

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 9 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 | 101 | | Rel-5 | Editor's note cleanup - clause 3 | F | 5.0.0 | 5.1.0 | N1-24 | N1-021174 |
| 24.229 | 102 | | Rel-5 | Editor's note cleanup - clause 4 | F | 5.0.0 | 5.1.0 | N1-24 | N1-021175 |
| 24.229 | 103 | | Rel-5 | Editor's note cleanup - clause 5.1 and deletion of void subclauses | F | 5.0.0 | 5.1.0 | N1-24 | N1-021176 |
| 24.229 | 104 | 1 | Rel-5 | Editor's note cleanup - clause 5.2 and deletion of void subclauses | F | 5.0.0 | 5.1.0 | N1-24 | N1-021487 |
| 24.229 | 105 | | Rel-5 | Editor's note cleanup - clause 5.3 | F | 5.0.0 | 5.1.0 | N1-24 | N1-021178 |
| 24.229 | 106 | | Rel-5 | Editor's note cleanup - clause 5.4 and deletion of void subclauses | F | 5.0.0 | 5.1.0 | N1-24 | N1-021179 |
| 24.229 | 107 | | Rel-5 | Editor's note cleanup - clause 5.5 and deletion of void subclauses | F | 5.0.0 | 5.1.0 | N1-24 | N1-021180 |
| 24.229 | 110 | | Rel-5 | Editor's note cleanup - clause 6 | F | 5.0.0 | 5.1.0 | N1-24 | N1-021183 |
| 24.229 | 111 | | Rel-5 | Editor's note cleanup - clause 9 | F | 5.0.0 | 5.1.0 | N1-24 | N1-021184 |

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 101** ⌘ 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

| | | | |
|------------------------|--|-----------------|--|
| Title: | ⌘ Editor's note cleanup - clause 3 | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) REL-4 (Release 4) REL-5 (Release 5) |

| | |
|--------------------------------------|--|
| Reason for change: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ The editor's notes in clause 3 refer to definitions that are in RFC 3261 but cannot be found in the definitions clause of that RFC. A solution has been found to make these references, and therefore the notes can be deleted. In addition, a number of additional terms have been added to the definitions list extracted from RFC 3261. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | | |
|------------------------------|---|---|--|
| Clauses affected: | ⌘ 3 | | |
| Other specs affected: | <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> 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.

3 Definitions and abbreviations

3.1 Definitions

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

Header:

~~Editor's note: To be provided.~~

~~**Option-tag:** unique identifiers used to designate new options in SIP
These tags are used in Require, Supported and Unsupported header fields.~~

~~Editor's note: Text extracted from RFC2543bis, but not specified as a definition.~~

~~**Redirect server:** a server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client~~

~~Unlike a proxy server, it does not initiate its own SIP request. Unlike a user agent server, it does not accept calls.~~

~~Editor's note: Previous version of this definition was in the bis draft, but has now been removed. Requires further study as to whether there is a more preferred term.~~

~~**Status-code:** a 3-digit integer result code that indicates the outcome of the attempt to understand and satisfy the request~~

~~Editor's note: Text extracted from RFC2543bis, but not specified as a definition.~~

For the purposes of the present document, the following terms and definitions given in RFC 2543bis [20] (*Editor's note – working title*) apply ([unless otherwise specified see clause 6](#)).

Client

Dialog

[Final response](#)

[Header](#)

[Header field](#)

[Loose routing](#)

Method

[Option-tag](#) (see RFC 3261 [20] subclause 19.2)

[Provisional response](#)

Proxy, proxy server

[Redirect server](#)

Registrar

[Request](#)

[Response](#)

Server

Session

(SIP) transaction

Stateful proxy

Stateless proxy

[Status-code](#) (see RFC 3261 [20] subclause 7.2)

[Tag](#) (see RFC 3261 [20] subclause 19.3)

User agent client (UAC)

User agent server (UAS)

User agent (UA)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4a.7 apply:

Breakout Gateway Control Function (BGCF)

Call Session Control Function (CSCF)

Media Gateway Control Function (MGCF) Media Resource Function Controller (MRFC)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclause 4.3.3.1 and subclause 4.6 apply:

