sip:Token(sip:scscf1.home1.net,
                  sip:pcscf1.home1.net)@home1.net;tokenized-by=home1.net,
        sip:[5555::aaa:bbb:ccc:ddd]
```

5.3.3.3 Decryption for Topology Hiding

Upon receiving and incoming requests/response to the hiding network the I-CSCF(THIG) shall perform the decryption for topology hiding purposes, i.e. the I-CSCF shall:

1) identify NAIs encrypted by the network this I-CSCF belongs to~~strings~~ within all headers of the incoming message;

2) use the user part of those NAIs~~all those encrypted strings~~ that carry the identification of the hiding network within the value of the tokenized-by tag as input to decryption;

3) use as encrypted string the user part of the NAI which follows~~data between~~ the sent-protocol (for Via Headers, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route Headers, e.g. "sip:")~~ and the tokenized-by tag;~~

4) replace all content of the received header which carries encrypted information with the entries resulting from decryption.

EXAMPLE: An encrypted entry to a Via header that looks like

```
Via:    SIP/2.0/UDP Token(SIP/1.0/UDP scscf1.home1.net,
        SIP/1.0/UDP pcscf1.home1.net)@home1.net;tokenized-by=home1.net
```

will be replaced with the following entries:

```
Via: SIP/1.0/UDP scscf1.home1.net, SIP/1.0/UDP pcscf1.home1.net
```

NOTE: Motivations for these decryption procedures are e.g. to allow the correct routeing of a response through the hiding network, to enable loop avoidance within the hiding network, or to allow the entities of the hiding network to change their entries within e.g. the Record-Route header.

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-020764021020021064021085021506454***
Budapest, Hungary, 13. – 17. May 2002

CR-Form-v5

CHANGE REQUEST

⌘	24.229	CR	008	⌘ rev	~~6~~ 7	⌘	Current version:	5.0.0	⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Support for services for unregistered users
Source:	⌘	Ericsson, Lucent, Siemens, Nortel, Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	15-May-02
Category:	⌘	**B**
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)

Reason for change:	⌘	Alignment with stage 2 specifications regarding support for services for unregistered users
Summary of change:	⌘	Procedures at the I-CSCF and S-CSCF are modified to cover the described case
Consequences if not approved:	⌘	Non existent stage 3 procedures describing the support for services for unregistered users

Clauses affected:	⌘	5.3.2.1, 5.4.3.2
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications
	⌘	
Other comments:	⌘	Revision 4 of this CR was created to incorporate to section 5.4.3.2 the interactions due to CRs 12, 13, 18, 31, 60, 62, 73. Therefore, implementation of clause 5.4.3.2 should be taken from this CR and ignored from the said CRs. Other subclauses modified by these CRs shall be implemented as is. Revision 6 of this CR was created to incorporate to section 5.4.3.2 the interactions due to CRs 094, 095, 096. Therefore, implementation of clause 5.4.3.2 should be taken from this CR and ignore from the said CRs. Other subclauses modified by these CRs shall be implemented as is. Revision 7 of this CR was created to incorporate changes relating to the addition of the p-access-network-info header.

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

Introduction

3GPP TS 23.228 v5.3.0 defines in clause 5.12.1 the *Mobile terminating call procedures to unregistered IMS subscriber that has services to unregistered state*.

However, 3GPP TS 24.229 does not reflect any of the stage 2 procedures. This CR implements the above mentioned stage 2 procedures in 3GPP TS 24.229

Proposed changes

********* First proposed change ****************

5.3.2 Further initial requests

5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for further initial requests.

When the I-CSCF receives an initial request, not containing a Route header, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [12] for the called user, indicated in the Request-URI.

Upon successful user location query, when the response contains the URL of the assigned S-CSCF ~~information about the required S-CSCF capabilities~~, the I-CSCF shall:

1) insert the URL received from the HSS as the topmost Route header;

2) store the value of the <icid> XML element, if present, received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body. If no <icid> XML element was found, then create a new, globally unique value for the <icid> XML element and insert it into the message body;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

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

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 29.228 [12]~~that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities~~;

2) insert the URL~~I~~ of the selected S-CSCF as the topmost Route header field value;~~ and~~

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URL of the assigned S-CSCF); and

4~~3~~) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query ~~(e.g., when the response from the HSS indicates that the user does not exist or the user is not registered and no services are provided)~~, the I-CSCF shall ~~:~~

1) return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or- 604 (Does not exist anywhere) in the case the user is not a user of the home network.

The response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

Upon an unsuccessful user location query (e.g.,when the response from the HSS indicates that the user does not exist or the user is not registered and no services are provided for such a user), the I-CSCF shall:

1) return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or- 604 (Does not exist anywhere) in the case the user is not a user of the home network. Thise response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request containing a Route header, the I-CSCF shall:

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

2) apply the procedures as described in subclause 5.3.3; and

3) forward the request based on the topmost Route header if present, or based on the Request-URI, in case no topmost Route header is available.

NOTE: In accordance with SIP the I-CSCF can add its own routeable SIP URL to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

********* Next proposed change ****************

5.4.3.2 Requests terminated at the served user

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:

- remove its own URL from the topmost Route header;
- 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 [12];
- 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 [12];
- check whether the initial request matches the initial filter criteria for unregistered user of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s).

  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.

  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; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body; and

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

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

~~— forward the request based on the topmost Route header.~~

When the S-CSCF receives, destined for ~~the~~ 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) ~~—~~remove its own URL from the topmost Route header;

2) ~~—~~check if P-Original-Dialog-ID header~~<original-dialog-id> XML element~~ is present in the ~~payload 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. The od-to-tag, od-from-tag and od-call-id parameter ~~<od-to-tag>, <od-from-tag> and <od-call-id> XML element~~ values from the P-Original-Dialog-ID header~~<original-dialog-id> XML element~~ may be used as additional parameters when searching for existing dialogs. ~~Local data shall be updated to indicate that this Application Server has been contacted for the initial request.~~ The S-CSCF shall determine the next hop using initial filter criteria ~~and local data on status of which Application Servers have been contacted~~. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header~~<original-dialog-id> XML element~~ in the message ~~body~~ of the request. If the next hop is not an Application Server, the S-CSCF shall ~~leave out~~remove the P-Original-Dialog-ID header~~<original-dialog-id> XML element~~ from the ~~payload of the~~ request;

3) check whether the initial request matches the initial filter criteria, 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: ~~— check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. 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; and

   b) ~~initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also~~ populate the P-Original-Dialog-ID header~~<original-dialog-id> XML element~~ in the message ~~body~~ with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.

4) 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~~insert a <charging-function-addresses> XML element in the message body (see subclause 5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS~~;

5~~4~~) ~~—~~store the value of the ~~<~~icid~~>~~ ~~XML element~~ parameter received in the ~~message body (see subclause 7.6)~~P-Charging-Vector header and retain the ~~<~~icid~~>~~ ~~XML element~~parameter in the ~~message body~~P-Charging-Vector header;

6) store the value of the ioi-originating parameter received in the P-Charging-Vector header, if present. The ioi-originating parameter identifies the sending network of the request message. The ioi-originating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS~~check if <ioi> XML element is present in the payload of the incoming request. If present, the <ioi-originating> child element identifies the sending network of the request message. Store the value of the <ioi-originating> child element received in the message body (see subclause 7.6) and only retain the <ioi> XML element in the message body if the next hop is an AS~~;

7~~5~~) ~~—~~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.~~1~~;

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

9~~6~~) 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.~~1~~;

10) build a Request-URI with the contents of the saved Contact URL determined in the previous step;~~7) build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];~~

11~~8~~) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

12~~9~~) 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 field from the request ~~(and from its appropriate responses)~~ in order to release the dialog when needed; and

~~10) replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and~~

13~~11~~) 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 and 2 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) execute the procedure described in step 2 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 [12];

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 [12];

4) execute the procedure described in step 3 and 4 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).

~~;check whether the initial request matches the initial filter criteria for unregistered user of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s).~~

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~~In case of contacting one or more application server(s) the S-CSCF shall:~~

~~5.a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and~~

~~5.b) initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.~~

5) execute the procedures described in the steps 5~~4~~, 6, 11~~8~~, 12~~9~~ and 13~~1~~ 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);

~~7) execute the procedure described in step 8 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);~~

~~8) execute the procedure described in step 9 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); and~~

~~9) execute the procedure described in step 11 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.

When the S-CSCF receives, destined for ~~the~~ a served user, a 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 ~~necessary~~ Contact header field~~s~~ from the refresh request ~~(and from its appropriate responses)~~ in order to release the dialog when needed; ~~and~~

3) remove the p-access-network-info header, if it is present, and may act upon it's contents accordingly; and

4~~3~~) ~~-~~forward the request based on the topmost Route header.

When the S-CSCF receives a response to the 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.

When the S-CSCF receives, destined for ~~the~~ a served user, a subsequent request other than 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.

3GPP TSG-CN1 Meeting #23
Fort Lauderdale, Florida, USA 08. - 12. April 2002

Tdoc N1-~~020778~~020921

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **009** ⌘ **rev** **-1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Editorials for GPRS Charging ID
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	~~01~~11.04.2002
Category:	⌘	~~D~~ 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)*

Reason for change:	⌘	Make GPRS Charging ID terminology in 24.229 consistent with 23.815.
Summary of change:	⌘	The XML definition and references to <gprs-charging-id> are changed to <gprs-charging-info>, which is a specific case of <access-network-info> containing <ggsn> and one or more <gcid> sub-elements for the GPRS access network. Also, the text for populating <access-network-info> is cleaned up.
Consequences if not approved:	⌘	Possible confusion if inconsistencies in terminology remain.

Clauses affected:	⌘	5.2.7.4, 5.2.9.1, 5.2.9.2, 5.4.4.2.1, 5.4.3.2.2 (should be renumbered as 5.4.4.2.2), 5.4.6.1.2, 5.4.6.1.3, 7.6.2, 7.6.3
Other specs affected:	⌘	**X** Other core specifications ⌘ 24.228 ☐ 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/3G_Specs/CRs.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

5.2.7 Initial INVITE

5.2.7.1 Determination MO or MT case

Editor's Note: It has to be discussed whether this section is needed or if the determination of MO/MT case at the P-CSCF shall be left implementation dependent.

5.2.7.2 Mobile-originating case

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

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

Editor's note: the case when the P-CSCF acts on behalf of the UE is FFS.

- if a media authorization token is generated by the PCF (i.e. when service-based local policy control is applied), insert the Media Authorization header containing that media authorization token.

When the P-CSCF sends the ~~COMET~~ UPDATE request towards the S-CSCF, the P-CSCF shall also include the <gprs-charging-~~id~~info> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging ~~identifier~~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 pre-loaded Route header. The received initial INVITE 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:

Editor's note: the case when the P-CSCF acts on behalf of the UE is FFS.

- if a media authorization token is generated by the PCF (i.e. when service-based local policy control is applied), insert the Media Authorization header containing that media authorization token.

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

When the P-CSCF sends 180 Ringing towards the S-CSCF, the P-CSCF shall also include the <gprs-charging-~~id~~info> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging ~~identifier~~information.

~~5.2.7.4 GPRS charging identifier~~5.2.7.4 GPRS charging information

The GPRS charging ~~identifier~~ information ~~is~~ shall be coded as the <gprs-charging-~~id~~info> XML element within the SIP message body as described in subclause 7.6.

The <access-network-info> child element of the <charging-vector> element shall contain an instance of the <gprs-charging-~~id~~info> ~~XML~~ element. ~~contains one~~The <ggsn> child element ~~and one or more <pdp-info> child elements~~shall contain the identifier of the associated GGSN. Each <~~pdp-info~~gcid> child ~~XML~~ element within <gprs-charging-~~id~~info> shall contain values corresponding~~s~~ to a PDP context that was established at the GGSN for a UE. Each <~~pdp-info~~gcid> ~~XML~~ element contains <pdp-id> and <pdp-index> child elements, where <pdp-id> ~~is~~ shall contain the PDP context identifier that the P-CSCF obtained from the GGSN and <pdp-index> ~~is~~ shall contain the relative index to the media stream in the SDP for the PDP context. The numbering for ~~the~~ <pdp-index> ~~will~~ shall start at 1 and ~~will be~~is associated with the 'm' lines in the SDP, where the counting is done from top to bottom.