Interrogating-CSCF (I-CSCF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

User Equipment (UE)

3.2 Abbreviations

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

| | |
|--------|---|
| 1xx | A status-code in the range 101 through 199, and excluding 100 |
| 2xx | A status-code in the range 200 through 299 |
| AS | Application Server |
| AUTN | Authentication TokeN |
| BGCF | Breakout Gateway Control Function |
| c | conditional |
| CK | Ciphering Key |
| CN | Core Network |
| CSCF | Call Session Control Function |
| DNS | Domain Name System |
| FQDN | Fully Qualified Domain Name |
| i | irrelevant |
| I-CSCF | Interrogating CSCF |
| IK | Integrity Key |
| IM | IP Multimedia |
| IP | Internet Protocol |
| ISC | IP multimedia Subsystem Service Control |
| m | mandatory |
| MAC | Message Authentication Code |
| MGCF | Media Gateway Control Function |
| MRFC | Media Resource Function Controller |
| n/a | not applicable |
| o | optional |
| P-CSCF | Proxy CSCF |
| PDU | Protocol Data Unit |
| RAND | RANDom challenge |
| RES | RESponse |
| RTP | Real-time Transport Protocol |
| S-CSCF | Serving CSCF |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SQN | SeQuence Number |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UE | User Equipment |
| URI | Universal Resource Identifier |
| URL | Universal Resource Locator |
| x | prohibited |

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 102** ⌘ 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

| | | | |
|------------------------|---|-----------------|---|
| Title: | ⌘ Editor's note cleanup - clause 4 | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | <i>Use one of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | <i>Use one of the following releases:</i> 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: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ The editor's note in 4.2 is deleted, no further work is required in this area for release 5. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | | |
|------------------------------|---|---|--|
| Clauses affected: | ⌘ 4.2 | | |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications ⌘ <input type="checkbox"/> 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.

4 General

4.1 Conformance of IM CN subsystem entities to SIP

SIP defines a number of roles which entities can implement in order to support capabilities. These roles are defined in annex A.

Each IM CN subsystem functional entity using an interface at the Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point and the Mw reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP, as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

The Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point and the Mw reference point are defined in 3GPP TS 23.002 [2]

The Mr reference point is defined in 3GPP TS 23.228 [7].

The ISC interface is defined in 3GPP TS 23.228 [7] subclause 4.2.4.

- The User Equipment (UE) shall provide the User Agent (UA) role with the exceptions and additional capabilities as described in subclause 5.1.
- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.2. When acting as the subscriber to or the recipient of event information, the P-CSCF shall provide the UA role, again with the exceptions and additional capabilities as described in subclause 5.2.
- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.
- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4. The S-CSCF shall provide the UA role with the additional capabilities as described in subclause 5.4. The S-CSCF shall also act as a registrar, with the exceptions and additional capabilities as described in subclause 5.4. However, as the notifier of event information the S-CSCF shall provide the UA role, again with the exceptions and additional capabilities as described in subclause 5.4.
- The BGCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.5.
- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.6.
- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5]), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2.
- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5]), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3.
- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5]), shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.
- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5]), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5.
- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8.

4.2 URL and address assignments

In order for SIP and SDP to operate, the following preconditions apply:

- 1) I-CSCFs used in registration are allocated FQDNs. Other IM CN subsystem entities may be allocated FQDNs. How these addresses are assigned to the logical entities is up to the network operator. For example, a single FQDN may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or a separate FQDN may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

~~Editor's note: The requirements for DNS SRV entries or alternatives require further discussion.~~

- 2) All IM CN subsystem entities are allocated IP addresses. Allocation of IPv6 and IPv4 addresses fulfils the requirements of of 3GPP TS 23.221 [6] subclause 5.1.
- 3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the USIM. This private user identity is available to the SIP application within the UE.

NOTE: The FQDNs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

- 4) The subscriber is allocated one or more public user identities by the home network operator. At least one of these is contained within the USIM. All public user identities are available to the SIP application within the UE.
- 5) The UE is dynamically assigned an IP version 6 address.