~~For the m~~Messages including the 3GPP IMS XML body with the <gprs-charging-id> XML element~~,~~ shall contain a Content-Type header field with ~~set~~ the value ~~of the Content-Type header to include~~ set to the associated MIME type specified in subclause 7.6, which may be one part of a multipart message body.

End of first change

Start of second change

5.2.9 Subsequent requests

5.2.9.1 Mobile-originating case

For a reINVITE request from the UE, when the P-CSCF sends the ~~COMET~~ UPDATE request towards the S-CSCF, the P-CSCF shall include the updated <gprs-charging-~~id~~info> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging ~~identifier~~information.

5.2.9.2 Mobile-terminating case

For a reINVITE request destined towards the UE, when the P-CSCF sends 200 OK response (to the INVITE) towards the S-CSCF, the P-CSCF shall include the updated <gprs-charging-~~id~~info> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging ~~identifier~~information.

End of second change

Start of third change

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.1.1 Determination of served user

Void.

5.4.4.1.2 Mobile-originating case

Void.

5.4.3.1.3 Mobile-terminating case

Void.

5.4.4.2 Subsequent requests

Editor's Note: PRACK and COMET can be handled in a generic way.

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives the ~~COMET~~ UPDATE request, the S-CSCF shall remove and store the <gprs-charging-~~id~~info> XML element from the message body (see subclause 7.6). The <gprs-charging-~~id~~info> XML element is not included in the message body when the ~~COMET~~ UPDATE request is forwarded.

5.4.~~3~~4.2.2 Mobile-terminating case

When the S-CSCF receives 180 Ringing response, the S-CSCF shall remove and store the <gprs-charging-~~id~~info> XML element from the message body (see subclause 7.6). The <gprs-charging-~~id~~info> XML element is not included in the message body when the 180 Ringing response is forwarded.

End of third change

Start of fourth change

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

5.4.6.1.2 Mobile-originating case

For a reINVITE request from the UE, when the S-CSCF receives the COMET request, the S-CSCF shall remove and store the updated <gprs-charging-~~id~~info> XML element from the message body (see subclause 7.6). The <gprs-charging-~~id~~info> XML element is not included in the message body when the COMET request is forwarded.

5.4.6.1.3 Mobile-terminating case

For a reINVITE request destined towards the UE, when the S-CSCF receives the 200 OK response (to the INVITE), the S-CSCF shall remove and store the updated <gprs-charging-~~id~~info> XML element from the message body (see subclause 7.6). The <gprs-charging-~~id~~info> XML element is not included in the message body when the 200 OK response is forwarded.

End of fourth change

Start of fifth change

7.6 3GPP IM CN subsystem XML body, version 1

7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The <icid> XML element is an exception to this rule; it may only be removed by the P-CSCF. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

7.6.2 Document Type Definition

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (vnid?, cell-id?,
        original-dialog-id?, destination-public-user-id?,
        access?, charging-vector?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- vnid element: Visited network identity -->
    <!ELEMENT vnid              (#PCDATA)>

    <!-- cell-id element: The Cell-Global-ID -->
    <!ELEMENT cell-id               (mcc, mnc, lac, ci)>
    <!ELEMENT mcc                   (#PCDATA)>
    <!ELEMENT mnc                   (#PCDATA)>
    <!ELEMENT lac                   (#PCDATA)>
    <!ELEMENT ci                    (#PCDATA)>
    <!ATTLIST cell-id rat (utran | geran)   #REQUIRED>

    <!-- original-dialog-id: original dialog ID -->
    <!ELEMENT original-dialog-id (od-from, od-to, od-call-id)>
    <!ELEMENT od-from               (#PCDATA)>
    <!ELEMENT od-to                 (#PCDATA)>
    <!ELEMENT od-call-id            (#PCDATA)>

    <!-- public-user-id: public user ID -->
    <!ELEMENT destination-public-user-id    (#PCDATA)>

    <!-- access: the type of access network →
    <!ELEMENT access            (access-type, technology?)>
    <!ELEMENT access-type   (gprs | wlan | fixed | (#PCDATA))>
    <!ELEMENT technology    (utran| geran | 802.11a |
                802.11b | sat | adsl | (#PCDATA))>

    <!-- charging-vector element: Charging Vector -->
    <!ELEMENT charging-vector       (icid, gprs-charging-idaccess-network-info?)>

    <!-- icid element: IMS charging identifier -->
    <!ELEMENT icid                  (#PCDATA)>

    <!-- gprsaccess-chargingnetwork-id info element: GPRS charging identifiersAccess Network
Information -->
    <!ELEMENT access-network-info   (gprs-charging-info?, other-access-info?)>

    <!-- gprs-charging-info element: GPRS access network charging information -->
    <!ELEMENT gprs-charging-idinfo      (ggsn, pdp-infogcid+)>
    <!ELEMENT ggsn                  (#PCDATA)>
    <!ELEMENT pdp-infogcid                  (pdp-index, pdp-id)>
    <!ELEMENT pdp-index             (#PCDATA)>
    <!ELEMENT pdp-id                (#PCDATA)>

    <!-- other-access-info element: other, non-GPRS, access network charging information -->
    <!ELEMENT other-access-info     (#PCDATA)>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition.

<ims-3gpp>: This is the root element of the 3GPP IMS XML body. It shall always be present. The version described in the present document is 1.

<vnid>: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.

<cell-id>: This element describes the identity of the cell that is serving the user.

The <cell-id> element contains the <ran> attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.

The <cell-id> element comprises four children elements: <mcc>, <mnc>, <lac> and <ci>. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].

<original-dialog-id>:The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies then dialogue.

The original-dialog-id element comprises three children elements: <od-from>, <od-to>, <od-call-id>. Their values contain, respectively, a copy of the From, To and Call-ID header values as received in the SIP message at the S-CSCF.

<destination-public-user-id>: The destination public-user-id URL of the current session.

<access>: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: <ant> and <technology>.

The <access-type> child element describes the access type. The predefined values are:

- gprs: the user is accessing the network through a GRPS access;
- wlan: the user is accessing the network through a wireless local area network;
- fixed: the user is accessing the network through a fixed access.

The <technology> child element, if present, describes the access technology. The pre-defined values are:

- utran: UTRAN, as defined in [3];
- geran: GERAN, as defined in [3];
- 802.11a: wireless local area network according to the 802.11a technology;
- 802.11b: wireless local area network according to the 802.11b technology;
- sat: satellite access;
- adsl: asymmetric digital subscriber line.

<charging-vector>: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: <icid> and <gprs-charging-id>.

The <icid> child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.

The <access-network-info> child element, if present, contains charging information pertaining to the access network: GPRS or non-GPRS.

The <gprs-charging-~~id~~info> child element, if present, contains GPRS charging ~~identifiers~~ information comprised of the following: <ggsn> and <~~pdp-info~~gcid>:

- <ggsn>: identifier of the GGSN;
- <~~pdp-info~~gcid>: one or more instances of GPRS charging identifiers, information for a PDP context, which is comprised of two children elements: <pdp-index> and <pdp-id>:

- <pdp-index>: relative index of PDP context as it correlates to a media stream in the SDP;
- <pdp-id>: unique identifier of the PDP context from the GGSN.

The <other-access-info> child element, if present, contains non-GPRS charging identifiers in a format not described within this specification.

<service-info>: the transparent element received from the HSS for a particular Application Server are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

End of fifth change

3GPP TSG-CN1 Meeting #23
Fort Lauderdale, Florida, USA 08. - 12. April 2002

Tdoc N1-~~020779~~020922

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **010** ⌘ **rev** **-1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Passing GCID to AS
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	~~01~~10.04.2002
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)*

Reason for change:	⌘	Make passing of GCID in 24.229 consistent with 23.815.
Summary of change:	⌘	Procedures are added to pass the GCID (access network charging information) from the S-CSCF to AS. The AS procedures are also modified to accept the entire charging vector.
Consequences if not approved:	⌘	AS will not have access to GPRS level information for charging purposes.

Clauses affected:	⌘	5.4.4.2.1, 5.4.3.2.2 (should be renumbered 5.4.4.2.2), 5.4.6.1.2, 5.4.6.1.3, 5.7.1.2		
Other specs affected:	⌘	**X** Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	24.228
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/3G_Specs/CRs.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

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.1.1 Determination of served user

Void.

5.4.4.1.2 Mobile-originating case

Void.

5.4.3.1.3 Mobile-terminating case

Void.

5.4.4.2 Subsequent requests

Editor's Note: PRACK and COMET can be handled in a generic way.

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives the ~~COMET~~ UPDATE request, the S-CSCF shall ~~remove and~~ store the <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is retained in the message body when the ~~COMET~~UPDATE request is forwarded to an AS. ~~-~~However, it is not included in the message body when the ~~COMET~~ UPDATE request is forwarded outside the home network of the S-CSCF.

5.4.3.2.2 Mobile-terminating case

When the S-CSCF receives 180 Ringing response, the S-CSCF shall ~~remove and~~ store the <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is retained in the message body when the 180 Ringing response is forwarded to an AS. ~~-~~However, it is not included in the message body when the 180 Ringing response is forwarded outside the home network of the S-CSCF.

End of first change

Start of second change

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

5.4.6.1.2 Mobile-originating case

For a reINVITE request from the UE, when the S-CSCF receives the ~~COMET~~ UPDATE request, the S-CSCF shall ~~remove and~~ store the updated <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is retained in the message body when the ~~COMET~~UPDATE request is forwarded to an AS. However, it is not included in the message body when the ~~COMET~~ UPDATE request is forwarded outside the home network of the S-CSCF.

5.4.6.1.3 Mobile-terminating case

For a reINVITE request destined towards the UE, when the S-CSCF receives the 200 OK response (to the INVITE), the S-CSCF shall ~~remove and~~ store the updated <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is retained in the message body when the 200 OK response is forwarded to an AS. ~~-~~However, it is not included in the message body when the 200 OK response is forwarded outside the home network of the S-CSCF.

End of second change

5.7 Procedures at the Application Server (AS)

NOTE: This subclause defines only the requirements on the application server that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

5.7.1 Common Application Server (AS) Procedures

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 OK or an appropriate failure response. For the success case, the 200 OK response shall contain Expires value equal to the value received in the REGISTER request.

Start of third change

5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the values ~~of~~ from the <~~icid~~charging-vector> XML element received in the message body (see subclause 7.6) and retain the <~~icid~~charging-vector> XML element in the message body.

End of third change

3GPP TSG-CN1 Meeting #23
Fort Lauderdale, Florida, USA 08. - 12. April 2002

Tdoc N1-~~020780~~020907

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **011** ⌘ **rev** **-1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Passing registration ICID
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	~~01~~10.04.2002
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)

Reason for change:	⌘	Update procedures in 24.229 to pass ICID with SIP REGISTER to be consistent with 23.815.
Summary of change:	⌘	Procedures are added to pass an instance of the <icid> XML element for SIP registration. The ICID is generated by the P-CSCF. It will be received and stored at the S-CSCF. The AS procedures are also modified to accept the <icid> for the 3rd party REGISTER.
Consequences if not approved:	⌘	P-CSCF, S-CSCF and AS will not have ~~separate~~ a correlation identifier to ~~charge on the SIP signalling channel used for~~ use for registration related charging procedures.
Clauses affected:	⌘	5.2.2, 5.4.1.2.1, 5.4.1.7, 5.7.1.1
Other specs affected:	⌘	**X** Other core specifications ⌘ 24.228 ☐ 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/3G_Specs/CRs.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

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support use of the Path header.