4.3 Routeing principles of IM CN subsystem entities

Each IM CN subsystem functional entity shall apply loose routeing policy as described in RFC 2543bis [20] with the following restrictions, when processing a SIP request.

CHANGE REQUEST

⌘ **24.229 CR 103** ⌘ 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

| | | | |
|------------------------|---|-----------------|--|
| Title: | ⌘ Editor's note cleanup - clause 5.1 and deletion of void subclauses | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | <p>Use <u>one</u> of the following categories:</p> <p>F (correction)</p> <p>A (corresponds to a correction in an earlier release)</p> <p>B (addition of feature),</p> <p>C (functional modification of feature)</p> <p>D (editorial modification)</p> <p>Detailed explanations of the above categories can be found in 3GPP TR 21.900.</p> | | <p>Use <u>one</u> of the following releases:</p> <p>2 (GSM Phase 2)</p> <p>R96 (Release 1996)</p> <p>R97 (Release 1997)</p> <p>R98 (Release 1998)</p> <p>R99 (Release 1999)</p> <p>REL-4 (Release 4)</p> <p>REL-5 (Release 5)</p> |

| | |
|--------------------------------------|---|
| Reason for change: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ The editor's note in clause 5.1.1.7 is deleted - it is not considered necessary to specify what occurs at the UE if all public user identities of one user have been deregistered, e.g. by releasing signalling PDP context, providing information to the user. The editor's note in clause 5.1.2.2 is deleted - this relates to future usage of further subclauses, and will not apply to release 5. The editor's note in clause 5.1.3 is deleted. The remainder of the unused subclauses in 5.1.3 are deleted, as it is not clear that these subclauses will ever be used in their current form. The editor's note in clause 5.1.4 is deleted. The remainder of the unused subclauses in 5.1.4 are deleted, as it is not clear that these subclauses will ever be used in their current form. The unused subclauses in 5.1.5 are deleted, as it is not clear that these subclauses will ever be used in their current form. The unused subclauses 5.1.6 and 5.1.7 are deleted as it is not clear these subclauses will ever be used in their current form. As a result, subclause 5.1.8 is renumbered. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | |
|--------------------------|--|
| Clauses affected: | ⌘ 5.1.1.7, 5.1.2.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8 |
| Other specs | ⌘ <input type="checkbox"/> Other core specifications ⌘ |

| | | |
|------------------------|--|--|
| affected: | <input type="checkbox"/> Test specifications | |
| | <input type="checkbox"/> 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.

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.

5.1.1.5 Authentication

5.1.1.5.1 General

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

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

- check the validity of a received authentication challenge, as described in 3GPP TS 33.102 [13] i.e. the locally calculated MAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range.

In the case that the 401 Unauthorized response is deemed to be valid the UE shall:

- extract the RAND and AUTN parameters, and use the derived keys (CK and IK) to protect future messages, see 3GPP TS 33.203 [14]; and
- send another REGISTER request using the derived IK to integrity protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter).

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

5.1.1.5.2 Network-initiated re-authentication

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package, which contains the registration state value "re-authenticate" for a public user identity, the UE shall start the re-authentication procedures by initiating a reregistration as described in subclause 5.1.1.4.

5.1.1.5.3 Abnormal cases

If, in a 401 Unauthorized response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER shall contain no response parameter (e.g. no RES or AUTS);
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER shall contain the AUTS parameter (see 3GPP TS 33.102 [13]).

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

5.1.1.6 Mobile-initiated deregistration

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

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 deregistered;
- c) the To header shall contain the public user identity to be deregistered;
- d) the Expires header, or the expires parameter of the Contact header, shall contain a value of zero, appropriate to the deregistration requirements of the user.

On receiving the 200 OK response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package as described in subclause 5.1.2.1, which contains the registration state value "closed", i.e. deregistered, for one or more public user identities that were previously stored as registered, the UE shall remove all registration details relating to these public user identities.

Editor's Note: The actions to be taken by the UE if all public user identities of one user have been deregistered are for further study, e.g. releasing signalling PDP context, information to the user, etc.

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID, To and From headers).

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

- if a registration state value "open", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;
- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

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. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE, i.e. the UE 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.