NOTE: The Path header is only applicable to the REGISTER request and its 200 OK response.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE that pertains to a given public user identity, the P-CSCF shall:

- insert a Path header in the request. The P-CSCF shall include in the Path header an entry containing the SIP URL identifying the P-CSCF;
- insert a Require header and a Proxy-Require header both containing the option tag "path";
- for the initial REGISTER request for a public user identity create a new, globally unique value for the <icid> XML element, save it locally and insert it into the message body (see subclause 7.6);
- for a reREGISTER request for a public user identity use the previously assigned value for the <icid> XML element and insert it into the message body (see subclause 7.6);
- if the REGISTER request was received with a valid integrity check, add information to the REGISTER request to indicate that the REGISTER request was received with a valid integrity check; and

Editor's Note : The exact mechanism for this is FFS.

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

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) remove its SIP URL from the list of Path headers, reverses the order of the list and save the resulting list of Path headers. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing Path headers with the new list;
2) associate the Path header information with the registered public user identity;
3) remove the list of Path headers and "path" option-tags from the 200 OK response before forwarding the response to the UE.

When the P-CSCF receives a 401 Unauthorized response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 Unauthorized response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

Editor's Note: The P-CSCF behaviour when 3xx or 4xx responses other than 401 Unauthorized are received is FFS.

Editor's Note: The text above assumes that public user identities are registered one by one. Public user identity might need to be changed to Service Profile in the case when public user identities can be implicitly registered.

NOTE: The P-CSCF will maintain two Route lists. The first Route list - created during the registration procedure - is used only to pre-load the routeing information into the initial INVITE request that originated at 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.

When the P-CSCF receives a 420 Bad Extension response to the above REGISTER request, the P-CSCF shall check the value of the Unsupported header field. When the value of the Unsupported header field is path, the P-CSCF shall take OA&M actions to indicate an error, in addition to passing on the 420 response to the UE. In all other cases, the P-CSCF shall proxy the 420 Bad Extension response.

End of first change

Start of second change

5.4 Procedures at the S-CSCF

Editor's note: The text on routeing needs to be enhanced to ensure interworking with RFC 2543 and RFC 2543bis networks.

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities, (see table A.150/2 and other capabilities in annex A dependent on that major capability).

The S-CSCF shall support the use of the Path header. The S-CSCF must also support the Require and Proxy-Require headers. The Path header is only applicable to the REGISTER request and its 200-OK response.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Normal procedures

When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.

The S-CSCF shall:

- check the existence of a Path header in the request;

Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.

- when a Path header exists in the request, insert its own FQDN, or IP address, in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;

- save the Contact header value for the entire duration of the registration;

- construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;

- include an expiration time in the 200 OK response, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE;

- save the list of preloaded Route headers for the entire duration of the registration;

NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);

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

- bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;

- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;

- store the <icid> XML element from the message body (see subclause 7.6);

- check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and

Editor's Note: The method by which the P-CSCF indicates this is FFS.

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

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 Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:

- the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).

End of second change

Start of third change

5.4.1.7 Notification of Application Servers about registration status

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each Application Server with the following information:

a) the Request-URI shall contain the FQDN or IP address of the AS in the form of a SIP URL;

b) the From header shall contain the FQDN or IP address of the S-CSCF in the form of a SIP URL;

c) the To header shall contain the public user identity as contained in the REGISTER request received form the UE;

d) the Contact header shall contain the FQDN or IP address of the S-CSCF in the form of a SIP URL;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header shall contain the same value that the S-CSCF returned in the 200 OK response for the REGISTER request received form the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER, such as IMSI to be delivered to IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [12]), then it shall be included in the REGISTER message body within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6~~.~~; and

h) for initial registration, a message body shall be included in the REGISTER request with the <icid> XML element (see subclause 7.6) populated with the same value received at the S-CSCF in the original REGISTER request;

End of third change

Start of fourth change

5.7 Procedures at the Application Server (AS)

NOTE: This subclause defines only the requirements on the application server that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

5.7.1 Common Application Server (AS) Procedures

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 OK or an appropriate failure response. For the success case, the 200 OK response shall contain Expires value equal to the value received in the REGISTER request. Also, the AS shall store the value of the <icid> XML element received in the ~~REGISTER~~ message body of the REGISTER request (see subclause 7.6).

5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body.

End of fourth change

3GPP TSG-CN1 Meeting #23 **Tdoc N1-~~020781~~02092~~3~~67**
Fort Lauderdale, Florida, USA 08. - 12. April 2002

CR-Form-v5

CHANGE REQUEST

⌘	24.229	CR	012	⌘ rev	~~-~~ ~~1~~ 2	⌘	Current version:	5.0.0	⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Passing IOI
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	~~01~~~~11~~12.04.2002
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)

Reason for change:	⌘	Make passing of IOI (Inter Operator Identification) in 24.229 consistent with 23.815.
Summary of change:	⌘	Procedures are added to pass the IOI from the S-CSCF to another 3GPP IMS network. The S-CSCF procedures are also modified to accept the received IOI. Both procedures apply to the IOI -~~reques~~originating in the initial message sent to another network and the IOI ~~respond~~terminating of the other network that is included in the response to the initial message. Also, the MGCF inserts IOI for calls originating from circuit-switched networks to identify the source network. IOI is added to the XML charging-vector element.
Consequences if not approved:	⌘	S-CSCF will not have access to peer network identification information for charging purposes. This may prevent associating charging records from different networks.

Clauses affected:	⌘	5.4.3, 5.5.3, 5.4.4, 7.6			
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	24.228	
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/3G_Specs/CRs.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

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

5.4.3.1 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:

- remove its own SIP URL from the topmost Route header;
- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. 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 an appropriate SIP response shall be sent to the originator;
- check if <original-dialog-id> XML element is present in the payload 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. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, 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; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- insert an <ioi> XML element ~~for the sending network~~ into the message body (see subclause 7.6) if the next hop is an AS, I-CSCF or outside of the current network. The <~~ioi-requesting~~ioi-originating> child element is set to a value that identifies the sending network and the <~~ioi-responding~~ioi-terminating> child element is set to an empty value;
- 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; and
- 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 header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and

- route the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- route the request based on the topmost Route header.

5.4.3.2 Requests terminated at the served user

When the S-CSCF receives, destined for 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:

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload 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. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. 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; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- check if <ioi> XML element is present in the payload of the incoming request. If present, the <~~ioi-requesting~~ioi-originating> child element~~it~~ identifies the sending network of the request message. Store the value of the <~~ioi-requesting~~ioi-originating> ~~XML~~child element received in the message body (see subclause 7.6) and only retain ~~remove~~ the <ioi> XML element ~~from~~in the message body if the next hop is an AS ~~before forwarding to the next hop~~;
- 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 5.4.1.2.1;
- 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 5.4.1.2.1;
- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and

- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

End of first change

Start of second change

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.1.1 Determination of served user

Void.

5.4.4.1.2 Mobile-originating case

Void.

5.4.3.1.3 Mobile-terminating case

Void.

5.4.4.2 Subsequent requests

Editor's Note: PRACK and COMET can be handled in a generic way.

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives the 183 response, the S-CSCF shall check if the <ioi> XML element is present in the payload of the incoming response. If present, the <~~ioi-responding~~ioi-terminating> child element~~it~~ identifies the sending network of the response message. The S-CSCF shall ~~remove and~~ store the <~~ioi-responding~~ioi-terminating> ~~XML~~child element from the message body (see subclause 7.6). The <ioi> XML element is ~~not~~only included in the message body when the next hop in forwarding the 183 response is ~~forwarded~~an AS.

When the S-CSCF receives the COMET request, the S-CSCF shall remove and store the <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is not included in the message body when the COMET request is forwarded.

5.4.3.2.2 Mobile-terminating case

When the S-CSCF sends the 183 response, the S-CSCF shall insert an <ioi> XML element ~~of the sending network~~ in the message body of the outgoing response (see subclause 7.6) if the response is sent to another network, an AS or an I-CSCF. The <~~ioi-responding~~ioi-terminating> child element is set to a value that identifies the sending network of the response and the <~~ioi-requesting~~ioi-originating> child element is set to the previously received value of <~~ioi-requesting~~ioi-originating>.

When the S-CSCF receives 180 Ringing response, the S-CSCF shall remove and store the <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is not included in the message body when the 180 Ringing response is forwarded.

End of second change

Start of third change

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore the dependencies of table 0.3/1 and table 0.3/2 shall not apply.

The use of the Path header shall not be supported by the MGCF.

5.5.2 Subscription and notification

5.5.2.1 Subscriptions to MGCF events

Void.

5.5.2.2 Gateway behaviour for SUBSCRIBE / NOTIFY

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see draft-ietf-sip-manyfolks-resource [22]); ~~and~~
  - create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6)~~.~~; and
  - insert an <ioi> XML element into the message body (see subclause 7.6). The <~~ioi-requesting~~ioi-originating> child element is set to a value that identifies the sending circuit-switched network and the <~~ioi-responding~~ioi-terminating> child element is set to an empty value.

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request, the MGCF shall:

- send 100 "Trying" response;
- assuming the "100rel" indicator was received and a matching codec is found,send 183 "Session Progress" response:
  - set the Require header to the value of "100rel";
  - set the Content-Disposition header to the value of "precondition"; and
  - store the value of the <icid> XML element received in the message body (see subclause 7.6).

Editor's note: must receive Supports header with value of 100rel in the INVITE.

Editor's note: need text to describe error legs.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 200 OK response to a PRACK request and notification that bearer setup is complete, the MGCF shall:

- send a COMET request.

5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 "Ringing" to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 OK to the UE.

5.5.4 Call release

5.5.4.1 Call release initiated by a circuit-switched network

When the MGCF receives an indication of call release from a circuit-switched network, the MGCF shall:

- send a BYE request to the UE.

5.5.4.2 S-CSCF-initiated call release

5.5.4.3 MGW-initiated call release

When the MGCF receives an indication from the MGW that the bearer was lost, the MGCF shall:

- send a BYE request towards the UE.

Editor's note: should the Error-Info header be used to indicate an error case for the session release?

5.5.5 Call-related requests

5.5.5.1 ReINVITE

5.5.5.1.1 Calls originating from circuit-switched networks

Editor's Note: When the bearer on the circuit-switched network side is halted/resumed, should the MGCF notify the UE with a reINVITE?

5.5.5.1.2 Calls terminating in circuit-switched networks

When the MGCF receives a reINVITE request for hold/resume operation, the MGCF shall:

- send 100 Trying response;
- after performing interaction with MGW to hold/resume the media flow, send 200 OK response.

5.5.5.2 REFER

5.5.5.2.1 Calls originating from circuit-switched networks

Void.

5.5.5.2.2 Calls terminating in circuit-switched networks

Void.

5.5.5.2.3 REFER initiating a new session

Void.

5.5.5.2.4 REFER replacing an existing session

Void.

5.5.5.3 INFO

Void.

5.5.6 Further initial requests

When the MGCF responds to an OPTIONS request with a 200 OK response, the MGCF may include a message body with an indication of the DTMF capabilities and supported codecs of the MGCF/MGW.

Editor's note: it is FFS how to identify the resources of the MGCF/MGW.