5.1.2.2 General SUBSCRIBE requirements

If the UA receives a 503 Service Unavailable response to an initial SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

~~Editor's Note: 5.1.2.3 is reserved for subscription and notification to future events~~

5.1.3 Call initiation - mobile originating case

~~Editor's Note: A more detailed description of the INVITE responses (183, 180, 200...) might be needed here.~~

5.1.3.1 Initial INVITE

3GPP terminals shall indicate the support for reliable provisional responses and specify it using the Supported header mechanism.

~~5.1.3.2 PRACK~~

~~Void.~~

~~5.1.3.3 COMET~~

~~Void.~~

~~5.1.3.4 ReINVITE~~

~~Void.~~

5.1.4 Call initiation - mobile terminating case

~~Editor's Note: A more detailed description of the INVITE responses (183, 180, 200...) might be needed here.~~

5.1.4.1 Initial INVITE

If the UA receives a 503 Service Unavailable response to an initial INVITE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

~~5.1.4.2 PRACK~~

~~Void.~~

~~5.1.4.3 COMET~~

~~Void.~~

~~5.1.4.4 ReINVITE~~

~~Void.~~

5.1.5 Call release

Void.

~~5.1.5.1 MO call release~~

~~Void.~~

~~5.1.5.2 MT call release~~

~~Void.~~

~~5.1.6 Call-related information~~

~~Void.~~

~~5.1.6.1 REFER~~

~~Void.~~

~~5.1.6.2 INFO~~

~~Void.~~

~~5.1.7 Call-independent information~~

~~Void.~~

~~5.1.7.1 OPTIONS~~

~~Void.~~

5.1.68 Emergency service

A UE shall not attempt to establish an emergency session via the IM CN Subsystem when the UE can detect that the number dialled is an emergency number. The UE shall use the CS domain as described in 3GPP TS 24.008 [8].

In the event the UE receives a 380 Alternative Service response to an INVITE request the response containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency", the UE shall automatically:

- send an ACK request to the P-CSCF as per normal SIP procedures;
- attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

The UE may also provide an indication to the user based on the text string contained in the <reason> element.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

CHANGE REQUEST

⌘ **24.229 CR 104** ⌘ 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: | ⌘ Editor's note cleanup - clause 5.2 and deletion of void subclauses | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 16/05/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | Use <u>one</u> of the following categories: | | Use <u>one</u> of the following releases: |
| | F (correction) | 2 (GSM Phase 2) | |
| | A (corresponds to a correction in an earlier release) | R96 (Release 1996) | |
| | B (addition of feature), | R97 (Release 1997) | |
| | C (functional modification of feature) | R98 (Release 1998) | |
| | D (editorial modification) | R99 (Release 1999) | |
| | Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | REL-4 (Release 4) |
| | | | REL-5 (Release 5) |

| | |
|--------------------------------------|---|
| Reason for change: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ <ul style="list-style-type: none"> • Clause 5.2.2, 2nd editor's note is deleted. It is not believed that this has requirements over and above the IETF drafts. • Clause 5.2.2, 3rd editor's note is deleted. It is believed that this editor's note is already met by requirements text. • Clause 5.2.7.1 editor's note has been deleted. The text resolving this editor's note is in the new clause 5.2.6.2 added by CR061R2. Rather than delete clause 5.2.7.1 along with the associated renumbering problems, it has been relabelled "Introduction" and some general text inserted. • Clause 5.2.7.2 editor's note has been deleted. It is believed that this editor's note is now fully covered by appropriate text. • Clause 5.2.7.3 editor's note has been deleted. It is believed that this editor's note is now fully covered by appropriate text. • Clause 5.2.10 and its subclauses are deleted as it is not expected that there is any requirement for these clauses. Clause 5.2.11 is therefore renumbered. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | |
|------------------------------|--|--|
| Clauses affected: | ⌘ 5.2.2, 5.2.7.1, 5.2.7.2, 5.2.7.3, 5.2.10, 5.2.11 | |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications | ⌘ <input type="checkbox"/> Test specifications |

Other comments: ☞ 1st Editor's note in clause 5.2.2 is deleted by CR053R2 so is not addressed by this CR.
Editor's note in clause 5.2.5.2 is deleted by CR064R0 so is not addressed by this CR.
1st editor's note in clause 5.2.6.2 has not been addressed as it is believed that a CR is due dealing with the security association, which will provide a solution for this editor's note and delete it (Nokia?).
2nd editor's note in clause 5.2.6.2 has not been addressed as no solution could be identified.