End of third change

Start of fourth change

7.6 3GPP IM CN subsystem XML body, version 1

7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The <icid> XML element is an exception to this rule; it may only be removed by the P-CSCF. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

7.6.2 Document Type Definition

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (vnid?, cell-id?,
        original-dialog-id?, destination-public-user-id?,
        access?, charging-vector?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- vnid element: Visited network identity -->
    <!ELEMENT vnid              (#PCDATA)>

    <!-- cell-id element: The Cell-Global-ID -->
    <!ELEMENT cell-id               (mcc, mnc, lac, ci)>
    <!ELEMENT mcc                   (#PCDATA)>
    <!ELEMENT mnc                   (#PCDATA)>
    <!ELEMENT lac                   (#PCDATA)>
    <!ELEMENT ci                    (#PCDATA)>
    <!ATTLIST cell-id rat (utran | geran)   #REQUIRED>

    <!-- original-dialog-id: original dialog ID -->
    <!ELEMENT original-dialog-id (od-from, od-to, od-call-id)>
    <!ELEMENT od-from               (#PCDATA)>
    <!ELEMENT od-to                 (#PCDATA)>
    <!ELEMENT od-call-id            (#PCDATA)>

    <!-- public-user-id: public user ID -->
    <!ELEMENT destination-public-user-id    (#PCDATA)>

    <!-- access: the type of access network →
    <!ELEMENT access            (access-type, technology?)>
    <!ELEMENT access-type   (gprs | wlan | fixed | (#PCDATA))>
    <!ELEMENT technology    (utran| geran | 802.11a |
                802.11b | sat | adsl | (#PCDATA))>

    <!-- charging-vector element: Charging Vector -->
    <!ELEMENT charging-vector       (icid, gprs-charging-id?, ioi?)>

    <!-- icid element: IMS charging identifier -->
    <!ELEMENT icid                  (#PCDATA)>
    <!-- gprs-charging-id element: GPRS charging identifiers -->
    <!ELEMENT gprs-charging-id      (ggsn, pdp-info+)>
    <!ELEMENT ggsn                  (#PCDATA)>
    <!ELEMENT pdp-info              (pdp-index, pdp-id)>
    <!ELEMENT pdp-index             (#PCDATA)>
    <!ELEMENT pdp-id                (#PCDATA)>

    <!-- ioi element: inter operator identifiers -->
    <!ELEMENT ioi                   (ioi-requestingioi-originating, ioi-respondingioi-terminating)>
    <!ELEMENT ioi-requestingioi-originating     (#PCDATA)>
    <!ELEMENT ioi-respondingioi-terminating     (#PCDATA)>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition.

<ims-3gpp>: This is the root element of the 3GPP IMS XML body. It shall always be present. The version described in the present document is 1.

<vnid>: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.

<cell-id>: This element describes the identity of the cell that is serving the user.

The <cell-id> element contains the <ran> attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.

The <cell-id> element comprises four children elements: <mcc>, <mnc>, <lac> and <ci>. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].

<original-dialog-id>:The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies then dialogue.

The original-dialog-id element comprises three children elements: <od-from>, <od-to>, <od-call-id>. Their values contain, respectively, a copy of the From, To and Call-ID header values as received in the SIP message at the S-CSCF.

<destination-public-user-id>: The destination public-user-id URL of the current session.

<access>: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: <ant> and <technology>.

The <access-type> child element describes the access type. The predefined values are:

- gprs: the user is accessing the network through a GRPS access;
- wlan: the user is accessing the network through a wireless local area network;
- fixed: the user is accessing the network through a fixed access.

The <technology> child element, if present, describes the access technology. The pre-defined values are:

- utran: UTRAN, as defined in [3];
- geran: GERAN, as defined in [3];
- 802.11a: wireless local area network according to the 802.11a technology;
- 802.11b: wireless local area network according to the 802.11b technology;
- sat: satellite access;
- adsl: asymmetric digital subscriber line.

<charging-vector>: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: <icid> and <gprs-charging-id>.

The <icid> child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.

The <gprs-charging-id> child element, if present, contains GPRS charging identifiers comprised of the following: <ggsn> and <pdp-info>:

- <ggsn>: identifier of the GGSN;

- <pdp-info>: one or more instances of information for a PDP context, which is comprised of two children elements: <pdp-index> and <pdp-id>:
  - <pdp-index>: relative index of PDP context as it correlates to a media stream in the SDP;
  - <pdp-id>: unique identifier of the PDP context from the GGSN.

The <ioi> child element contains ~~an~~ two inter operator identifiers that uniquely identifies ~~an~~ IMS networks: <~~ioi requesting~~ioi-originating> and <~~ioi responding~~ioi-terminating>.

- <~~ioi requesting~~ioi-originating>~~It~~ identifies the network that originated the initial dialog request or standalone message ~~containing the <ioi> element~~.
- <~~ioi responding~~ioi-terminating> identifies the network that responded to the initial dialog request or standalone message.

<service-info>: the transparent element received from the HSS for a particular Application Server are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

End of fourth change

3GPP TSG-CN1 Meeting #23
Fort Lauderdale, Florida, USA 08. - 12. April 2002

Tdoc N1-~~020782~~020924

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **013** ⌘ **rev** **-1** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Passing charging function addresses
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	~~01~~11.04.2002
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)*

Reason for change:	⌘	Make passing of off-line and on-line charging function addresses in 24.229 consistent with 23.815.
Summary of change:	⌘	Procedures are added to pass the off-line and on-line charging function addresses from the S-CSCF to other network entities within the same 3GPP IMS network. The AS, BGCF, MGCF, MRFC, I-CSCF and P-CSCF procedures are modified to accept the received off-line charging function addresses. The AS and MRFC procedures are modified to accept the on-line charging function addresses. A new XML element, separate from <charging-vector>, is defined for the charging function addresses.
Consequences if not approved:	⌘	The AS, BGCF, MGCF, MRFC, I-CSCF and P-CSCF network entities may not have access to the correct charging functions. This may prevent associating charging records from within the network.
Clauses affected:	⌘	5.2.2, 5.2.6.2, 5.2.6.3, 5.3.1.2, 5.3.2.1, 5.4.1.7, 5.4.3, 5.4.4, 5.5.3.1.1, 5.5.3.1.2, 5.6.2, 5.7, 5.8.2.1.1, 7.6
Other specs affected:	⌘	**X** Other core specifications ⌘ 24.228 ☐ 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/3G_Specs/CRs.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

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support use of the Path header.

NOTE: The Path header is only applicable to the REGISTER request and its 200 OK response.

When the P-CSCF sends any request or response to the UE, before sending the message the P-CSCF shall:

- remove the <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6), if present, from the message body of the request or response.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6), if present, from the message body of the received request or response. Also, the P-CSCF shall ignore any data received in the <charging-vector> and <charging-function-addresses> XML elements; and

- may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before forwarding the message.

5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE that pertains to a given public user identity, the P-CSCF shall:

- insert a Path header in the request. The P-CSCF shall include in the Path header an entry containing the SIP URL identifying the P-CSCF;

- insert a Require header and a Proxy-Require header both containing the option tag "path";

- if the REGISTER request was received with a valid integrity check, add information to the REGISTER request to indicate that the REGISTER request was received with a valid integrity check; and

Editor's Note : The exact mechanism for this is FFS.

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

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) remove its SIP URL from the list of Path headers, reverses the order of the list and save the resulting list of Path headers. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing Path headers with the new list;

2) associate the Path header information with the registered public user identity;

3) remove the list of Path headers and "path" option-tags from the 200 OK response before forwarding the response to the UE.

When the P-CSCF receives a 200 OK response to a REGISTER request, the P-CSCF shall remove and store the <charging-function-addresses> ~~<charging-functions>~~ XML element from the message body (see subclause 7.6).

When the P-CSCF receives a 401 Unauthorized response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 Unauthorized response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

Editor's Note: The P-CSCF behaviour when 3xx or 4xx responses other than 401 Unauthorized are received is FFS.

Editor's Note: The text above assumes that public user identities are registered one by one. Public user identity might need to be changed to Service Profile in the case when public user identities can be implicitly registered.

NOTE: The P-CSCF will maintain two Route lists. The first Route list - created during the registration procedure - is used only to pre-load the routeing information into the initial INVITE request that originated at 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.

When the P-CSCF receives a 420 Bad Extension response to the above REGISTER request, the P-CSCF shall check the value of the Unsupported header field. When the value of the Unsupported header field is path, the P-CSCF shall take OA&M actions to indicate an error, in addition to passing on the 420 response to the UE. In all other cases, the P-CSCF shall proxy the 420 Bad Extension response.

End of first change

5.2.3 Subscription to the users registration-state event package

Upon receipt of a 2xx response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the users registration-state event package at the users registrar (S-CSCF). Therefore the P-CSCF shall generate a SUBSCRIBE request with the following elements:

- a Request-URI set to the topmost entry of the path information that was obtained during the users registration;
- a From header set to a SIP URL that contains the P-CSCF's FQDN;
- a To header, set to a SIP URL that contains the public user identity that was previously registered;
- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher then the Expires header of the before sent REGISTER request from the user; and
- a Route header according to the path information that was obtained during the users registration. Th S-CSCF shall set the last Route header entry to the resource to which it wants to subscribe to, i.e. to a SIP URL the public user identity that was previously registered.

Afterwards the P-CSCF shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE message, the P-CSCF shall store the information for the so established dialog and the expiration time as indicated in the Expires header of the received response.

5.2.4 Registration of multiple public user identites

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package, the P-CSCF shall perform the following actions:

- if a registration state value "open", i.e. registered is received for one or more public user identities, the P-CSCF shall bind the indicated public user identities as registered to the contact information of the user;
- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the P-CSCF shall release all stored information for these public user identities.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. These automatically registered public user identities belong to the same service profile of the user and they are not available at the P-CSCF, i.e. P-CSCF does not know that they have been registered. The here-described procedures provide a mechanism to inform the UE about these automatically registered public user identities.

5.2.5 Deregistration

5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 OK response to a REGISTER request (sent according to subclause 5.2.2), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall remove the public user identity found in the To header field from the registered public user identities list and all related stored information.

NOTE: There is no requirement to distinguish a REGISTER request relating to a registration from that relation to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

5.2.5.2 Network-initiated deregistration

If the P-CSCF has subscribed for the event providing registration state information of a certain public user identity and an incoming NOTIFY request addressed to P-CSCF arrives containing information about network-initiated deregistration, then the P-CSCF shall remove the deregistered public user identity from the registered public user identities list and all related stored information.

Editor's note: The above text came from N1-011984, the text below from N1-011988. The two texts are attempting to specify the same thing. This conflict needs to be resolved in a future contribution.

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package as described in subclause 5.2.3, which contains the registration state value "closed", i.e. deregistered, for one or more public user identities that were previously stored as registered, the P-CSCF shall release all stored information for that public user identity of that user.

If all public user identities that have been bound to one contact information are marked as deregistered, the P-CSCF shall release all resources for that specific user, i.e. the user then is treated as deregistered from the IM CN subsystem.

Start of second change

5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method. Procedures in subsequent clauses to subclause 5.2.6 apply in addition to the procedures of subclause 5.2.6.

5.2.6.2 Requests initiated by the UE

When the P-CSCF receives from the UE an initial request for a dialog, and a Path header list exists for the initiator of the request, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the Path mechanism (see subclause 5.2.3);
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL;
- create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6); and
- forward the request based on the topmost Route header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- remove and store the <charging-function-addresses> ~~<charging-functions>~~ XML element from the message body (see subclause 7.6);
- remove the list of Record-Route headers from the received response; and
- create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE a refresh request for a dialog, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the exchange of the initial request and its associated response;
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL; and
- forward the request based on the topmost Route header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- remove the list of Record-Route headers from the received response; and
- overwrite any existing list of stored Route headers, or create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE the request for a standalone transaction, and a Path header list exists for the initiator of the request, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the Path mechanism (see subclause 7.2.1);
- pre-load the list of Route headers to the request;
- create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6); and
- forward the request based on the topmost Route header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- remove and store the <charging-function-addresses> ~~<charging-functions>~~ XML element from the message body (see subclause 7.6); and
- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE subsequent requests other than a refreshing request that pertains to an existing dialog, the P-CSCF shall:

- select the list of Route headers that was created during the exchange of the initial request and associated response for this call;
- pre-load the list of Route headers to the request; and
- forward the request based on the topmost Route header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, valid or not, from the received response and forward it to the UE.

When the P-CSCF receives from the UE an initial request for a dialog, a refresh request for a dialog, or the request of a standalone transaction, and a Path header list does not exist for the initiator of the request, the P-CSCF shall:

- send a 403 Forbidden response back to the UE containing a warning header.

Editor's Note: how to find out whether the user has a valid registration in the P-CSCF is FFS.

Editor's Note: The correct value for the warning code is yet to be assigned by IANA.

When the P-CSCF receives from the UE the request for an unknown method, and a Path header list exists for the initiator of the request, the P-CSCF shall:

- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the Path mechanism (see subclause 7.2.1);
- pre-load the list of Route headers to the request, and
- forward the request based on the topmost Route header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- remove any list of Record-Route headers, even though invalid, from the received response and forward it to the UE.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the <charging-vector> XML element (see subclause 7.6), if present, from the message body of the received request or response.

5.2.6.3 Requests terminated by the UE

When the P-CSCF receives, destined for the UE, an initial request for a dialog, or a refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

- remove its own SIP URL from the topmost Route header;
- remove the list of Record-Route headers, and shall convert it into a list of Route headers. The Contact header shall not be appended to the bottom of the list of Route headers. The P-CSCF shall save this list of Route headers and append this list to all UE originated requests for this dialog;
- add itself on the top of the removed list of Record-Route headers and save the list. The list will be appended to UE originated response to the SUBSCRIBE request;
- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter . The P-CSCF shall append the list of Via headers to the UE originated response for this request; ~~and~~
- remove and store the <charging-function-addresses> ~~<charging-functions>~~ XML element from the message body (see subclause 7.6); and
- remove and store the <icid> XML element from the message body (see subclause 7.6).

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- append the saved list of Record-Route headers to the response; and,

- append the saved list of Via headers to the response.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- append the saved list of Via headers to the response.

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a refresh request, or a request for a stand-alone transaction, prior to forwarding the request, the P-CSCF shall:

- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter . The P-CSCF shall append this list of Via headers to the UE originated response for this transaction; ~~and~~

- remove and store the <charging-function-addresses> ~~<charging functions>~~ XML element from the message body (see subclause 7.6); and

- remove and store the <icid> XML element from the message body (see subclause 7.6).

When the P-CSCF any response to the above request, the P-CSCF shall:

- append the saved list of Via headers to the response.

When the P-CSCF sends any request or response to the UE, the P-CSCF shall:

- remove the <charging-vector> XML element (see subclause 7.6) from the message body of the request or response.

End of second change

5.2.7 Initial INVITE

5.2.7.1 Determination MO or MT case

Editor's Note: It has to be discussed whether this section is needed or if the determination of MO/MT case at the P-CSCF shall be left implementation dependent.

5.2.7.2 Mobile-originating case

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

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

Editor's note: the case when the P-CSCF acts on behalf of the UE is FFS.

- if a media authorization token is generated by the PCF (i.e. when service-based local policy control is applied), insert the Media Authorization header containing that media authorization token.

When the P-CSCF sends the COMET request towards the S-CSCF, the P-CSCF shall also include the <gprs-charging-id> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging identifier.

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 pre-loaded Route header. The received initial INVITE 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:

Editor's note: the case when the P-CSCF acts on behalf of the UE is FFS.

- if a media authorization token is generated by the PCF (i.e. when service-based local policy control is applied), insert the Media Authorization header containing that media authorization token.

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

When the P-CSCF sends 180 Ringing towards the S-CSCF, the P-CSCF shall also include the <gprs-charging-id> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging identifier.

5.2.7.4 GPRS charging identifier

The GPRS charging identifier is coded as the <gprs-charging-id> XML element within the SIP message body as described in subclause 7.6.

The <gprs-charging-id> XML element contains one <ggsn> child element and one or more <pdp-info> child elements. Each <pdp-info> child XML element within <gprs-charging-id> corresponds to a PDP context that was established at the GGSN for a UE. Each <pdp-info> XML element contains <pdp-id> and <pdp-index> child elements, where <pdp-id> is the PDP context identifier that the P-CSCF obtained from the GGSN and <pdp-index> is the relative index to the media stream in the SDP for the PDP context. The numbering for the <pdp-index> will start at 1 and will be associated with the 'm' lines in the SDP, where the counting is done from top to bottom.

For the messages including the <gprs-charging-id> XML element, set the value of the Content-Type header to include the MIME type specified in subclause 7.6, which may be one part of a multipart message body.

5.2.8 Call release

5.2.8.1 P-CSCF-initiated call release

5.2.8.1.1 Cancellation of a session currently being established

Upon receipt of an indication that radio coverage is no longer available for a served user, for whom one ore more ongoing multimedia session are currently being established, the P-CSCF shall cancel the related dialogs by sending out a CANCEL request according to the procedures described in draft-ietf-sip-rfc2543bis-05 [20].

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that radio coverage is no longer available for a served user, for whom one or more ongoing session exists, the P-CSCF shall release each of the related dialogs by applying the following steps:

1) If the P-CSCF serves the calling user of a session it shall generate a BYE message based on the information saved for the related dialog, including:

   - a Request-URI, set to the topmost entry of the stored routeing information towards the called user;
   - a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog, exclusively the topmost entry (which appears in the Request-URI);
   - further headers, based on local policy or the requested session release reason.

2) If the P-CSCF serves the called user of a session it shall generate a BYE message based on the information saved for the related dialog, including:

   - a Request-URI, set to the topmost entry of the stored routeing information towards the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;

- a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;

- a Route header, set to the routeing information towards the calling user as stored for the dialog, exclusively the topmost entry (which appears in the Request-URI);

- further headers, based on local policy or the requested session release reason.

3) Afterwards the P-CSCF shall send the so generated BYE message towards the indicated user.

4) Upon receipt of the 2xx responses for the BYE request, the P-CSCF shall delete all information related to the dialog and the related multimedia session.

5.2.8.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the P-CSCF initiated session release, the P-CSCF shall terminate this received request and answer it with a 481 Call/Transaction Does Not Exist response.

5.2.8.2 Call release initiated by any other entity

When the P-CSCF receives a 2xx response for a BYE request matching an existing dialog, it shall delete all the stored information related to the dialog.

5.2.9 Subsequent requests

5.2.9.1 Mobile-originating case

For a reINVITE request from the UE, when the P-CSCF sends the COMET request towards the S-CSCF, the P-CSCF shall include the updated <gprs-charging-id> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging identifier.

5.2.9.2 Mobile-terminating case

For a reINVITE request destined towards the UE, when the P-CSCF sends 200 OK response (to the INVITE) towards the S-CSCF, the P-CSCF shall include the updated <gprs-charging-id> XML element in the message body. See subclause 5.2.7.4 for further information on the GPRS charging identifier.

5.2.10 Further initial requests

5.2.10.1 Mobile-originating case

Void.

5.2.10.2 Mobile-terminating case

Void.

5.2.11 Emergency service

The P-CSCF shall inspect the Request URI of all INVITE requests for known emergency numbers and emergency URLs from a configurable list. If the P-CSCF detects that the Request-URI of the INVITE request matches one of the numbers in this list, the INVITE request shall not be forwarded. The P-CSCF shall answer the INVITE request with a 380 Alternative Service response.

The 380 Alternative Service response shall contain a Content-Type header field with the value set to associated MIME type of the 3GPP IMS XML body as described in subclause 7.6.1.

The 3GPP IMS XML body shall contain an <alternative-service> element that indicates the parameters of the alternative service. The <type> child element shall be set to "emergency" to indicate that it was an emergency call. An operator configurable <reason> child element shall be included with a reason phrase.

The P-CSCF shall have a configurable list of emergency numbers and emergency URLs (e.g. sos@domain). The list is used to determine whether the INVITE is destined for an emergency centre or not.

Start of third change

5.3 Procedures at the I-CSCF

5.3.1 Registration procedure

Editor's note: The text on routeing needs to be enhanced to ensure interworking with RFC 2543 and RFC 2543bis networks.

5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [12].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

1) replace the Request-URI of the received REGISTER request with the SIP URL received from the HSS in the Server-Name AVP;

2) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;

2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF. ~~Also, the I-CSCF shall store the <charging-functions> XML element received in the message body (see subclause 7.6).~~

5.3.1.3 Abnormal cases

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 Forbidden response.

If the the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 Temporarily Unavailable response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF; or

- sends back a 3xx or 480 Temporarily Unavailable response;

the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 Busy Everywhere response to the user.

When the I-CSCF receives a 420 Bad Extension response to a REGISTER request, and the Unsupported header contains the value path, the I-CSCF shall take OA&M actions to indicate an error. If the algorithm to select the S-CSCF in 1. above enables an alternative S-CSCF to be selected, then the I-CSCF shall repeat steps 1 through 5 to this new S-CSCF. If no alternative S-CSCF can be selected, the I-CSCF shall proxy the 420 Bad Extension response. In all other cases, the I-CSCF shall proxy the 420 Bad Extension response.

5.3.2 Further initial requests

5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for further initial requests.

When the I-CSCF receives an initial request, not containing a Route header, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [12] for the called user, indicated in the Request-URI.

Upon successful user location query, the I-CSCF shall:

1) insert the URL received from the HSS as the topmost Route header;

2) store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body. If no <icid> XML element was found, then create a new, globally unique value for the <icid> XML element and insert it into the message body;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

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

When the I-CSCF receives an initial request containing a Route header, the I-CSCF shall:

- remove its own SIP URL from the topmost Route header;

- apply the procedures as described in subclause 5.3.3; and

- forward the request based on the topmost Route header if present, or based on the Request-URI, in case no topmost Route header is available.

NOTE: In accordance with SIP the I-CSCF can add its own routeable SIP URL to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the <charging-function-addresses> ~~<charging_functions>~~ XML element from the message body (see subclause 7.6), if present. If the next hop is outside of the current network, then the I-CSCF shall remove the <charging-function-addresses> ~~<charging-functions>~~ XML element from the message body.

5.3.2.2 Abnormal cases

If the HSS sends a negative response to the user location query, the I-CSCF shall send back a 404 Not Found response.

Editor's Note: The procedures for selection of a default S-CSCF are ffs.

If the I-CSCF receives a CANCEL request and if the I-CSCF finds an internal state indicating a pending Cx transaction with the HSS, the I-CSCF:

- shall answer the CANCEL with a 200 OK;

- shall answer the original request with a 487 Request Terminated; and
- shall silently discard the later arriving (pending) Cx answer message from the HSS.

5.3.3 THIG functionality in the I-CSCF(THIG)

5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

All headers which reveal topology information, such as Via, Route, Record-Route, Path, shall be subject to topology hiding. The Refer-To header shall not be subject to topology hiding.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URL of an I-CSCF(THIG) to the top of the Path header.

Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URL to the top of the Record-Route header.

Upon receiving an outgoing initial request for which topology hiding has to be applied and which includes <charging-function-addresses> ~~<charging-functions>~~ XML element in the message body, the I-CSCF(THIG) shall remove the <charging-function-addresses> ~~<charging-functions>~~ XML element from the message body (see subclause 7.6).

5.3.3.2 Encryption for topology hiding

Upon receiving an outgoing request/response from the hiding network the I-CSFC(THIG) shall perform the encryption for topology hiding purposes, i.e. the I-CSCF(THIG) shall:

1) use the whole header values which were added by one or more specific entity of the hiding network as input to encryption, besides the UE entry;
2) not change the order of the headers subject to encryption when performing encryption;
3) use for one encrypted string all received consecutive header entries subject to encryption, regardless if they appear in separate consecutive headers or if they are consecutive entries in a comma separated list in one header;
4) add after the encrypted string a "tokenized-by=" tag, indicating the encrypting network as a parameter;
5) form one valid entry for the specific header out of the resulting string, e.g. add "SIP/2.0/UDP" for Via headers and "sip:" for Route and Record-Route headers.

NOTE 1: Even if consecutive entries of the same network in a specific header are encrypted, they will result in only one encrypted header entry. For example:

```
Via: SIP/2.0/UDP icscf1_s.home1.net,
     SIP/2.0/UDP Token( SIP/2.0/UDP scscf1.home1.net,
                        SIP/2.0/UDP pcscf1.home1.net);tokenized-by=home1.net,
     SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
```

NOTE 2: If multiple entries of the same network are within the same type of headers, but they are not consecutive, then these entries will be tokenized to different strings. For example:

```
Route:  sip:icscf1_s.home1.net,
        sip:Token(sip:scscf1.home1.net);tokenized-by=home1.net,
        sip:as1.foreign.net,
        sip:Token(sip:scscf1.home1.net,
                  sip:pcscf1.home1.net);tokenized-by=home1.net,
        sip:[5555::aaa:bbb:ccc:ddd]
```

5.3.3.3 Decryption for Topology Hiding

Upon receiving and incoming requests/response to the hiding network the I-CSCF(THIG) shall perform the decryption for topology hiding purposes, i.e. the I-CSCF shall:

1) identify encrypted strings within all headers of the incoming message;

2) use all those encrypted strings that carry the identification of the hiding network within the value of the tokenized-by tag as input to decryption;

3) use as encrypted string the data between the sent-protocol (for Via Headers, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route Headers, e.g. "sip:") and the tokenized-by tag;

4) replace all content of the received header which carries encrypted information with the entries resulting from decryption.