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.

5.2 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";
- 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 routing 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 routing 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.

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 identities

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.

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 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 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 <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 <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.

5.2.7 Initial INVITE

5.2.7.1 ~~Determination MO or MT case~~ [Introduction](#)

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

~~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 or more ongoing multimedia sessions 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 sessions exist, 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 routing 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 routing 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 routing 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 routing 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.~~

5.2.10⁴ 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.

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 105** ⌘ 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

| | | | |
|------------------------|---|-----------------|---|
| Title: | ⌘ Editor's note cleanup - clause 5.3 | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | <i>Use one of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | <i>Use one of the following releases:</i> 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: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ Editor's note in clause 5.3.2. It is proposed to delete this note as it is believed it is not appropriate to specify procedures for selection of particular S-CSCFs. This is a configuration matter between the operators and the manufacturers. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | | |
|------------------------------|---|---|--|
| Clauses affected: | ⌘ 5.3.2.2 | | |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications | ⌘ | |
| Other comments: | ⌘ The editor's note in clause 5.3.1 is proposed to be deleted by CR037R1, and is therefore not covered in this CR. | | |

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 Procedures at the I-CSCF

5.3.1 Registration procedure

Editor's note: The text on routing 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 than 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.

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 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.

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.

5.3.3.2 Encryption for topology hiding

Upon receiving an outgoing request/response from the hiding network the I-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) 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:asl.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 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 routing 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.

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 106** ⌘ 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

| | | | |
|------------------------|---|-----------------|---|
| Title: | ⌘ Editor's note cleanup - clause 5.4 and deletion of void subclauses | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | <i>Use one of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | <i>Use one of the following releases:</i> 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: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ Editor's note at the start of clause 5.4.2 deleted as the current text in 5.4.2 already reflects the intent of this editor's note. The editor's note in clause 5.4.2.1.1 is deleted as the recent change to the Event package covered in another CR renders this note obsolete. Clause 5.4.2.2 is deleted as it is presumed that there is nothing further to say about proxy behaviour on SUBSCRIBE / NOTIFY beyond the events draft. In clause 5.4.4.1 the empty subclauses are deleted as it is believed that contents in this structure are not currently required. In clause 5.4.4.2 the editor's note is deleted as the content already reflects the editor's note. In clause 5.4.5.1 the superfluous word "Void" is deleted - inserted in error by MCC. Clause 5.4.6.2 is deleted as it is believed it will not be used in future. Clause 5.4.7 is deleted as it is believed it will not be used in future. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | |
|------------------------------|---|
| Clauses affected: | ⌘ 5.4.2, 5.4.2.1.1, 5.4.2.2, 5.4.4.1, 5.4.4.2, 5.4.5.1, 5.4.6.2, 5.4.7 |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications |

O&M Specifications

Other comments: ☼ Editor's note in 5.4 before 5.4.1 has already been deleted by CR037R1.
Handling of editor's notes in 5.4.1.2.1 requires an amendment to CR060 because otherwise the CRs will interact.
Handling of editor's note in 5.4.1.4 is expected to be covered by a CR on the path header changes (Dynamicsoft?).
Handling of editor's note in 5.4.1.5 is expected to be covered by a CR on the Event package changes (Siemens?).

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 Procedures at the S-CSCF

Editor's note: The text on routing 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 than 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-Require 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 from 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 from 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.

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;
- 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 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
- 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;
- 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 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 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 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.