EXAMPLE: An encrypted entry to a Via header that looks like:

```
Via:    SIP/2.0/UDP Token(SIP/1.0/UDP scscf1.home1.net,
        SIP/1.0/UDP pcscf1.home1.net);tokenized-by=home1.net
```

will be replace with the following entries:

```
Via: SIP/1.0/UDP scscf1.home1.net, SIP/1.0/UDP pcscf1.home1.net
```

NOTE: Motivations for these decryption procedures are e.g. to allow the correct routeing of a response through the hiding network, to enable loop avoidance within the hiding network, or to allow the entities of the hiding network to change their entries within e.g. the Record-Route header.

End of third change

Start of fourth change

5.4 Procedures at the S-CSCF

Editor's note: The text on routeing needs to be enhanced to ensure interworking with RFC 2543 and RFC 2543bis networks.

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities, (see table A.150/2 and other capabilities in annex A dependent on that major capability).

The S-CSCF shall support the use of the Path header. The S-CSCF must also support the Require and Proxy-Require headers. The Path header is only applicable to the REGISTER request and its 200-OK response.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Normal procedures

When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.

The S-CSCF shall:

- check the existence of a Path header in the request;

Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.

- when a Path header exists in the request, insert its own FQDN, or IP address, in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;

- save the Contact header value for the entire duration of the registration;

- construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;

- include an expiration time in the 200 OK response, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE;

- save the list of preloaded Route headers for the entire duration of the registration;

NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);

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

- bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;

- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;

- check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and

Editor's Note: The method by which the P-CSCF indicates this is FFS.

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

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 Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:

- the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).

5.4.1.2.2 Abnormal cases

In the case that the authentication response from the UE is incorrect the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE is incorrect for three consecutive attempts then the S-CSCF shall deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE indicates that the authentication challenge was invalid with no RES or AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- respond with the relevant 4xx response (e.g. 401 Unauthorized to initiate a further authentication attempt, or 403 Forbidden if the authentication attempt is to be abandoned).

In the case that the response from the UE indicates that the authentication challenge was invalid with the AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation; and
- on receipt of the new vectors send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

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 with a 423 Registration Too Brief, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2.

5.4.1.4 User-initiated deregistration

When the S-CSCF receives a REGISTER request, it shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Requre header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- deregister the subscriber and remove all related stored information;
- insert its own FQDN or IP address in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;
- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response; and

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

5.4.1.5 Network-initiated deregistration

When a network-initiated deregistration event occurs for a public user identity, and the UE has subscribed for that event, the S-CSCF shall generate a NOTIFY request in order to inform the UE of the network-initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

When a network-initiated deregistration event occurs for a public user identity, and the P-CSCF has subscribed for registration events for that public user identity, the S-CSCF shall generate a NOTIFY request in order to inform the P-CSCF of the network initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

If the network-initiated deregistration is for a set of public user identities associated with the subscriber, the NOTIFY shall send the registration state of all public user identities of the subscriber.

Editor's note: The possible values of the event header are: presence, registration-state, a new subpackage of presence.

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

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs (i.e. the dialog between S-CSCF and the UE and additionally between S-CSCF and P-CSCF) which have been established due to subscription to the registration-state event package of that user. The S-CSCF shall populate the content of the NOTIFY request and additionally shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value; and
- indicate a public user identity of the user for which the private user identity needs to be re-authenticated in the body of the NOTIFY request with registration state "re-authenticate".

Afterwards the S-CSCF shall:

- wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication might be requested from the HSS or may occur due to internal processing within the S-CSCF.

In case S-CSCF receives no data it can authenticate the subscriber from, the S-CSCF may as an implementation option try to request the UE by other means to re-authenticate, e.g. by sending a REFER method in order to request a REGISTER message.

If UE does not re-authenticate within a certain period of time, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.

5.4.1.7 Notification of Application Servers about registration status

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each Application Server with the following information:

a) the Request-URI shall contain the FQDN or IP address of the AS in the form of a SIP URL;

b) the From header shall contain the FQDN or IP address of the S-CSCF in the form of a SIP URL;

c) the To header shall contain the public user identity as contained in the REGISTER request received form the UE;

d) the Contact header shall contain the FQDN or IP address of the S-CSCF in the form of a SIP URL;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header shall contain the same value that the S-CSCF returned in the 200 OK response for the REGISTER request received form the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER, such as IMSI to be delivered to IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [12]), then it shall be included in the REGISTER message body within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6.

i) for initial registration, a message body shall be included in the REGISTER request with a <charging-function-addresses> ~~<charging-function>~~ XML element (see subclause ~~7.6~~5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network.

5.4.2 Subscription and notification

Editors Note: This should be handled in a generic way

5.4.2.1 Subscriptions to S-CSCF events

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the registration-state event package, the S-CSCF shall generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the subscription was successful. Furthermore, the response shall include:

- an Expires header which either contains the same or a decreased value as the Expires in SUBSCRIBE request; and
- a Contact header which is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

Editor's note: Authorization needs to be applied before subscribing for the event providing information about the registration state. This is FFS.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

5.4.2.1.2 Notification about registration state

If the registration state of one or more public user identities changes, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the registration-state event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value;
- indicate registration state "open" for all public user identities which are currently registered;
- indicate registration state "closed" for all public user identities which are currently deregistered; and
- indicate within the "<detail>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

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

```
<tuple name="sip:user1_public1@home1.net">
  <status><value>open</value></status>
</tuple>

<tuple name="sip:user1_public2@home1.net">
  <status> <value>open</value> </status>
  <detail>automatically by sip:user1_public1@home1.net</detail>
</tuple>
```

Afterwards the S-CSCF shall send the generated NOTIFY request on the dialog and await a 2xx response.

5.4.2.2 Proxy behaviour for SUBSCRIBE / NOTIFY

Void.

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

5.4.3.1 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:

- remove its own SIP URL from the topmost Route header;
- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. 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 an appropriate SIP response shall be sent to the originator;
- check if <original-dialog-id> XML element is present in the payload 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. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, 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; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- insert a <charging-function-addresses> ~~<charging functions>~~ XML element in the message body (see subclause ~~7.6~~5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

- 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; and

- 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 header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

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

- remove its own URL from the topmost Route header;

- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and

- route the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and

- route the request based on the topmost Route header.

5.4.3.2 Requests terminated at the served user

When the S-CSCF receives, destined for 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:

- remove its own URL from the topmost Route header;

- check if <original-dialog-id> XML element is present in the payload 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. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;

- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. 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; and

  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.

- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;

- insert a <charging-function-addresses> ~~<charging functions>~~ XML element in the message body (see subclause ~~7.6~~5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

- 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 5.4.1.2.1;

- 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 5.4.1.2.1;

- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

5.4.3.3 Original dialog identifier

The original dialog identifier is coded as the <original-dialog-id> XML element within the SIP message body as described in subclause 7.6.

For the messages including the <original-dialog-ID> XML element, set the value of the Content-Type header to include the MIME type specified in subclause 7.6, which may be one part of a multipart message body.

5.4.3.4 Charging function addresses

The charging function addresses shall be coded as the <charging-function-addresses> XML element within the SIP message body as described in subclause 7.6.

The <charging-function-addresses> element shall contain an instance of the <ccf-addr> child element and may contain an instance of the <ecf-addr> child element. The <ccf-addr> element shall contain an instance of the <primary-ccf> child element with the identifier/address of the primary Charging Collection Function (CCF) received from the HSS for offline charging. If the HSS provided one or more secondary CCF addresses, they shall be included in the <secondary-ccf> child element. The <ecf-addr> element, if included, shall contain an instance of the <primary-ecf> child element with the identifier/address of the primary Event Charging Function (ECF) received from the HSS for online charging. If the HSS provided one or more secondary ECF addresses, they shall be included in the <secondary-ecf> child element.

Messages including the 3GPP IMS XML body with the <charging-function-addresses> XML element shall contain a Content-Type header field with the value set to the associated MIME type specified in subclause 7.6, which may be one part of a multipart message body.

5.4.3.45 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using <original-dialog-id> XML element) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an <original-dialog-id> XML element that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.1.1 Determination of served user

Void.

5.4.4.1.2 Mobile-originating case

Void.

5.4.3.1.3 Mobile-terminating case

Void.

5.4.4.2 Subsequent requests

Editor's Note: PRACK and COMET can be handled in a generic way.

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives the 183 response, the S-CSCF shall insert a <charging-function-addresses> ~~<charging-functions>~~ XML element into the message body (see subclause ~~7.6~~5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives the COMET request, the S-CSCF shall remove and store the <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is not included in the message body when the COMET request is forwarded.

When the S-CSCF receives any request or response related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before forwarding the message within the S-CSCF home network, including towards AS.

5.4.3.2.2 Mobile-terminating case

When the S-CSCF sends the 183 response, the S-CSCF shall insert a <charging-function-addresses> ~~<charging-function>~~ XML element into the message body of the outgoing response (see subclause ~~7.6~~5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives 180 Ringing response, the S-CSCF shall remove and store the <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is not included in the message body when the 180 Ringing response is forwarded.

When the S-CSCF receives any request or response related to a mobile-terminated dialog or standalone transaction, the S-CSCF may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before forwarding the message within the S-CSCF home network, including towards AS.

5.4.5 Call release

5.4.5.1 S-CSCF-initiated session release

Void.

5.4.5.1.1 Cancellation of a session currently being established

Upon receipt of an network internal indication to release a session which is currently being established, the S-CSCF shall cancel the related dialogs by sending the CANCEL request according to the procedures described in draft-ietf-sip-rfc2543bis-05 [20].

5.4.5.1.2 Release of an existing session

Upon receipt of a network internal indication to release an existing multimedia session, the S-CSCF shall:

1) generate a first BYE message for the called user based on the information saved for the related dialog, including:
   - a Request-URI, set to the topmost entry of the stored routeing information towards the called user;
   - a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog, exclusively the topmost entry (which appears in the Request-URI);
   - further headers, based on local policy or the requested session release reason.
2) generate a second BYE message for the calling user based on the information saved for the related dialog, including:
   - a Request-URI, set to the topmost entry of the stored routeing information towards the calling user;
   - a To header, set to the From header value as received in the initial INVITE request;
   - a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
   - a Route header, set to the routeing information towards the calling user as stored for the dialog, exclusively the topmost entry (which appears in the Request-URI);
   - further headers, based on local policy or the requested session release reason.
3) If the S-CSCF serves the calling user it shall:
   - treat the first BYE message as if received directly from the calling user, i.e. send it to internal service control and based on the outcome further on towards the called user;
   - send the second BYE message directly to the calling user.
4) If the S-CSCF serves the called user it shall:
   - send the first BYE message directly to the called user;

- treat the second BYE message as if received directly from the called user, i.e. shall send it to internal service control and based on the outcome further on towards to the called user.

Upon receipt of the 2xx responses for both BYE requests, the S-CSCF shall release all information related to the dialog and the related multimedia session.

5.4.4.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the S-CSCF initiated session release, the S-CSCF shall terminate the received request and answer it with a 481 Call/Transaction Does Not Exist response.

5.4.4.2 Session release initiated by any other entity

Upon receipt of a 2xx response for a BYE request matching an existing dialog, the S-CSCF shall delete all the stored information related to the dialog.

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

5.4.6.1.2 Mobile-originating case

For a reINVITE request from the UE, when the S-CSCF receives the COMET request, the S-CSCF shall remove and store the updated <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is not included in the message body when the COMET request is forwarded.

5.4.6.1.3 Mobile-terminating case

For a reINVITE request destined towards the UE, when the S-CSCF receives the 200 OK response (to the INVITE), the S-CSCF shall remove and store the updated <gprs-charging-id> XML element from the message body (see subclause 7.6). The <gprs-charging-id> XML element is not included in the message body when the 200 OK response is forwarded.

5.4.6.2 REFER

5.4.6.2.1 Mobile-originating case

Void.

5.4.6.2.2 Mobile-terminating case

Void.

5.4.6.2.3 REFER initiating a new session

Void.

5.4.6.2.4 REFER replacing an existing session

Void.

5.4.6.3 INFO

Editor's Note: It has to be determined which of these requests can be handled in a generic way.

5.4.7 Further initial requests

Editor's Note: Generic handling of e.g. OPTIONS should be described here

End of fourth change

Start of fifth change

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore the dependencies of table 0.3/1 and table 0.3/2 shall not apply.

The use of the Path header shall not be supported by the MGCF.

When the MGCF sends any request or response related to a dialog or standalone transaction, the MGCF may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before sending the message.

5.5.2 Subscription and notification

5.5.2.1 Subscriptions to MGCF events

Void.

5.5.2.2 Gateway behaviour for SUBSCRIBE / NOTIFY

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see draft-ietf-sip-manyfolks-resource [22]); and
  - create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6).

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request, the MGCF shall:

- send 100 "Trying" response;
- assuming the "100rel" indicator was received and a matching codec is found,send 183 "Session Progress" response:

- set the Require header to the value of "100rel";
- set the Content-Disposition header to the value of "precondition"; ~~and~~
- store the value of the <icid> XML element received in the message body (see subclause 7.6~~).~~); and
- store the values of the <charging-function-addresses> ~~<charging-functions>~~ XML element received in the message body (see subclause 7.6).

Editor's note: must receive Supports header with value of 100rel in the INVITE.

Editor's note: need text to describe error legs.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- store the values of the <charging-function-addresses> ~~<charging-functions>~~ XML element received in the message body (see subclause 7.6).

When the MGCF receives 200 OK response to a PRACK request and notification that bearer setup is complete, the MGCF shall:

- send a COMET request.

5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 "Ringing" to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 OK to the UE.

5.5.4 Call release

5.5.4.1 Call release initiated by a circuit-switched network

When the MGCF receives an indication of call release from a circuit-switched network, the MGCF shall:

- send a BYE request to the UE.

5.5.4.2 S-CSCF-initiated call release

5.5.4.3 MGW-initiated call release

When the MGCF receives an indication from the MGW that the bearer was lost, the MGCF shall:

- send a BYE request towards the UE.

Editor's note: should the Error-Info header be used to indicate an error case for the session release?

5.5.5 Call-related requests

5.5.5.1 ReINVITE

5.5.5.1.1 Calls originating from circuit-switched networks

Editor's Note: When the bearer on the circuit-switched network side is halted/resumed, should the MGCF notify the UE with a reINVITE?

5.5.5.1.2 Calls terminating in circuit-switched networks

When the MGCF receives a reINVITE request for hold/resume operation, the MGCF shall:

- send 100 Trying response;
- after performing interaction with MGW to hold/resume the media flow, send 200 OK response.

5.5.5.2 REFER

5.5.5.2.1 Calls originating from circuit-switched networks

Void.

5.5.5.2.2 Calls terminating in circuit-switched networks

Void.

5.5.5.2.3 REFER initiating a new session

Void.

5.5.5.2.4 REFER replacing an existing session

Void.

5.5.5.3 INFO

Void.

5.5.6 Further initial requests

When the MGCF responds to an OPTIONS request with a 200 OK response, the MGCF may include a message body with an indication of the DTMF capabilities and supported codecs of the MGCF/MGW.

Editor's note: it is FFS how to identify the resources of the MGCF/MGW.

End of fifth change

Start of sixth change

5.6 Procedures at the BGCF

5.6.1 General

The use of the Path header shall not be supported by the BGCF.

When the BGCF receives any request or response related to a dialog or standalone transaction, the BGCF may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before forwarding the message.

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. The BGCF shall store the values of the <icid> and <charging-function-addresses> ~~<charging-functions>~~ XML elements received in the message body (see subclause 7.6) and retain the <icid> and <charging-function-addresses> ~~<charging-functions>~~ XML elements in the message body.

NOTE: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

End of sixth change

Start of seventh change

5.7 Procedures at the Application Server (AS)

NOTE: This subclause defines only the requirements on the application server that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

5.7.1 Common Application Server (AS) Procedures

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 OK or an appropriate failure response. For the success case, the 200 OK response shall contain Expires value equal to the value received in the REGISTER request. Also, the AS shall store the values of the <icid> and <charging-function-addresses> ~~<charging-functions>~~ XML elements received in the REGISTER message body (see subclause 7.6).

5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the values of the <icid> and <charging-function-addresses> ~~<charging-functions>~~ XML elements received in the message body (see subclause 7.6) and retain the <icid> and <charging-function-addresses> ~~<charging-functions>~~ XML elements in the message body.

When an AS sends any request or response related to a dialog or standalone transaction, the AS may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before sending the message.

5.7.2 Application Server (AS) acting as terminating UA, or redirect server

Editors Note: When acting as a terminating UA the AS shall behave as defined for a UE in 5.1.4.

The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes an <original-dialog-id> XML element in these requests, the AS shall include this <original-dialog-id> XML element in any responses and/or subsequent requests sent on this dialog.

An Application Server acting as redirect server shall propagate any received 3GPP message body in the redirected message.

5.7.3 Application Server (AS) acting as originating UA

Editors Note: When acting as an originating UA the AS shall behave as defined for a UE in 5.1.3.

When an AS acting as originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6).

5.7.4 Application Server (AS) acting as a SIP proxy

The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes an <original-dialog-id> XML element in these requests, the AS shall include this <original-dialog-id> XML element in any responses and/or subsequent requests sent on this dialog.

When the AS acting as a SIP proxy receives a request from the S-CSCF, prior to forwarding the request it shall:

- remove its own URL from the topmost Route header; and
- after executing the required services, route the request based on the topmost Route header.

The AS may modify the SIP requests based on service logic, prior to forwarding the request back to the S-CSCF.

An Application Server acting as a SIP proxy shall propagate any received 3GPP message body in the forwarded message.

5.7.5 Application Server (AS) performing 3rd party call control

5.7.5.1 General

The AS performing 3rd party call control acts as a B2BUA. The B2BUA AS will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. These decisions are specific to each AS and are outside the scope of the present document.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

5.7.5.2 Call initiation

5.7.5.2.1 Initial INVITE

When the AS receives an initial INVITE request, it will contain the AS's SIP URL in the Request-URI. Before generating a new INVITE back to the S-CSCF, the AS:

- performs the Application Server specific functions. See 3GPP TS 23.218 [5]; and
- if successful, generate and send a new INVITE request to the S-CSCF to establish a new dialog. The AS shall look for the presence of the <original-dialog-id> XML element in the message body of the initial INVITE request and populate the same <original-dialog-id> XML element in the message body of the new INVITE request.

5.7.5.2.2 Subsequent requests

Editor's Note: subsequent requests can be handled in a generic way. Is there anything needed here?

5.7.5.3 Call release

5.7.5.4 Call-related requests

Editor's Note: call-related requests can be handled in a generic way. Is there anything needed here?

An Application Server may initiate a call release. See 3GPP TS 23.218 [5] for possible reasons. The BYE request shall be sent simultaneously for both dialogs managed by the B2BUA.

5.7.5.5 Further initial requests

Editor's Note: call-related requests can be handled in a generic way. Is there anything needed here?

End of seventh change

Start of eighth change

5.8 Procedures at the MRFC

5.8.1 General

Void.

5.8.2 Call initiation

5.8.2.1 Initial INVITE

5.8.2.1.1 MRFC-terminating case

When the MRFC receives an initial INVITE request, the MRFC shall store the values of the <icid> and <charging-function-addresses> ~~<charging-functions>~~ XML elements received in the message body (see subclause 7.6).

5.8.2.1.1.1 Tones and announcements

The MRFC can receive INVITE requests to set up a session to play tones and announcements. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for a tone or announcement, the MRFC shall:

- send 100 Trying response.

Editor's note: it is FFS how to identify the tone or announcement to be played.

5.8.2.1.1.2 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (e.g. Multiparty Call) or to add parties from the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator to initiate ad hoc conferencing, the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conference resources are available, send 200 OK response with an MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

When the MRFC receives an INVITE request with an indicator to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

Editor's note: it is FFS how to identify the resources of the MRFC/MRFP.

5.8.2.1.1.3 Transcoding

The MRFC may receive INVITE requests to set up transcoding between endpoints with incompatible codecs. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for transcoding and a codec is supplied in SDP, the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the transcoding request is granted, send 200 OK response.

When the MRFC receives an INVITE request with an indicator for transcoding but no SDP, the MRFC shall:

- send 183 Session Progress response with list of codecs supported by the MRFC/MRFP.

5.8.2.1.2 MRFC-originating case

Void.

5.8.2.2 Subsequent requests

When the MRFC sends any request or response related to a dialog or standalone transaction, the MRFC may insert previously saved values into <charging-vector> and <charging-function-addresses> XML elements (see subclause 7.6) into the message body before sending the message.

Editor's Note: PRACK and COMET can be handled in a generic way.

5.8.2.2.1 Tones and announcements

When the MRFC receives an ACK request for a session, this may be considered as an event to direct the MRFP to start the playing of a tone or announcement.

5.8.3 Call release

5.8.3.1 S-CSCF-initiated call release

5.8.3.1.1 Tones and announcements

When the MRFC receives a BYE request for a session, the MRFC shall direct the MRFP to stop the playing of a tone or announcement.

5.8.3.2 MRFC-initiated call release

5.8.3.2.1 Tones and announcements

When the MRFC has a timed session to play tones and announcements and the time expires, the MRFC shall:

- send a BYE request towards the UE.

When the MRFC is informed by the MRFP that tone or announcement resource has been released, the MRFC shall:

- send a BYE request towards the UE.

5.8.2.2.2 Transcoding

When the MRFC receives a PRACK request (in response to the 183) with an indicator for transcoding and codec supplied in SDP, the MRFC shall:

- after the MRFP indicates that the transcoding request is granted, send 200 OK response.

5.8.4 Call-related requests

5.8.4.1 ReINVITE

5.8.4.1.1 MRFC-terminating case

5.8.4.1.1.1 Ad-hoc conferences

The MRFC can receive reINVITE requests to modify an ad-hoc conferencing session (e.g. Multiparty Call) for purposes of floor control and for parties to leave and rejoin the conference.

When the MRFC receives a reINVITE request, the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

Editor's note: it is FFS how to identify the resources of the MRFC/MRFP.

5.8.4.1.2 MRFC-originating case

Void.

5.8.4.2 REFER

5.8.4.2.1 MRFC-terminating case

Void.

5.8.4.2.2 MRFC-originating case

Void.

5.8.4.2.3 REFER initiating a new session

Void.

5.8.4.2.4 REFER replacing an existing session

Void.

5.8.4.3 INFO

Editor's Note: It has to be determined which of these requests can be handled in a generic way.

5.8.5 Further initial requests

When the MRFC responds to an OPTIONS request with a 200 OK response, the MRFC may include a message body with an indication of the supported tones/announcement packages, DTMF capabilities, supported codecs and conferencing options of the MRFC/MRFP.

Editor's note: it is FFS how to identify the resources of the MRFC/MRFP.