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 a 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 routing 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 routing 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 routing 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 routing 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~~

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 107** ⌘ 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

| | | | |
|------------------------|---|-----------------|--|
| Title: | ⌘ Editor's note cleanup - clause 5.5 and deletion of void subclauses | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | <i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | <i>Use <u>one</u> of the following releases:</i> 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: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ Empty subclauses in 5.5.2 relating to subscription and notification are deleted as it is believed they will not be filled in this form. Empty subclauses 5.5.5.2 and 5.5.5.3 relating to REFER and INFO are deleted as it is believed that they are not needed in this form. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | | |
|------------------------------|--|--|--|
| Clauses affected: | ⌘ 5.5.2, 5.5.5.2, 5.5.5.3 | | |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications | | |
| Other comments: | ⌘ Two editor's notes in 5.5.3.1.2 are deleted by CR020R2. Editor's note in 5.5.4.3 is deleted by CR020R2. Editor's note in 5.5.1.1.1 is deleted by a proposed CR089. Editor's note in 5.5.6 is deleted by a proposed CR088. | | |

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.

5.5 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

[Void.](#)

~~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).

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.

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 110** ⌘ 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

| | | | |
|------------------------|---|-----------------|--|
| Title: | ⌘ Editor's note cleanup - clause 6 | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) REL-4 (Release 4) REL-5 (Release 5) |

| | |
|--------------------------------------|---|
| Reason for change: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ The first editor's note in clause 6.1 is deleted because there is no optimised voice mode in release. The second editor's note in clause 6.1 is deleted because this is an issue of conformance to RFC3261 and offer answer which is dealt with in those drafts. The editor's note in clause 6.4.1 is deleted because it has already been agreed to deleted the equivalent editor's note from 24.228. The editor's note in clause 6.4.2 is deleted because it has already been agreed to deleted the equivalent editor's note from 24.228. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | | |
|------------------------------|---|---|--|
| Clauses affected: | ⌘ 6.1, 6.4.1, 6.4.2 | | |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> 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.

6 Application usage of SDP

6.1 Procedures at the UE

Usage of SDP by the UE:

1. An INVITE request generated by a UE may contain SDP payload. In case preconditions will be used for session setup then SDP payload shall be present. The SDP payload shall reflect the UE#1's terminal capabilities and user preferences for the session.

~~Editor's Note: The requirements for SDP payload in the case of Optimised Voice Mode are FFS.~~

2. The first 183 provisional response sent out shall contain SDP information. The SDP payload shall reflect UE#2's terminal capabilities and user preferences.

~~Editor's Note: The case/action needed when a UE generates a 183 response without SDP payload is FFS.~~

3. When UE sends out an 183 with SDP payload, it shall indicate the support for preconditions and in addition request confirmation for the result of the resource reservation at the originating end point.
4. UE shall include SDP in the PRACK request for acknowledging the 183 Session Progress response if the codec negotiation during the INVITE request and 183 Session Progress response resulted in more than one codec per media line. It is recommended not to include any SDP payload if the SDP payload in the 183 Session Progress response contains only one codec information for each media line.
5. After the initial SDP has been sent the subsequent SDPs sent by the UE shall only contain a subset of the media descriptions of the initial SDP. In order to modify the media descriptors a reINVITE shall be used.
6. If Resource Reservation has been finished before sending the 200 OK for INVITE, then it shall contain the SDP payload that reflects the reserved resources on the radio interface.
7. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description.
8. For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor in the SDP. For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [11].
9. The UE shall include the DTMF media format at the end of the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [17].

6.2 Procedures at the P-CSCF

When the P-CSCF receives an INVITE or reINVITE, the P-CSCF shall examine the media parameters in the received SDP, and remove those which are not allowed on the network by local policy. The P-CSCF will also remove those codecs from the approved media streams which are not allowed by local policy. If the P-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the P-CSCF should ignore the b= lines.

6.3 Procedures at the S-CSCF

When the S-CSCF receives an INVITE or reINVITE, the S-CSCF shall examine the media parameters in the received SDP, and remove those media streams which are not allowed based on the subscription. The S-CSCF will also remove those codecs from the approved media streams which are not allowed by the subscription. If the S-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the S-CSCF should ignore the b= lines.

6.4 Procedures at the MGCF

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1.