End of eighth change

Start of ninth change

7.6 3GPP IM CN subsystem XML body, version 1

7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The <icid> XML element is an exception to this rule; it may only be removed by the P-CSCF. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

7.6.2 Document Type Definition

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (vnid?, cell-id?,
        original-dialog-id?, destination-public-user-id?,
        access?, charging-vector?, charging-function-addresses?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- vnid element: Visited network identity -->
    <!ELEMENT vnid              (#PCDATA)>

    <!-- cell-id element: The Cell-Global-ID -->
    <!ELEMENT cell-id               (mcc, mnc, lac, ci)>
    <!ELEMENT mcc                   (#PCDATA)>
    <!ELEMENT mnc                   (#PCDATA)>
    <!ELEMENT lac                   (#PCDATA)>
    <!ELEMENT ci                    (#PCDATA)>
    <!ATTLIST cell-id rat (utran | geran)   #REQUIRED>

    <!-- original-dialog-id: original dialog ID -->
    <!ELEMENT original-dialog-id (od-from, od-to, od-call-id)>
    <!ELEMENT od-from               (#PCDATA)>
    <!ELEMENT od-to                 (#PCDATA)>
    <!ELEMENT od-call-id            (#PCDATA)>

    <!-- public-user-id: public user ID -->
    <!ELEMENT destination-public-user-id    (#PCDATA)>

    <!-- access: the type of access network →
    <!ELEMENT access            (access-type, technology?)>
    <!ELEMENT access-type   (gprs | wlan | fixed | (#PCDATA))>
    <!ELEMENT technology    (utran| geran | 802.11a |
                802.11b | sat | adsl | (#PCDATA))>

    <!-- charging-vector element: Charging Vector -->
    <!ELEMENT charging-vector       (icid, charging-functions?, gprs-charging-id?)>

    <!-- icid element: IMS charging identifier -->
    <!ELEMENT icid                  (#PCDATA)>

    <!-- charging-functions element: offline and online charging function identifiers -->
    <!ELEMENT charging-functions    (ccf*, ecf*)>
    <!-- ccf element: offline charging collection function identifier -->
    <!ELEMENT ccf                   (#PCDATA)>
    <!-- ecf element: online event charging function identifier -->
    <!ELEMENT ecf                   (#PCDATA)>

    <!-- gprs-charging-id element: GPRS charging identifiers -->
    <!ELEMENT gprs-charging-id      (ggsn, pdp-info+)>
    <!ELEMENT ggsn                  (#PCDATA)>
```

```
    <!ELEMENT pdp-info              (pdp-index, pdp-id)>
    <!ELEMENT pdp-index             (#PCDATA)>
    <!ELEMENT pdp-id                (#PCDATA)>

    <!-- charging-function-addresses element: offline and online charging function addresses -->
    <!ELEMENT charging-function-addresses   (ccf-addr, ecf-addr?)>

    <!-- ccf element: offline charging collection function identifiers -->
    <!ELEMENT ccf-addr              (primary-ccf, secondary-ccf*)>
    <!ELEMENT primary-ccf           (#PCDATA)>
    <!ELEMENT secondary-ccf         (#PCDATA)>
    <!-- ecf element: online event charging function identifiers -->
    <!ELEMENT ecf-addr              (primary-ecf, secondary-ecf*)>
    <!ELEMENT primary-ecf           (#PCDATA)>
    <!ELEMENT secondary-ecf         (#PCDATA)>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition.

<ims-3gpp>: This is the root element of the 3GPP IMS XML body. It shall always be present. The version described in the present document is 1.

<vnid>: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.

<cell-id>: This element describes the identity of the cell that is serving the user.

The <cell-id> element contains the <ran> attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.

The <cell-id> element comprises four children elements: <mcc>, <mnc>, <lac> and <ci>. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].

<original-dialog-id>:The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies then dialogue.

The original-dialog-id element comprises three children elements: <od-from>, <od-to>, <od-call-id>. Their values contain, respectively, a copy of the From, To and Call-ID header values as received in the SIP message at the S-CSCF.

<destination-public-user-id>: The destination public-user-id URL of the current session.

<access>: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: <ant> and <technology>.

The <access-type> child element describes the access type. The predefined values are:

- gprs: the user is accessing the network through a GRPS access;
- wlan: the user is accessing the network through a wireless local area network;
- fixed: the user is accessing the network through a fixed access.

The <technology> child element, if present, describes the access technology. The pre-defined values are:

- utran: UTRAN, as defined in [3];
- geran: GERAN, as defined in [3];
- 802.11a: wireless local area network according to the 802.11a technology;
- 802.11b: wireless local area network according to the 802.11b technology;
- sat: satellite access;
- adsl: asymmetric digital subscriber line.

<charging-vector>: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: <icid> and <gprs-charging-id>.

The <icid> child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.

~~The <charging-functions> child element, if present, contains one or more instances of two possible child elements for off-line and on-line charging network entities: <ccf> and <ecf>:~~

~~- <ccf>: off-line charging collection function identifier;~~

~~- <ecf>: on-line event charging function identifier.~~

The <gprs-charging-id> child element, if present, contains GPRS charging identifiers comprised of the following: <ggsn> and <pdp-info>:

- <ggsn>: identifier of the GGSN;
- <pdp-info>: one or more instances of information for a PDP context, which is comprised of two children elements: <pdp-index> and <pdp-id>:
  - <pdp-index>: relative index of PDP context as it correlates to a media stream in the SDP;
  - <pdp-id>: unique identifier of the PDP context from the GGSN.

<charging-function-addresses> the charging-function-addresses element, if present, contains one or two child elements for offline and online charging network entities: <ccf-addr> and <ecf-addr>:

- <ccf-addr>: offline charging collection function identifiers, consisting of one <primary-ccf> and zero or more <secondary-ccf>;
- <ecf-addr>: optional online event charging function identifiers, consisting of one <primary-ecf> and zero or more <secondary-ecf>.

<service-info>: the transparent element received from the HSS for a particular Application Server are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

End of ninth change

3GPP TSG-CN1 Meeting #23 ***Tdoc N1-020787***
Fort Lauderdale, Florida, USA 08. - 12. April 2002

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **018** ⌘ **rev** **-** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Corrections to original-dialog-id
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	01.04.2002
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)

Reason for change:	⌘	IETF rfc2543bis-09 (soon to be RFC 3261) now identifies a dialog with tag fields on the To and From headers instead of using the To and From header values directly. The definition and use of the original-dialog-id field needs to be updated to align with the IETF change.
Summary of change:	⌘	The XML definition is updated to change the sub-elements od-from and od-to to be called od-from-tag and od-to-tag. Procedures are modified to describe populating the od-from-tag and od-to-tag sub-elements with the tag fields of the To and From headers.
Consequences if not approved:	⌘	The To and From headers (plus call-id) will not be unique for identifying the dialog. As such, false positive matches would happen when try to compare a saved dialog-id with a received message.

Clauses affected:	⌘	5.4.3.1, 5.4.3.2, 5.4.3.3, 7.6.2, 7.6.3
Other specs affected:	⌘	☐ 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/3G_Specs/CRs.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

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

5.4.3.1 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:

- remove its own SIP URL from the topmost Route header;
- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. 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 an appropriate SIP response shall be sent to the originator;
- check if <original-dialog-id> XML element is present in the payload 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. The <od-to-tag>, <od-from-tag> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, 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; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- 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; and
- 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 header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- route the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- route the request based on the topmost Route header.

5.4.3.2 Requests terminated at the served user

When the S-CSCF receives, destined for 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:

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload 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. The <od-to-tag>, <od-from-tag> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. 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; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- 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 5.4.1.2.1;
- 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 5.4.1.2.1;
- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

5.4.3.3 Original dialog identifier

The original dialog identifier is coded as the <original-dialog-id> XML element within the SIP message body as described in subclause 7.6.

For the messages including the 3GPP IMS XML body, e.g. due to the inclusion of the <original-dialog-ID> XML element, set the value of the Content-Type header to include the MIME type specified in subclause 7.6, which may be one part of a multipart message body.

5.4.3.4 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using <original-dialog-id> XML element) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an <original-dialog-id> XML element that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

End of first change

Start of second change

7.6 3GPP IM CN subsystem XML body, version 1

7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The <icid> XML element is an exception to this rule; it may only be removed by the P-CSCF. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

7.6.2 Document Type Definition

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (vnid?, cell-id?,
        original-dialog-id?, destination-public-user-id?,
        access?, charging-vector?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- vnid element: Visited network identity -->
    <!ELEMENT vnid              (#PCDATA)>

    <!-- cell-id element: The Cell-Global-ID -->
    <!ELEMENT cell-id               (mcc, mnc, lac, ci)>
    <!ELEMENT mcc                   (#PCDATA)>
    <!ELEMENT mnc                   (#PCDATA)>
    <!ELEMENT lac                   (#PCDATA)>
    <!ELEMENT ci                    (#PCDATA)>
    <!ATTLIST cell-id rat (utran | geran)   #REQUIRED>

    <!-- original-dialog-id: original dialog ID -->
    <!ELEMENT original-dialog-id (od-from-tag, od-to-tag, od-call-id)>
    <!ELEMENT od-from-tag           (#PCDATA)>
    <!ELEMENT od-to-tag             (#PCDATA)>
    <!ELEMENT od-call-id            (#PCDATA)>

    <!-- public-user-id: public user ID -->
    <!ELEMENT destination-public-user-id    (#PCDATA)>

    <!-- access: the type of access network →
    <!ELEMENT access            (access-type, technology?)>
    <!ELEMENT access-type   (gprs | wlan | fixed | (#PCDATA))>
    <!ELEMENT technology    (utran| geran | 802.11a |
                802.11b | sat | adsl | (#PCDATA))>

    <!-- charging-vector element: Charging Vector -->
    <!ELEMENT charging-vector       (icid, gprs-charging-id?)>

    <!-- icid element: IMS charging identifier -->
    <!ELEMENT icid                  (#PCDATA)>
    <!-- gprs-charging-id element: GPRS charging identifiers -->
    <!ELEMENT gprs-charging-id      (ggsn, pdp-info+)>
    <!ELEMENT ggsn                  (#PCDATA)>
    <!ELEMENT pdp-info              (pdp-index, pdp-id)>
    <!ELEMENT pdp-index             (#PCDATA)>
    <!ELEMENT pdp-id                (#PCDATA)>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition.

<ims-3gpp>: This is the root element of the 3GPP IMS XML body. It shall always be present. The version described in the present document is 1.

<vnid>: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.

<cell-id>: This element describes the identity of the cell that is serving the user.

The <cell-id> element contains the <ran> attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.

The <cell-id> element comprises four children elements: <mcc>, <mnc>, <lac> and <ci>. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].

<original-dialog-id>: The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies the~~n~~ dialogue.

The original-dialog-id element comprises three children elements: <od-from-tag>, <od-to-tag>, <od-call-id>. Their values contain, respectively, a copy of the From tag, To tag and Call-ID header values as received in the SIP message at the S-CSCF.

<destination-public-user-id>: The destination public-user-id URL of the current session.

<access>: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: <ant> and <technology>.

The <access-type> child element describes the access type. The predefined values are:

- gprs: the user is accessing the network through a GRPS access;
- wlan: the user is accessing the network through a wireless local area network;
- fixed: the user is accessing the network through a fixed access.

The <technology> child element, if present, describes the access technology. The pre-defined values are:

- utran: UTRAN, as defined in [3];
- geran: GERAN, as defined in [3];
- 802.11a: wireless local area network according to the 802.11a technology;
- 802.11b: wireless local area network according to the 802.11b technology;
- sat: satellite access;
- adsl: asymmetric digital subscriber line.

<charging-vector>: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: <icid> and <gprs-charging-id>.

The <icid> child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.

The <gprs-charging-id> child element, if present, contains GPRS charging identifiers comprised of the following: <ggsn> and <pdp-info>:

- <ggsn>: identifier of the GGSN;
- <pdp-info>: one or more instances of information for a PDP context, which is comprised of two children elements: <pdp-index> and <pdp-id>:
  - <pdp-index>: relative index of PDP context as it correlates to a media stream in the SDP;
  - <pdp-id>: unique identifier of the PDP context from the GGSN.

<service-info>: the transparent element received from the HSS for a particular Application Server are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

End of second change