6.4.1 Calls originating from circuit-switched networks

When the MGCF generates and sends an INVITE request for a call originating in a circuit-switched network, the MGCF shall:

- populate the SDP with the codecs supported by the associated MGW (see 3GPP TS 26.235 [10] for the supported codecs);
- set the "t" field with the <stop time> set to zero, which indicates an unbounded session;
- set the "a:qos" attribute with the values of "mandatory" and "sendrecv".

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

- check that a supported codec has been indicated in the SDP.

~~Editor's note: the current 3GPP TS 24.228 call flow in 7.2.4.1 shows the use of Final SDP in the PRACK. Should that example be changed to align with the offer/answer model that does not include SDP in the PRACK? Will there be a requirement for the UE to only select one codec? Or, should the MGCF procedures allow for the possibility that the UE sends multiple codecs and that the MGCF selects the codec and includes the result in the SDP in the PRACK?~~

6.4.2 Calls terminating in circuit-switched networks

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

- check for a codec that matches the requested SDP, which may include DTMF support.

When the MGCF generates and sends a 183 Session Progress response to an initial INVITE request, the MGCF shall:

- set SDP indicating the selected codec, which may include DTMF support;
- set the "t" field with the <stop time> set to zero, which indicates an unbounded session;
- set the "a:qos" attribute with the values of "mandatory", "sendrecv" and "confirm".

~~Editor's note: the current 3GPP TS 24.228 call flow in 7.4.4.1 shows the use of Final SDP in the PRACK. Should that example be changed to align with the offer/answer model that does not include SDP in the PRACK?~~

6.5 Procedures at the MRFC

Void.

CR-Form-v5

CHANGE REQUEST

⌘ **24.229 CR 111** ⌘ 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

| | | | |
|------------------------|---|-----------------|--|
| Title: | ⌘ Editor's note cleanup - clause 9 | | |
| Source: | ⌘ Lucent Technologies | | |
| Work item code: | ⌘ IMS-CCR | Date: | ⌘ 30/04/02 |
| Category: | ⌘ F | Release: | ⌘ Rel-5 |
| | Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 . | | Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) REL-4 (Release 4) REL-5 (Release 5) |

| | |
|--------------------------------------|--|
| Reason for change: | ⌘ All editor's notes must be resolved before 24.229 can be frozen. It has been found possible to resolve many editor's notes and therefore they can be deleted. In some cases the editor's note has already been resolved, but the note has not been deleted. In the worst case, an editor's note may be unresolved, but the absence of a solution does not preclude implementation of release 5, or interoperability with other release 5 implementations, and therefore the note can be deleted. Detailed handling is specified below. |
| Summary of change: | ⌘ The editor's note in subclause 9.2.1 is deleted. Specification of an APN for IMS will either happen or not happen, but whichever occurs will have no impact on the contents of 24.229. The editor's note does not therefore represent an issue for 24.229. |
| Consequences if not approved: | ⌘ 24.229 cannot be frozen |

| | | | |
|------------------------------|---|---|--|
| Clauses affected: | ⌘ 9.2.1 | | |
| Other specs affected: | ⌘ <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> 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.

9 GPRS aspects when connected to the IM CN subsystem

9.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by GPRS to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the GGSN in support of this communication are specified in [FFS].

9.2 Procedures at the UE

9.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) perform a GPRS attach procedure;
- b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4]. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with an IPv6 address. This PDP context can be either a primary or a secondary PDP context;

~~Editor's note: Actual APN values for IMS are yet not determined.~~

- c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

- I. Employ DHCP and if needed DNS after PDP context activation.

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or
- request a list of SIP server IPv6 addresses of P-CSCF(s).

- II. Transfer P-CSCF address(es) within The PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE when activating the PDP context.

If the GGSN provides the UE with a list of P-CSCF IPv6 addresses, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options IE as the P-CSCF address with the highest priority. The coding of the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

The UE can freely select method I or II for P-CSCF discovery. In case several P-CSCF addresses are provided to the UE, the selection of P-CSCF address shall be performed according to the resolution of host name as indicated in RFC 2543bis [20]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

If the UE is designed to use I above, but receives in the PDP context activation P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

9.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

9.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

9.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 25.304 [9] and 3GPP TS 44.018 [15] shall apply while the UE is connected to the IM CN subsystem.

9.2.5 PDP contexts for media

During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling.