**3GPP TSG CN Meeting #27** **NP-050073**
**9th - 11th March 2005. Tokyo, Japan.**

**Source:** **TSG CN WG1**

**Title:** **CR to Rel-6 WI “IMS2” for TS 24.229, 24.247, 23.218, 24.147 and 24.141**

**Agenda item:** **9.1**

**Document for:** **APPROVAL**

---

This document contains 18 **CRs on Rel-6 Work Item “IMS2”**, that have been agreed by TSG CN WG1 CN#37 meeting and forwarded to TSG CN Plenary meeting #27 for approval.

| TDoc # | Tdoc Title | Spec | CR # | Rev | CAT | C_Version | WI | Rel |
|---|---|---|---|---|---|---|---|---|
| N1-050061 | Resolution of references to 24.228 | 23.218 | 072 | | F | 6.2.0 | IMS2 | Rel-6 |
| N1-050066 | Incorporation of draft-ietf-sip-rfc3312-update-03.txt | 24.229 | 729 | 1 | F | 6.5.1 | IMS2 | Rel-6 |
| N1-050076 | Registration - Abnormal Case | 24.229 | 790 | | F | 6.5.1 | IMS2 | Rel-6 |
| N1-050080 | RFC 3966 | 24.229 | 794 | | F | 6.5.1 | IMS2 | Rel-6 |
| N1-050107 | MESSAGE to unregistered user | 24.247 | 3 | | F | 6.0.1 | IMS2 | Rel-6 |
| N1-050129 | Editorial corrections | 24.229 | 817 | | D | 6.5.1 | IMS2 | Rel-6 |
| N1-050225 | Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules | 24.229 | 841 | | F | 6.5.1 | IMS2 | Rel-6 |
| N1-050288 | Default handling | 23.218 | 74 | 1 | F | 6.2.0 | IMS2 | Rel-6 |
| N1-050297 | Handling topmost Route header at the P-CSCF | 24.229 | 821 | 1 | F | 6.5.1 | IMS2 | Rel-6 |
| N1-050299 | Removal of I-CSCF normative requirement on Cx interface | 24.229 | 848 | 1 | F | 6.5.1 | IMS2 | Rel-6 |
| N1-050315 | Removing CPCP from 24.247 | 24.247 | 10 | 2 | C | 6.0.1 | IMS2 | Rel-6 |
| N1-050316 | Corrections to Message Session Flows to align with draft-ietf-simple-message-sessions-09 | 24.247 | 11 | 1 | F | 6.0.1 | IMS2 | Rel-6 |
| N1-050318 | Alignment between TS 23.228/ TS 22.340 and TS 24.247 for immediate messaging | 24.247 | 8 | 1 | F | 6.0.1 | IMS2 | Rel-6 |
| N1-050321 | Resolution of references to 24.228 | 24.141 | 034 | 1 | F | 6.2.0 | IMS2 | Rel-6 |
| N1-050322 | Resolution of references to 24.228 | 24.147 | 020 | 1 | F | 6.1.0 | IMS2 | Rel-6 |
| N1-050323 | Resolution of references to 24.228 | 24.247 | 001 | 1 | F | 6.0.1 | IMS2 | Rel-6 |
| N1-050324 | Cleanups resulting from CR changes for last version | 24.229 | 786 | 1 | F | 6.5.1 | IMS2 | Rel-6 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| N1-050326 | Corrections to addition of session set-up not requiring preconditions and reliable transport of provisional responses | 24.229 | 849 | 1 | F | 6.5.1 | IMS2 | Rel-6 |

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050061**
**Sydney, Australia, 14-18 February 2004**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **23.218** | **CR** | **072** | ⌘ **rev** | **-** | ⌘ | Current version: | **6.2.0** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Resolution of references to 24.228 | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 15/12/2004 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | It has been agreed at CN1#36 and at CN#26 that a release 6 version of 24.228 will not be created. 3GPP TS 23.218 makes a number of references to 24.228, which by default are supposed to be to the release 6 version.<br>Depending on the nature of the reference, a number of resolutions are possible, ranging from deleting all the references, making the reference specific to release 5, or reproducing the referenced material in the referencing specification.<br>For 23.218 it is considered that the references are only valid in identifying that other material exists at this release, and as the 24.228 material does not exist, it can be deleted. That is therefore the proposal in this CR. |
| ***Summary of change:*** | ⌘ | All references to 24.228 are deleted. |
| ***Consequences if not approved:*** | ⌘ | Invalid references will exist in the specificiation. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 1, 2, 4.3, 4.4, 4.5, 6.4 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

**How to create CRs using this form:**

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

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

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

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

PROPOSED CHANGE

# 1 Scope

The present document specifies the IP Multimedia (IM) Call Model for handling of an IP multimedia session origination and termination for an IP Multimedia subscriber.

The present document includes interactions between an Application Server and IP multimedia sessions.

The IP Multimedia (IM) Subsystem stage 2 is specified in 3GPP TS 23.228 [3]~~ and the signalling flows for the IP multimedia call control based on SIP and SDP are specified in 3GPP TS 24.228 [4]~~.

PROPOSED CHANGE

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] Void.

[2] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[3] 3GPP TS 23.228: " IP multimedia subsystem; Stage 2".

[4] ~~3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; stage 3"~~void.

[5] 3GPP TS 24.229: "IP multimedia call control protocol based on SIP and SDP; stage 3".

[6] IETF RFC 3261: "SIP: Session Initiation Protocol".

[7] 3GPP TR 29.998-4-4: "Open Service Access (OSA); Application Programming Interface (API) Mapping for Open Service Access (OSA); Part 4: Call Control Service Mapping; Subpart 4: Multiparty Call Control SIP".

[8] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".

[9] 3GPP TS 23.278: "Customised Applications for Mobile network Enhanced Logic (CAMEL); IP Multimedia System (IMS) interworking; Stage 2".

[10] 3GPP TS 23.008: "Organisation of subscriber data".

[11] 3GPP TS 33.203: "Access security for IP based services".

[12] 3GPP TS 29.198: "Open Service Access (OSA); Application programming Interface (API)".

[13] IETF RFC 3265: "Session Initiation Protocol (SIP) Event Notification".

[14] 3GPP TS 29.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3; CAMEL Application Part (CAP) specification".

[15] IETF RFC 3264: "An Offer/Answer Model with Session Description Protocol".

[16] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[17] 3GPP TS 29.229: "Cx Interface based on the Diameter protocol".

[18] 3GPP TS 29.328: "IP Multimedia Subsystem (IMS) Sh Interface; Signalling flows and message contents".

[19] 3GPP TS 29.329: "Sh Interface based on the Diameter protocol".

[20] 3GPP TS 32. 240: "Telecommunication management; Charging management; Charging architecture and principles".

[21] 3GPP TS 32. 260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

PROPOSED CHANGE

# 4 Architecture and information flows for IM multimedia session

Clauses 4.1 and 4.2 show the architecture for handling a basic MO multimedia session and a basic MT multimedia session. A basic mobile-to-mobile multimedia session is treated as the concatenation of a MO multimedia session and a MT multimedia session.

Clauses 4.3, 4.4 and 4.5 show the information flows for handling a basic MO multimedia session and a basic MT multimedia session.

## 4.1 Architecture for a mobile originated IP multimedia session

This is specified in 3GPP TS 23.228 [3].

## 4.2 Architecture for a mobile terminated IP multimedia session

This is specified in 3GPP TS 23.228 [3].

## 4.3 ~~Information flow for a mobile originated IP multimedia session~~void

~~The information flow for a MO multimedia session is specified in 3GPP TS 24.228 [4].~~

## 4.4 ~~Information flow for retrieval of routeing information for mobile terminated IP multimedia session~~void

~~The information flow for retrieval of routeing information for a MT multimedia session is specified in 3GPP TS 24.228 [4].~~

## 4.5 ~~Information flow for a mobile terminated IP multimedia session~~void

~~The information flow for a MT multimedia session is specified in 3GPP TS 24.228 [4].~~

PROPOSED CHANGE

## 6.4 Handling of mobile originating requests

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request.

The initial filter criteria (subset of the profile) has already been downloaded from the HSS and is stored locally at the S-CSCF, ~~as specified in 3GPP TS 24.228 [4],~~ and 3GPP TS 24.229 [5].

When such a session request comes in, the S-CSCF shall first check whether this is an originating request or a terminating request in order to perform the matching procedure with SPTs within initial filter criteria. This clause describes the requirements for the S-CSCF when this request is a mobile originating request. So, if this request is a mobile originating request, the S-CSCF shall:

- check whether this request matches the initial filter criteria with the highest priority for that user by checking the service profile against the public user identity, which was used to place this request;
- if this request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server;
- if this request does not match the highest priority initial filter criteria, check for matching of the following filter criteria priorities until one applies;
- if no more (or none) of the initial filter criteria apply, the S-CSCF shall forward this request downstream based on the route decision;
- in any instance, if the contact of the application server fails, the S-CSCF shall use the "default handling" associated with the initial Filter Criteria to determine if it shall either terminate the call or let the call continue 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 let the call continue as the default behaviour.

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050066**
**Sydney, Australia, 14-18 February 2004**

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **24.229 CR 729** ⌘**rev** **1** ⌘ Current version: **6.5.1** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | |
|---|---|---|---|
| ***Title:*** ⌘ | Incorporation of draft-ietf-sip-rfc3312-update-03.txt | | |
| ***Source:*** ⌘ | Lucent Technologies | | |
| ***Work item code:*** ⌘ | IMS2 | ***Date:*** ⌘ | 04/11/2004 |
| ***Category:*** ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |
| | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use one of the following releases:*<br>*Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

| | |
|---|---|
| ***Reason for change:*** ⌘ | draft-ietf-sip-rfc3312-update-03.txt has just been approved as a proposed standard by IESG as a document that updates RFC 3312. RFC 3312 is referenced from 3GPP TS 24.229, and some of the changes proposed in draft-ietf-sip-rfc3312-update-03.txt have impact (minor in nature) on the manner in which RFC 3312 is used in the context of these references.<br><br>In order to ensure that session establishment does not take place until certain preconditions are met, the RFC-3312 introduces two state variables that describe the state of the media stream: current status and desired status. Session establishment stops until the current status reaches or surpasses the threshold indicated in the desired status. Once this threshold is reached or surpassed, session establishment resumes.<br><br>RFC 3312 assumes that the media streams do not move around. That is, media is sent between the same end-points throughout the duration of the session. However, media stream are not always static. For example, in case of call transfer, an existing media stream from point A to B is moved to new transport address C. Moving an existing media stream to a new termination point, from the preconditions point of view, is like establishing a new media stream. Therefore, it is appropriate to set all the current status values of the media streams to "No" and start a new precondition negotiation.<br><br>While the RFC 3312 allows to update current status information using offers, it does not allow to downgrade current status values in answers, as shown in the third row of Table 3 of RFC-3312. Since such downgrades are sometimes |

| | | |
|---|---|---|
| | | needed, the Table 3 of RFC 3312 needs to be updated to allow answers to downgrade current status values. The document draft-ietf-sip-rfc3312-update-03.txt provides the required updates that will allow moving an existing stream to a new location [i.e. transport address].<br>Additionally, even if 3GPP preclude this occurring in 3GPP IMS, given release 6 interworking with other SIP network we cannot prevent such requests entering the IMS and having to be dealt with |
| ***Summary of change:*** | ⌘ | Add a reference [30A] to draft-ietf-sip-rfc3312-update-03.txt.<br>Replace all references to RFC 3312 [30] by text stating RFC 3312 [30] as revised by draft-ietf-sip-rfc3312-update [30A].<br>The references used for the UPDATE method are incorrectly using [30] at the moment, when they should be to [29] so these are changed. |
| ***Consequences if not approved:*** | ⌘ | Use of obsolete and incomplete reference RFC. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 5.1.3.1.2.1, 5.1.4.1.2.2, 5.1.4.1.2.3, 5.5.3.1.1, 6.1, A.2.1.2, A.2.1.3, A.2.2.2, A.2.2.3, A.3.2.1, A.3.3.1 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] draft-ietf-iptel-rfc2806bis-09 (June 2004): "The tel URI for Telephone Numbers".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-15 (November 2004): "Session Timers in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[64] draft-ietf-sip-rfc3312-update-03 (September 2004): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-simple-xcap-package-01 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

# PROPOSED CHANGE

### 5.1.3.1.2 "Integration of resource management" required by originating UE

#### 5.1.3.1.2.1 Preconditions required by originating UE

Upon generating an initial INVITE request using preconditions, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement of precondition and specify it using the Require header mechanism.

When the initial INVITE has been created and forwarded the forthcoming procedures are identical to the procedures described in subclause 5.1.3.1.1.

If the UE receives a 420 (Bad Extension) response to an initial INVITE request with "precondition" option-tag in the Unsupported header field, the UE shall either:

a) abort the session attempt and shall not resend this INVITE request without "precondition" option-tag in the Require header, or

b) try to complete the session by relaxing the requirement on the usage of the "integration of resource management in SIP" extension as described in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64] and proceed with the procedures described in subclause 5.1.3.2 and subclause 6.1.

PROPOSED CHANGE

### 5.1.4.1.2.2 Preconditions not used by originating UE but preconditions required by terminating UE

Upon receiving an initial INVITE request without the "precondition" option-tag in the Require header, and the preconditions extension as described in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64] is required by the terminating UE, the terminating UE shall generate a 421 (Extension Required) response indicating the required extension in the Require header field value.

PROPOSED CHANGE

### 5.1.4.1.2.3 Preconditions not used by originating UE and preconditions not required by terminating UE

Upon receiving an initial INVITE request without containing  the "precondition" option-tag in the Require header, if the terminating UE is configured to not use the preconditions extension as described in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64], the UE shall:

1) send none or more provisional response(s) (eg. 183 Session Progress); and

2) send a 200 (OK) response, when the resources have been reserved and the call has been accepted by the terminating user.

PROPOSED CHANGE

## 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 to I-CSCF:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64]);
  - include an P-Asserted-Identity header;
  - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
  - insert an orig-ioi parameter into the P-Charging-Vector header. The orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the term-ioi parameter shall not be included.

PROPOSED CHANGE

## 6.1 Procedures at the UE

Usage of SDP by the UE:

1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP payload with the most preferred codec listed first.

3. If the SIP request includes a "precondition" option-tag in the Require header, the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

   If the SIP request does not include the "precondition" option-tag in the Require header, the UE shall not indicate that it mandates local QoS. The UE may indicate its desire for optional local QoS, by including the following preconditions:

   a=des:qos optional local sendrecv

   In the case described in subclause 5.1.3.1.2.2 in the first SDP offer the UE sends, the UE shall set each media stream in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

NOTE 1: When setting the media streams in the inactive mode, the UE may include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

4. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, and the precondition mechanism is used as described in subclause 5.1.4.1.2.1, the first 183 (Session Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.

   In the case described in subclause 5.1.4.1.3 no specific SDP procedures for integration of resource reservation have to be performed.

   In the case described in subclause 5.1.4.1.2.3 in the first SDP answer the UE sends, the UE shall set each media streams in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

   If the UE is setting one or more media streams in active mode, it shall apply the procedures described in draft-ietf-mmusic-sdp-new [39] with respect to setting the direction of media streams.

5. When the UE sends a 183 (Session Progress) response with SDP payload including one or more "m=" media descriptions, if the preconditions extension as described in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64] is supported by the calling UE, the called UE shall request confirmation for the result of the resource reservation at the originating end point.

6. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261[26].

7. 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 and the "AS" bandwidth modifier in the SDP.

If the media line in the SDP indicates the usage of RTP/RTCP, in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP.

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 [13].

NOTE 2: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer will typically get the value of zero.

8. The UE shall include the MIME subtype "telephone-event" in 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 [23].

9. The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

10. If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].

11. If the UE builds SDP for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE may be attempting a session establishment through multiple networks with different policies and potentially may need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

PROPOSED CHANGE

### A.2.1.2 Major capabilities

**Table A.4: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| 1 | client behaviour for registration? | [26] subclause 10.2 | o | c3 |
| 2 | registrar? | [26] subclause 10.3 | o | c4 |
| 2A | registration of multiple contacts for a single address of record | [26] 10.2.1.2, 16.6 | o | o |
| 2B | initiating a session? | [26] subclause 13 | o | o |
| 3 | client behaviour for INVITE requests? | [26] subclause 13.2 | c18 | c18 |
| 4 | server behaviour for INVITE requests? | [26] subclause 13.3 | c18 | c18 |
| 5 | session release? | [26] subclause 15.1 | c18 | c18 |
| 6 | timestamping of requests? | [26] subclause 8.2.6.1 | o | o |
| 7 | authentication between UA and UA? | [26] subclause 22.2 | c34 | c34 |
| 8 | authentication between UA and registrar? | [26] subclause 22.2 | o | n/a |
| 8A | authentication between UA and proxy? | [26] 20.28, 22.3 | o | o |
| 9 | server handling of merged requests due to forking? | [26] 8.2.2.2 | m | m |
| 10 | client handling of multiple responses due to forking? | [26] 13.2.2.4 | m | m |
| 11 | insertion of date in requests and responses? | [26] subclause 20.17 | o | o |
| 12 | downloading of alerting information? | [26] subclause 20.4 | o | o |
| | **Extensions** | | | |
| 13 | the SIP INFO method? | [25] | o | n/a |
| 14 | reliability of provisional responses in SIP? | [27] | c19 | c18 |
| 15 | the REFER method? | [36] | o | c33 |
| 16 | integration of resource management and SIP? | [30] [64] | c19 | c18 |
| 17 | the SIP UPDATE method? | [29] | c5 | c18 |
| 19 | SIP extensions for media authorization? | [31] | o | c14 |
| 20 | SIP specific event notification? | [28] | o | c13 |
| 21 | the use of NOTIFY to establish a dialog? | [28] 4.2 | o | n/a |
| 22 | acting as the notifier of event information? | [28] | c2 | c15 |
| 23 | acting as the subscriber to event information? | [28] | c2 | c16 |
| 24 | session initiation protocol extension header field for registering non-adjacent contacts? | [35] | o | c6 |
| 25 | private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks? | [34] | o | m |
| 26 | a privacy mechanism for the Session Initiation Protocol (SIP)? | [33] | o | m |
| 26A | request of privacy by the inclusion of a Privacy header indicating any privacy option? | [33] | c9 | c11 |
| 26B | application of privacy based on the received Privacy header? | [33] | c9 | n/a |
| 26C | passing on of the Privacy header transparently? | [33] | c9 | c12 |
| 26D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the | [33] 5.1 | c10 | c27 |

| | | | | |
|---|---|---|---|---|
| | assistance of intermediaries are obscured? | | | |
| 26E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs? | [33] 5.2 | c10 | c27 |
| 26F | application of the privacy option "user" such that user level privacy functions are provided by the network? | [33] 5.3 | c10 | c27 |
| 26G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network? | [34] 7 | c10 | n/a |
| 27 | a messaging mechanism for the Session Initiation Protocol (SIP)? | [50] | o | c7 |
| 28 | session initiation protocol extension header field for service route discovery during registration? | [38] | o | c17 |
| 29 | compressing the session initiation protocol? | [55] | o | c8 |
| 30 | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)? | [52] | o | m |
| 31 | the P-Associated-URI header extension? | [52] 4.1 | c21 | c22 |
| 32 | the P-Called-Party-ID header extension? | [52] 4.2 | c21 | c23 |
| 33 | the P-Visited-Network-ID header extension? | [52] 4.3 | c21 | c24 |
| 34 | the P-Access-Network-Info header extension? | [52] 4.4 | c21 | c25 |
| 35 | the P-Charging-Function-Addresses header extension? | [52] 4.5 | c21 | c26 |
| 36 | the P-Charging-Vector header extension? | [52] 4.6 | c21 | c26 |
| 37 | security mechanism agreement for the session initiation protocol? | [48] | o | c20 |
| 38 | the Reason header field for the session initiation protocol? | [34A] | o | o (note 1) |
| 39 | an extension to the session initiation protocol for symmetric response routeing? | [56A] | o | x |
| 40 | caller preferences for the session initiation protocol? | [56B] | C29 | c29 |
| 40A | the proxy-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 40B | the cancel-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 40C | the fork-directive within caller-preferences? | [56B] 9.1 | o.5 | c28 |
| 40D | the recurse-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 40E | the parallel-directive within caller-preferences? | [56B] 9.1 | o.5 | c28 |
| 40F | the queue-directive within caller-preferences? | [56B] 9.1 | o.5 | o.5 |
| 41 | an event state publication extension to the session initiation protocol? | [70] | o | c30 |
| 42 | SIP session timer? | [58] | c19 | c19 |
| 43 | the SIP Referred-By mechanism? | [59] | o | c33 |
| 44 | the Session Inititation Protocol (SIP) "Replaces" header? | [60] | c19 | c19 (note 1) |
| 45 | the Session Inititation Protocol (SIP) "Join" header? | [61] | c19 | c19 (note 1) |
| 46 | the callee capabilities? | [62] | o | c35 |

c2: IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.

c3: IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UE or S-CSCF functional entity.

c4: IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.

c5: IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.

c6: IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.

c7: IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing $3^{rd}$ party call control.

c8: IF A.3/1 THEN m ELSE n/a - - UE behaviour.

c9: IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).

c10: IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.

c11: IF A.3/1 OR A.3/6 THEN o ELSE n/a - - UE or MGCF.

c12: IF A.3/7D THEN m ELSE n/a - - AS performing 3rd-party call control.

c13: IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE behaviour or S-CSCF.

c14: IF A.3/1 THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE or P-CSCF.

c15: IF A.4/20 and A.3/4 THEN m ELSE o – SIP specific event notification extensions and S-CSCF.

c16: IF A.4/20 and (A.3/1 OR A.3/2) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF.

c17: IF A.3/1 or A.3/4 THEN m ELSE n/a - - UE or S-CSCF.

c18: IF A.4/2B THEN m ELSE n/a - - initiating sessions.

c19: IF A.4/2B THEN o ELSE n/a - - initiating sessions.

c20: IF A.3/1 THEN m ELSE n/a - - UE behaviour.

c21: IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).

c22: IF A.4/30 AND (A.3/1 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UA.

c23: IF A.4/30 AND A.3/1 THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE.

c24: IF A.4/30 AND A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF.

c25: IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CSCF or AS acting as terminating UA or AS acting as third-party call controller.

c26: IF A.4/30 AND (A.3/6 OR A.3/7A OR A.3/7B or A.3/7D) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller.

c27: IF A.3/7D THEN o ELSE x - - AS performing 3rd party call control.

c28: IF A.3/1 THEN m ELSE o.5 - - UE.

c29: IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.

c30: IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS.

c33: IF A.3/11 OR A.3/12 OR A.4/44 THEN m ELSE o - - conference focus or conference participant or the Session Inititation Protocol (SIP) "Replaces" header.

c34: IF A.4/44 OR A.4/45 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header or the Session Inititation Protocol (SIP) "Join" header.

c35: IF A.3/4 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8) THEN o ELSE n/a - - UE, MGCF, AS MRFC or S-CSCF functional entity.

o.1: At least one of these capabilities is supported.

o.2: At least one of these capabilities is supported.

o.3: At least one of these capabilities is supported.

o.4: At least one of these capabilities is supported.

o.5: At least one of these capabilities is supported.

NOTE 1: At the MGCF, the interworking specifications do not support a handling of the header associated with this extension.

Prerequisite A.5/20 - - SIP specific event notification

### Table A.4A: Supported event packages

| Item | Does the implementation support | Subscriber | | | Notifier | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | reg event package? | [43] | c1 | c3 | [43] | c2 | c4 |
| 2 | refer package? | [36] 3 | c13 | c13 | [36] 3 | c13 | c13 |
| 3 | presence package? | [74] 6 | c1 | c5 | [74] 6 | c2 | c6 |
| 4 | eventlist with underlying presence package? | [75], [74] 6 | c1 | c7 | [75], [74] 6 | c2 | c8 |
| 5 | presence.winfo template-package? | [72] 4 | c1 | c9 | [72] 4 | c2 | c10 |
| 6 | xcap-change package? | [77] 2 | c1 | c11 | [77] 2 | c2 | c12 |
| 7 | conference package? | [78] 3 | c1 | c21 | [78] 3 | c1 | c22 |

c1: IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.

c2: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.

c3: IF A.3/1 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, P-CSCF, AS.

c4: IF A.3/4 THEN m ELSE n/a - - S-CSCF.

c5: IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.

c6: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - watcher, acting as the notifier of event information.

c7: IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.

c8: IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.

c9: IF A.3A/1 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.

c10: IF A.3A/2 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.

c11: IF A.3A/2 OR A.3A/4 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - watcher or presence user agent, acting as the subscriber to event information.

c12: IF A.3A/1 OR A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server, acting as the notifier of event information.

c13: IF A.4/15 THEN m ELSE n/a - - the REFER method.

c21: IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.

c22: IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.

# PROPOSED CHANGE

## A.2.1.3 PDUs

**Table A.5: Supported methods**

| Item | PDU | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | **Ref.** | **RFC status** | **Profile status** | **Ref.** | **RFC status** | **Profile status** |
| 1 | ACK request | [26] 13 | c10 | c10 | [26] 13 | c11 | c11 |
| 2 | BYE request | [26] 15.1 | c12 | c12 | [26] 15.1 | c12 | c12 |
| 3 | BYE response | [26] 15.1 | c12 | c12 | [26] 15.1 | c12 | c12 |
| 4 | CANCEL request | [26] 9 | m | m | [26] 9 | m | m |
| 5 | CANCEL response | [26] 9 | m | m | [26] 9 | m | m |
| 8 | INVITE request | [26] 13 | c10 | c10 | [26] 13 | c11 | c11 |
| 9 | INVITE response | [26] 13 | c11 | c11 | [26] 13 | c10 | c10 |
| 9A | MESSAGE request | [50] 4 | c7 | c7 | [50] 7 | c7 | c7 |
| 9B | MESSAGE response | [50] 4 | c7 | c7 | [50] 7 | c7 | c7 |
| 10 | NOTIFY request | [28] 8.1.2 | c4 | c4 | [28] 8.1.2 | c3 | c3 |
| 11 | NOTIFY response | [28] 8.1.2 | c3 | c3 | [28] 8.1.2 | c4 | c4 |
| 12 | OPTIONS request | [26] 11 | m | m | [26] 11 | m | m |
| 13 | OPTIONS response | [26] 11 | m | m | [26] 11 | m | m |
| 14 | PRACK request | [27] 6 | c5 | c5 | [27] 6 | c5 | c5 |
| 15 | PRACK response | [27] 6 | c5 | c5 | [27] 6 | c5 | c5 |
| 15A | PUBLISH request | [70] 11.1.3 | c20 | c20 | [70] 11.1.3 | c20 | c20 |
| 15B | PUBLISH response | [70] 11.1.3 | c20 | c20 | [70] 11.1.3 | c20 | c20 |
| 16 | REFER request | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 17 | REFER response | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 18 | REGISTER request | [26] 10 | c8 | c8 | [26] 10 | c9 | c9 |
| 19 | REGISTER response | [26] 10 | c9 | c9 | [26] 10 | c8 | c8 |
| 20 | SUBSCRIBE request | [28] 8.1.1 | c3 | c3 | [28] 8.1.1 | c4 | c4 |
| 21 | SUBSCRIBE response | [28] 8.1.1 | c4 | c4 | [28] 8.1.1 | c3 | c3 |
| 22 | UPDATE request | [~~30~~29] 6.1 | c6 | c6 | [~~30~~29] 6.2 | c6 | c6 |
| 23 | UPDATE response | [~~30~~29] 6.2 | c6 | c6 | [~~30~~29] 6.1 | c6 | c6 |

c1: IF A.4/15 THEN m ELSE n/a - - the REFER method extension.
c3: IF A.4/23 THEN m ELSE n/a - - recipient for event information.
c4: IF A.4/22 THEN m ELSE n/a - - notifier of event information.
c5: IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses extension.
c6: IF A.4/17 THEN m ELSE n/a - - the SIP update method extension.
c7: IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.
c8: IF A.4/1 THEN m ELSE n/a - - client behaviour for registration.
c9: IF A.4/2 THEN m ELSE n/a - - registrar.
c10: IF A.4/3 THEN m ELSE n/a - - client behaviour for INVITE requests.
c11: IF A.4/4 THEN m ELSE n/a - - server behaviour for INVITE requests.
c12: IF A.4/5 THEN m ELSE n/a - - session release.
c20: IF A.4/41 THEN m ELSE n/a.

# PROPOSED CHANGE

## A.2.2.2 Major capabilities

**Table A.162: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| 3 | initiate session release? | [26] 16 | x | c27 |
| 4 | stateless proxy behaviour? | [26] 16.11 | o.1 | c28 |
| 5 | stateful proxy behaviour? | [26] 16.2 | o.1 | c29 |
| 6 | forking of initial requests? | [26] 16.1 | c1 | c31 |
| 7 | support of indication of TLS connections in the Record-Route header on the upstream side? | [26] 16.7 | o | n/a |
| 8 | support of indication TLS connections in the Record-Route header on the downstream side? | [26] 16.7 | o | n/a |
| 8A | authentication between UA and proxy? | [26] 20.28, 22.3 | o | x |
| 9 | insertion of date in requests and responses? | [26] 20.17 | o | o |
| 10 | suppression or modification of alerting information data? | [26] 20.4 | o | o |
| 11 | reading the contents of the Require header before proxying the request or response? | [26] 20.32 | o | o |
| 12 | adding or modifying the contents of the Require header before proxying the REGISTER request or response | [26] 20.32 | o | m |
| 13 | adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER? | [26] 20.32 | o | o |
| 14 | being able to insert itself in the subsequent transactions in a dialog (record-routing)? | [26] 16.6 | o | c2 |
| 15 | the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing? | [26] 16.7 | c3 | c3 |
| 16 | reading the contents of the Supported header before proxying the response? | [26] 20.37 | o | o |
| 17 | reading the contents of the Unsupported header before proxying the 420 response to a REGISTER? | [26] 20.40 | o | m |
| 18 | reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER? | [26] 20.40 | o | o |
| 19 | the inclusion of the Error-Info header in 3xx - 6xx responses? | [26] 20.18 | o | o |
| 19A | reading the contents of the Organization header before proxying the request or response? | [26] 20.25 | o | o |
| 19B | adding or concatenating the Organization header before proxying the request or response? | [26] 20.25 | o | o |
| 19C | reading the contents of the Call-Info header before proxying the request or response? | [26] 20.25 | o | o |
| 19D | adding or concatenating the Call-Info header before proxying the request or response? | [26] 20.25 | o | o |

| | | | | |
|---|---|---|---|---|
| 19E | delete Contact headers from 3xx responses prior to relaying the response? | [26] 20 | o | o |
| | **Extensions** | | | |
| 20 | the SIP INFO method? | [25] | o | o |
| 21 | reliability of provisional responses in SIP? | [27] | o | i |
| 22 | the REFER method? | [36] | o | o |
| 23 | integration of resource management and SIP? | [30] [64] | o | i |
| 24 | the SIP UPDATE method? | [29] | c4 | i |
| 26 | SIP extensions for media authorization? | [31] | o | c7 |
| 27 | SIP specific event notification | [28] | o | i |
| 28 | the use of NOTIFY to establish a dialog | [28] 4.2 | o | n/a |
| 29 | Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts | [35] | o | c6 |
| 30 | extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks | [34] | o | m |
| 30A | act as first entity within the trust domain for asserted identity | [34] | c5 | c8 |
| 30B | act as subsequent entity within trust network that can route outside the trust network | [34] | c5 | c9 |
| 31 | a privacy mechanism for the Session Initiation Protocol (SIP) | [33] | o | m |
| 31A | request of privacy by the inclusion of a Privacy header | [33] | n/a | n/a |
| 31B | application of privacy based on the received Privacy header | [33] | c10 | c12 |
| 31C | passing on of the Privacy header transparently | [33] | c10 | c13 |
| 31D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | [33] 5.1 | x | x |
| 31E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs? | [33] 5.2 | n/a | n/a |
| 31F | application of the privacy option "user" such that user level privacy functions are provided by the network? | [33] 5.3 | n/a | n/a |
| 31G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network? | [34] 7 | c11 | c12 |
| 32 | Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration | [38] | o | c30 |
| 33 | a messaging mechanism for the Session Initiation Protocol (SIP) | [50] | o | m |
| 34 | Compressing the Session Initiation Protocol | [55] | o | c7 |
| 35 | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)? | [52] | o | m |
| 36 | the P-Associated-URI header extension? | [52] 4.1 | c14 | c15 |
| 37 | the P-Called-Party-ID header extension? | [52] 4.2 | c14 | c16 |
| 38 | the P-Visited-Network-ID header extension? | [52] 4.3 | c14 | c17 |

| | | | | |
|---|---|---|---|---|
| 39 | reading, or deleting the P-Visited-Network-ID header before proxying the request or response? | [52] 4.3 | c18 | n/a |
| 41 | the P-Access-Network-Info header extension? | [52] 4.4 | c14 | c19 |
| 42 | act as first entity within the trust domain for access network information? | [52] 4.4 | c20 | c21 |
| 43 | act as subsequent entity within trust network for access network information that can route outside the trust network? | [52] 4.4 | c20 | c22 |
| 44 | the P-Charging-Function-Addresses header extension? | [52] 4.5 | c14 | m |
| 44A | adding, deleting or  reading the P-Charging-Function-Addresses header before proxying the request or response? | [52] 4.6 | c25 | c26 |
| 45 | the P-Charging-Vector header extension? | [52] 4.6 | c14 | m |
| 46 | adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response? | [52] 4.6 | c23 | c24 |
| 47 | security mechanism agreement for the session initiation protocol? | [48] | o | c7 |
| 48 | the Reason header field for the session initiation protocol | [34A] | o | o |
| 49 | an extension to the session initiation protocol for symmetric response routeing | [56A] | o | x |
| 50 | caller preferences for the session initiation protocol? | [56B] | c33 | c33 |
| 50A | the proxy-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50B | the cancel-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50C | the fork-directive within caller-preferences? | [56B] 9.1 | o.4 | c32 |
| 50D | the recurse-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 50E | the parallel-directive within caller-preferences? | [56B] 9.1 | o.4 | c32 |
| 50F | the queue-directive within caller-preferences? | [56B] 9.1 | o.4 | o.4 |
| 51 | an event state publication extension to the session initiation protocol? | [70] | o | m |
| 52 | SIP session timer? | [58] | o | o |
| 53 | the SIP Referred-By mechanism? | [59] | o | o |
| 54 | the Session Inititation Protocol (SIP) "Replaces" header? | [60] | o | o |
| 55 | the Session Inititation Protocol (SIP) "Join" header? | [61] | o | o |
| 56 | the callee capabillities? | [62] | o | o |

c1: IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.

c2: IF A.3/2 OR A.3/3A OR A.3/4 THEN m ELSE o - - P-CSCF, I-CSCF(THIG) or S-CSCF.

c3: IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion.

c4: IF A.162/23 THEN m ELSE o - - integration of resource management and SIP.

c5: IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.

c6: IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG).

c7: IF A.3/2 THEN m ELSE n/a - - P-CSCF.

c8: IF A.3/2 AND A.162/30 THEN m ELSE n/a - - P-CSCF and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.

c9: IF A.3/2 AND A.162/30 THEN m ELSE IF A.3/7C AND A.162/30 THEN o ELSE n/a - - S-CSCF or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (NOTE).

c10: IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).

c11: IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header.

c12: IF A.162/31 AND A.3/4 THEN m ELSE n/a - - S-CSCF.

c13: IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C) THEN m ELSE n/a - - P-CSCF OR I-CSCF OR AS acting as a SIP proxy.

c14: IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).

c15: IF A.162/35 AND (A.3/2 OR A.3/3) THEN m THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF.

c16: IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or S-CSCF.

c17: IF A.162/35 AND (A.3/2 OR A.3/3) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF.

c18: IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension.

c19: IF A.162/35 AND (A.3/2 OR A.3.3 OR A.3/4 OR A.3/7 THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy.

c20: IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension.

c21: IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF.

c22: IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF.

c23: IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension.

c24: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.

c25: IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.

c26: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function Addresses header extension.

c27: IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF.

c28: IF A.3/2 OR A.3/4 OR A.3/6 then m ELSE o - - P-CSCF or S-CSCF of MGCF.

c29: IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m - - P-CSCF or S-CSCF of MGCF.

c30: IF A.3/2 o ELSE i - - P-CSCF.

c31: IF A.3/4 THEN m ELSE x - - S-CSCF.

c32: IF A.3/4 THEN m ELSE o.4 - - S-CSCF.

c33: IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.

o.1: It is mandatory to support at least one of these items.

o.2: It is mandatory to support at least one of these items.

o.3: It is mandatory to support at least one of these items.

o.4 At least one of these capabilities is supported.

NOTE: An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.

# PROPOSED CHANGE

## A.2.2.3 PDUs

**Table A.163: Supported methods**

| Item | PDU | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | ACK request | [26] 13 | m | m | [26] 13 | m | m |
| 2 | BYE request | [26] 16 | m | m | [26] 16 | m | m |
| 3 | BYE response | [26] 16 | m | m | [26] 16 | m | m |
| 4 | CANCEL request | [26] 16.10 | m | m | [26] 16.10 | m | m |
| 5 | CANCEL response | [26] 16.10 | m | m | [26] 16.10 | m | m |
| 8 | INVITE request | [26] 16 | m | m | [26] 16 | m | m |
| 9 | INVITE response | [26] 16 | m | m | [26] 16 | m | m |
| 9A | MESSAGE request | [50] 4 | c5 | c5 | [50] 7 | c5 | c5 |
| 9B | MESSAGE response | [50] 4 | c5 | c5 | [50] 7 | c5 | c5 |
| 10 | NOTIFY request | [28] 8.1.2 | c3 | c3 | [28] 8.1.2 | c3 | c3 |
| 11 | NOTIFY response | [28] 8.1.2 | c3 | c3 | [28] 8.1.2 | c3 | c3 |
| 12 | OPTIONS request | [26] 16 | m | m | [26] 16 | m | m |
| 13 | OPTIONS response | [26] 16 | m | m | [26] 16 | m | m |
| 14 | PRACK request | [27] 6 | c6 | c6 | [27] 6 | c6 | c6 |
| 15 | PRACK response | [27] 6 | c6 | c6 | [27] 6 | c6 | c6 |
| 15A | PUBLISH request | [70] 11.1.1 | c20 | c20 | [70] 11.1.1 | c20 | c20 |
| 15B | PUBLISH response | [70] 11.1.1 | c20 | c20 | [70] 11.1.1 | c20 | c20 |
| 16 | REFER request | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 17 | REFER response | [36] 3 | c1 | c1 | [36] 3 | c1 | c1 |
| 18 | REGISTER request | [26] 16 | m | m | [26] 16 | m | m |
| 19 | REGISTER response | [26] 16 | m | m | [26] 16 | m | m |
| 20 | SUBSCRIBE request | [28] 8.1.1 | c3 | c3 | [28] 8.1.1 | c3 | c3 |
| 21 | SUBSCRIBE response | [28] 8.1.1 | c3 | c3 | [28] 8.1.1 | c3 | c3 |
| 22 | UPDATE request | [~~30~~29] 7 | c4 | c4 | [~~30~~29] 7 | c4 | c4 |
| 23 | UPDATE response | [~~30~~29] 7 | c4 | c4 | [~~30~~29] 7 | c4 | c4 |

c1: IF A.162/22 THEN m ELSE n/a - - the REFER method.
c3 IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.
c4 IF A.162/24 THEN m ELSE n/a - - the SIP UPDATE method.
c5: IF A.162/33 THEN m ELSE n/a - - the SIP MESSAGE method.
c6: ÌF A.162/21 THEN m ELSE n/a - - reliability of provisional responses.
c20: IF A.4/51 THEN m ELSE n/a

PROPOSED CHANGE

## A.3.2.1 Major capabilities

**Table A.317: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| | | | | |
| | **Extensions** | | | |
| 22 | Integration of resource management and SIP? | [30] [64] | o | m |
| 23 | Grouping of media lines | [53] | o | c1 |
| 24 | Mapping of Media Streams to Resource Reservation Flows | [54] | o | c1 |
| 25 | SDP Bandwidth Modifiers for RTCP Bandwidth | [56] | o | o (NOTE 1) |
| c1: IF A.3/1 THEN m ELSE n/a - - UE role.<br>NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified. | | | | |

PROPOSED CHANGE

## A.3.3.1 Major capabilities

**Table A.328: Major capabilities**

| Item | Does the implementation support | Reference | RFC status | Profile status |
|---|---|---|---|---|
| | **Capabilities within main protocol** | | | |
| | | | | |
| | **Extensions** | | | |
| 1 | Integration of resource management and SIP? | [30] [64] | o | n/a |
| 2 | Grouping of media lines | [53] | o | c1 |
| 3 | Mapping of Media Streams to Resource Reservation Flows | [54] | o | c1 |
| 4 | SDP Bandwidth Modifiers for RTCP Bandwidth | [56] | o | c1 |
| c1: IF A.3/2 THEN m ELSE n/a - - P-CSCF role. | | | | |

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050076**
**Sydney, Australia, 14-18 February 2004**

CR-Form-v7.1

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **790** | ⌘**rev** | **-** | ⌘ | Current version: | **6.5.1** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Registration - Abnormal Case | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 01/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | ***Rel-6*** |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use one of the following releases:*<br>*Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

***Reason for change:*** ⌘

When the REGISTER request that has the "integrity-protected" parameter in the Authorization header set to "yes" arrives at the S-CSCF, the current procedure in subclause 5.4.1.2.3 specifies the case to be "Abnormal" only if *"… the authentication challenge response from the UE does not match with the expected authentication challenge response"*.

However, the treatment of the "integrity-protected" REGISTER request [subclause 5.4.1.2.2] states in, that:

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

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

If the Call-ID does not match, the procedure is not defined in 24.229, i.e. it is not handled either by subclause 5.4.1.2.3 or subclause 5.4.1.2.2.

***Summary of change:*** ⌘ Text added to handle the case stated above.

***Consequences if not approved:*** ⌘ Incomplete Specification

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.4.1.2.3 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs*** | ⌘ | | **X** | Other core specifications | ⌘ | |

| | | | | |
|---|---|---|---|---|
| ***affected:*** | | X | Test specifications | |
| | | X | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | |

## How to create CRs using this form:

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

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

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

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

### 5.4.1.2.3 Abnormal cases

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050080**
**Sydney, Australia, 14-18 February 2004**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **794** | ⌘**rev** | **-** | ⌘ | Current version: | **6.5.1** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | RFC 3966 | | |
| ***Source:*** | ⌘ | Siemens | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 12/01/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | draft-ietf-iptel-rfc2806bis-09 was published as rfc 3966. Resulting changes are provided with this CR. |
| ***Summary of change:*** | ⌘ | Reference to rfc 3966 is updated<br>"TEL URL" is substituted with "tel URI" |
| ***Consequences if not approved:*** | ⌘ | Incorrect handling of requests containing the tel URI format |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, 4.2, 5.4.3.2, 5.4.3.3 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

****** 1st change ******

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[13A] 3GPP TS 29.209: "Policy control over Gq interface".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[19A] 3GPP TS 33.210: "IP Network Layer Security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers"

~~draft-ietf-iptel-rfc2806bis-09 (June 2004): "The tel URI for Telephone Numbers".~~

~~Editor's note: The above document cannot be formally referenced until it is published as an RFC.~~

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".

[26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".

[28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".

[33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".

[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-15 (November 2004): "Session Timers in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[60] RFC 3891 (September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

[61] RFC 3911 (October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

[62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".

[70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".

[71] Void.

[72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-simple-xcap-package-01 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[79] draft-ietf-rohc-sigcomp-sip-01 (February 2004): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

****** next change ******

## 4.2 URI and address assignments

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

1) I-CSCFs used in registration are allocated SIP URIs. Other IM CN subsystem entities may be allocated SIP URIs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URI may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URIs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IPv6 addresses in accordance with the constraints specified in 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 ISIM application, if present. Where no ISIM application is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A). This private user identity is available to the SIP application within the UE.

NOTE: The SIP URIs 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. The public user identity shall take the form of SIP URI as specified in RFC 3261 [26] or ~~TEL URL~~tel URI as specified in RFC 3966 ~~draft-ietf-iptel-rfc2806bis-09~~ [22]. At least one of these is SIP URI and it is contained within the ISIM application, if ISIM application is present. Where no ISIM application is present but USIM is present, the UE derives a temporary public user identity (see subclause 5.1.1.1A). All registered public user identities are available to the SIP application within the UE, after registration.

5) The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities and different contact addresses. When reregistering and deregistering a given public user identity and associated contact address, the UE will use the same private user identity that it has used during the initial registration of the respective public user identity and associated contact address.

6) For the purpose of access to the IM CN subsystem, UEs are assigned IPv6 prefixes in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures).

****** next change ******

### 5.4.3.2 Requests initiated by the served user

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

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

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

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

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

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

4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:

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

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

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;

7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the request is not forwarded to an AS and if the outgoing Request-URI is a ~~TEL URL~~tel URI, the S-CSCF shall translate the E.164 address (see RFC 3966~~draft-ietf-iptel-rfc2806bis~~ [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem , then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

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

12) in case of an initial request for a dialog originated from a served user, either:

   - if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

   - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;

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

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

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

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header; and

2) apply the same privacy mechanism to the P-Access-Network-Info header, if present.

NOTE 4: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 5: The optional procedures above are in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

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

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

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

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

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

4) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header;

5) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and

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

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

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

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

2) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

3) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and

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

****** next change ******

### 5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a statically pre-configured PSI or a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

7) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

8) check whether the Request-URI equals to the saved value of the Request-URI. If there is no match, then:

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

   b) forward the request based on the Request-URI and skip the following steps;

   If there is a match, then continue with the further steps;

9) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B];

10) 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. Furthermore, the S-CSCF shall:

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

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

      - if the fork directive in the Request Disposition header was set to "no-fork", the contact with the highest qvalue parameter shall be used when building the Request-URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally what contact address to be used when building the Request-URI; otherwise

      - fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF determine the contact address to be used when building the Request-URI as directed by the Request Disposition header as described in RFC 3841 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

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

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

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

12) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header and apply the same privacy mechanism to the P-Access-Network-Info header;

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

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

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

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;

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

4) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header; and

5) in case the response is sent towards the originating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

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

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

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

1) remove its own URI from the topmost Route header;
2) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;
3) create a Record-Route header containing its own SIP URI; and
4) forward the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

1) if the response corresponds to an INVITE request, save the Record-Route and Contact header field values in the response such that the S-CSCF is able to release the session if needed; and
2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the originating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

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

1) remove its own URI from the topmost Route header; and
2) forward the request based on the topmost Route header.

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050107**
**Sydney, Australia, 14-18 February 2004**

*CR-Form-v7.1*

# CHANGE REQUEST

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.247** | **CR** | **003** | ⌘**rev** | **-** | ⌘ | Current version: | **6.0.1** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

|  |  |  |  |  |
|---|---|---|---|---|
| ***Title:*** | ⌘ | MESSAGE to unregistered user | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 01/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use one of the following releases:*<br>*Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

|  |  |  |
|---|---|---|
| ***Reason for change:*** | ⌘ | The Stage 2 document 23.228 [subclause 5.16.1.1.2] describes the procedures related to the delivery of immediate messages to unregistered public user identity. The corresponding Stage 3 text shoud be added to the document 24.247 to reflect these requirements. |
| ***Summary of change:*** | ⌘ | The added text specifies two methods of delivery of immediate messages to unregistered public user identity. |
| ***Consequences if not approved:*** | ⌘ | Incomplete specification |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.2.1 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

**How to create CRs using this form:**

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

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

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

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

#### 5.3.1.3 Receiving an immediate message

Upon receipt of a MESSAGE request, the participant shall perform the procedures as described in RFC 3428 [8] and subclause 5.1.2A.2 of 3GPP TS 24.229 [5].

NOTE: A MESSAGE request can be used for applications other than immediate messaging (e.g. 3GPP TS 23.228 [6] subclause 5.4.9), and the handling of received MESSAGE requests for such applications is outside the scope of this specification.

### 5.3.2 Application Server (AS)

#### 5.3.2.1 Receiving an immediate message for unregistered Public User Identity

When an immediate message destined for an unregistered Public User Identity arrives at the user's home network, the I-CSCF and S-CSCF perform the actions as specified in 3GPP TS 24.229 [5].

If  the Public User Identity has services related to unregistered state activated (i.e., hold the MESSAGE request temporarily in the network.), the MESSAGE request will be routed to an AS, which processes the request further on. The AS may then hold the MESSAGE request and deliver the MESSAGE request when either the UE becomes reachable or the validity of the message expires as specified in RFC 3428 [8].

# 6 Protocol using SIP for session-mode messaging

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050129**
**Sydney, Australia, 14-18 February 2004**

# 3 Definitions and abbreviations

## 3.1 Definitions

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

**Newly established set of security associations**: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200 (OK) response to a REGISTER request was received.

**Old set of security associations:** Two pairs of IPsec security associations still in existence after another set of security associations has been established due to a successful authentication procedure.

**Temporary set of security associations:** Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

**Integrity protected:** See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirements exists to check that information was received "integrity protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B].

**Fully-Qualified Domain Name (FQDN)**

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

**Back-to-Back User Agent (B2BUA)**
**Client**
**Dialog**
**Final response**
**Header**
**Header field**
**Loose routeing**
**Method**
**Option-tag** (see RFC 3261 [26] 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 [26] subclause 7.2)
**Tag** (see RFC 3261 [26] subclause 19.3)
**Target Refresh Request**
**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 4.1.1.1 and subclause 4a.7 apply:

**Breakout Gateway Control Function (BGCF)**

**Call Session Control Function (CSCF)**
**Home Subscriber Server (HSS)**
**Media Gateway Control Function (MGCF)**
**Multimedia Resource Function Controller (MRFC)**
**Multimedia Resource Function Processor (MRFP)**
**Subscription Locator Function (SLF)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclause 3.1 apply:

**Filter criteria**
**Initial filter criteria**
**Initial request**
**Standalone transaction**
**Subsequent request**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6 and 5.4.12.1 apply:

**Interrogating-CSCF (I-CSCF)**
**IMS Application Level Gateway (IMS-ALG)**
**IP-Connectivity Access Network (IP-CAN)**
**Policy Decision Function (PDF)**
**Private user identity**
**Proxy-CSCF (P-CSCF)**
**Public Service Identity (PSI)**
**Public user identity**
**Serving-CSCF (S-CSCF)**
**Statically pre-configured PSI**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

**IM Subscriber Identity Module (ISIM)**
**Protected server port**
**Protected client port**

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

**Universal Integrated Circuit Card (UICC)**
**Universal Subscriber Identity Module (USIM)**
**User Equipment (UE)**

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

**Security association**

NOTE: A number of different security associations exist within the IM CN subsystem. Within this document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is the only security association that has direct impact on SIP.

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

**International public telecommunication number**

## 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 |
| APN | Access Point Name |
| AUTN | Authentication TokeN |

| | |
|---|---|
| B2BUA | Back-to-Back User Agent |
| BGCF | Breakout Gateway Control Function |
| c | conditional |
| CCF | Charging Collection Function |
| CDR | Charging Data Record |
| CK | Ciphering Key |
| CN | Core Network |
| CSCF | Call Session Control Function |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DTD | Document Type Definition |
| ECF | Event Charging Function |
| FQDN | Fully Qualified Domain Name |
| GCID | GPRS Charging Identifier |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| HSS | Home Subscriber Server |
| i | irrelevant |
| I-CSCF | Interrogating CSCF |
| ICID | IM CN subsystem Charging Identifier |
| IK | Integrity Key |
| IM | IP Multimedia |
| IMS | IP Multimedia core network Subsystem |
| IMS-ALG | IMS Application Level Gateway |
| IMSI | International Mobile Subscriber Identity |
| IOI | Inter Operator Identifier |
| IP | Internet Protocol |
| IP-CAN | IP-Connectivity Access Network |
| IPsec | IP security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| ISC | IP ~~m~~Multimedia Subsystem Service Control |
| ISIM | IM Subscriber Identity Module |
| m | mandatory |
| MAC | Message Authentication Code |
| MCC | Mobile Country Code |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MNC | Mobile Network Code |
| MRFC | Multimedia Resource Function Controller |
| MRFP | Multimedia Resource Function Processor |
| PDP | Packet Data Protocol |
| PLMN | Public Land Mobile Network |
| PSTN | Public Switched Telephone Network |
| n/a | not applicable |
| NAI | Netework Access Identifier |
| o | optional |
| P-CSCF | Proxy CSCF |
| PDU | Protocol Data Unit |
| PSI | Public Service Identity |
| RAND | RANDom challenge |
| RES | RESponse |
| RTCP | Real-time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| S-CSCF | Serving CSCF |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SLF | Subscription Locator Function |
| SQN | SeQuence Number |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |

| | |
|---|---|
| UE | User Equipment |
| UICC | Universal Integrated Circuit Card |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UDVM | Universal Decompressor Virtual Machine |
| USIM | Universal Subscriber Identity Module |
| x | prohibited |
| XMAC | expected MAC |
| XML | eXtensible Markup Language |

[ ... ]

# 5 Application usage of SIP

## 5.1 Procedures at the UE

### 5.1.1 Registration and authentication

[ ... ]

#### 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 reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

The UE shall use the default public user identiy for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initia~~ia~~l registratio~~i~~n is not barred.

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

a) a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header set to a SIP URI that contains the public user identity used for subscription;

c) a To header set to a SIP URI that contains the public user identity used for subscription;

d) an Event header set to the "reg" event package;

e) an Expires header set to 600 000 seconds as the value desired for the duration of the subscription

f) a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3); and

g) a Contact header set to contain the same IP address or FQDN, and with the protected server port value as in the initial registration.

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

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

[ ... ]

# 5.3 Procedures at the I-CSCF

[ ... ]

## 5.3.2 Initial requests

### 5.3.2.1 Normal procedures

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

The I-CSCF shall verify for all requests whether they arrived from a trusted domain or not. If the request arrived from a non trusted domain, then the I-CSCF shall:

1) respond with 403 (Forbidden) response if the request is a REGISTER request;

2) remove all P-Asserted-Identity headers, all P-Access-Network-Info headers, all P-Charging-Vector headers and all P-Charging-Function-Addresses headers the request may contain, if the request is other than REGISTER request; and

3) continue with the procedures below.

If the request arrived from a trusted domain, the I-CSCF shall perform the procedures below.

NOTE 1: The I-CSCF may find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

When the I-CSCF receives an initial request for a dialog or standalone transaction, that does not contain a Route header, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer [58] clause 8.

NOTE 2: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, the I-CSCF shall:

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

2) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

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

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

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

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URI of the selected S-CSCF as the topmost Route header field value;

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

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

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the I-CSCF shall perform the procedures described for the case when there is no Route header present. If the I-CSCF determines that hiding must be performed for an outgoing request, ~~then the THIG functionality in I-CSCF received an outgoing initial request for which topology hiding has to be applied, and~~ the I-CSCF shall:

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

2) perform the procedures described in subclause 5.3.3; and

3) route the request based on the Request-URI header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header, the I-CSCF shall:

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

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

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

NOTE 3: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

[ ... ]

# 5.4 Procedures at the S-CSCF

## 5.4.1 Registration and authentication

### 5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs belonging to ~~of~~ the IM CN subsystem and with public user identities.

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

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 Unprotected REGISTER

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

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

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", for an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

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

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated deregistration procedure only for the previous contact information as described in subclause 5.4.1.5.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", which is not for an already registered public user identity linked to the same private user identity, the S-CSCF shall:

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

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

3) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

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

NOTE 3: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be used ~~indicated~~ by the HSS ~~for all further~~ to direct all subsequent incoming initial requests for a dialog or standalone transactions destined for this user~~, in order to direct all these requests~~ to this S-CSCF.

NOTE 4: When passing its SIP URI to the HSS, the S-CSCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

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

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

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

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

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

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

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

[ ... ]

## 5.4.2 Subscription and notification

### 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 reg event package, the S-CSCF shall:

1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:

   - all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;
   - all the entities identified by the Path header (i.e. the P-CSCF to which this user is attached to); and
   - all the ASs listed in the initial filter criteria and not belonging to third-party providers.

NOTE: The S-CSCF finds the identity for authentication of the subscription in the P-Asserted-Identity header received in the SUBSCRIBE request.

2) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in RFC 3680 [43]. The S-CSCF shall populate the header fields as follows:

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

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

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

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

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

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

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

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

   b) if the public user identity:

      I) has been deregistered (i.e. no active contact left) then:

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

      II) has been registered then:

- set the <unknown-param> element to any additional header parameters contained in the contact header of the REGISTER request according to RFC 3680 [43];

- set the state attribute within the <registration> element to "active", if not already set to "active", otherwise leave it unchanged; and either:

- for the contact address to be registered: set the state attribute within the <contact> element to "active"; and set the event attribute within the <contact> element to "registered"; or

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

III) has been automatically registered, and have not been previously automatically registered:

- set the <unknown-param> element to any additional header parameters contained in the contact header of the originsl REGISTER request according to RFC 3680 [43];

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

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

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

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

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

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

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

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

When all UE's contact addresses have been deregistered  (i.e.there is no <contact> element set to "active" for this UE), the S-CSCF shall consider subscription to the reg event package belonging to the UE cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

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

## 5.8 Procedures at the MRFC

[ ... ]

## 5.8.2 Call initiation

### 5.8.2.1 Initial INVITE

### 5.8.2.1.1 MRFC-terminating case

[ ... ]

### 5.8.2.1.1.3 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (e.g. Multiparty Call) or to add parties to~~from~~ the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator to initiate ad hoc conferencing, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conference resources are available, send 200 (OK) response with an MRFC conference identifier.If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 (OK), then the conference identifier may also be included in the 183 (Session Progress) response.

When the MRFC receives an INVITE request with an indicator to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

[ ... ]

# 9 IP-Connectivity Access Network aspects when connected to the IM CN subsystem

## 9.1 Introduction

A UE accessing the IM CN subsystem and the IM CN subsystem itself utilises the services supported by the IP-CAN to provide packet-mode communication between the UE and the IM CN subsystem. General requirements for the UE on the use of these packet-mode services are specified in this clause.

Possible aspects particular to each IP-CAN is described separately for each IP-CAN.

[ ... ]

# Annex A (normative): Profiles of IETF RFCs for 3GPP usage

## A.1 Profiles

### A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications which are referenced by this specification, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) which are referenced by this specification and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex.

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column.

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not ~~be~~ in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

For all IETF specifications that are not referenced by this document or that are not mentioned within the 3GPP profile of SIP and SDP, the generic rules as defined by RFC 3261 [26] and in addition the rules in clauses 5 and 6 of this specification apply, e.g..

- a proxy which is built in accordance to this specification passes on any unknown method, unknown header field or unknown header parameter after applying procedures such as filtering, insertion of P-Asserted-Identity header, etc.;
- an UA  which is built in accordance to this specification will
  - handle received unknown methods in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 400 (Bad Request) response; and
  - handle unknown header fields and unknown header parameters in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 420 (Bad Extension) if an extension identified by an option tag in the Require header of the received request is not supported by the UA.

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050225**

*CR-Form-v7.1*

## CHANGE REQUEST

⌘ **24.229** **CR** **841** ⌘ **rev** **-** ⌘ Current version: **6.5.1** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 27/01/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

***Reason for change:*** ⌘

At CN1#35, CR 688 R2 to 24.229 (N1-041641 → NP-040381) was agreed which made changes to the operation of the P-Access-Network-Info header across network boundaries. There appears to be some fundamental mistakes in the reasoning for parts of the above CR, which we consider need to be discussed further. There are some valid changes in the CR, but see the discussion in N1-041885 and below.

Essentially the P-Access-Network-Information header as currently used seems to carry two types of information:

1. a definition of the type of access network in use, and therefore an understanding of the associated restrictions on service applying to that user dependent on access network;
2. information relating to MCC, MNC and cell identity of the local user, and thus information on the geographic location of the local user.

Both of these types of information could be conceivably of use in providing both local and remote services however this needs to considered in regard to other extensions in SIP also defined to provide this information. Extensions are currently under development for the carriage of geographic information of variuous kinds in SIP, meeting all the requirements of GEOPRIV including privacy requirements. This mechanism should certainly used for the carriage of geolocation information in SIP between networks. It is perfectly appropriate to map P-Access-Network-Information data into these new mechanisms in the originating side network. The callee capabilities extension is the appropriate manner of providing information between user agents of the restriction of service capabilities between end user agents (including UEs and application servers), and therefore information of this form gained from the P-Access-Network-

| | | |
|---|---|---|
| | | Information header is really only of use to the local CSCFs, where callee capabilities information is not available for use.<br>This leads us to the conclusion that the P-Access-Network-Information header has no valid functionality between the originating side network and the terminating side network, as all the information contained should already be available to the remote side network with support of appropriate extensions. It is justified that the information goes to a local application server, e.g. for mapping into geolocation information. CN1 should however look for rapid support of the appropriate IETF SIP extension for carrying geolocation information. There is a valid exception to this rule which is that for emergency calls, all available information about the user/subscriber should be sent to the emergency call centre, even if geographic information is available from other means. However we are not dealing with emergency calls in release 6.<br>There is an assumption that "id" privacy can arbitrarily be applied by 3GPP to other headers other than the P-Asserted-Identity such as the P-Access-Network-Information header. Such extension of functionality really requires specification in an RFC and consequent expert review by IETF. If we restrict the use of the P-Access-Network-Information as indicated above, and therefore never result in its being sent to the remote user, we do not meet these problems, as privacy between networks is guaranteed by always removing the information (except in the case of emergency calls). Additionally, as now defined, it is impossible to separate the user privacy requirements relating to the P-Acess-Network-Info header from that of the P-Asserted-Identity. As a user, we may desire my CLI to be passed to the remote terminal, in case the remote user has usage of a service such as Anonymous Call Rejection (a service designed to deter spam callers). However we may certainly wish to keep my location, or any hint of our location, private in such circumstances. As defined currently, either both are private, or neither is private. |
| ***Summary of change:*** | ⌘ | The P-Access-Network-Info should be removed when the associated request/response is sent from the local to the remote side of the transaction.<br>The P-Access-Network-Info header does not need therefore to be subject to the "id" privacy. |
| ***Consequences if not approved:*** | ⌘ | Support of an extension to the "id" privacy in release 6 that is not accepted in IETF. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

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

### 5.4.3.1 Determination of mobile-originated or mobile-terminated case

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

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Service-Route header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,
- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the topmost Route header of the request contains the "orig" parameter. The S-CSCF shall remove the "orig" parameter from the topmost Route header; or,
- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

### 5.4.3.2 Requests initiated by the served user

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

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

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

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

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

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

4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:

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

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

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;

7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the request is not forwarded to an AS and if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see draft-ietf-iptel-rfc2806bis [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem , then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

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

12) in case of an initial request for a dialog originated from a served user, either:

   - if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

   - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) based on ~~local policy rules and~~ the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;

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

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

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

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header~~; and~~

~~2) apply the same privacy mechanism to the P-Access-Network-Info header, if present~~.

NOTE 4: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 5: The optional procedure~~s~~ above ~~are~~ is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

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

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

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

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

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

~~4) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header;~~

~~5~~4) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain ~~based on local policy rules and the destination user (Request-URI)~~, remove the P-Access-Network-Info header; and

~~6~~5) route the request based on the topmost Route header.

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

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

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

~~2) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and~~

3) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain ~~based on local policy rules and the destination user (Request-URI)~~, remove the P-Access-Network-Info header; and

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

### 5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a statically pre-configured PSI or a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

- If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

7) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

8) check whether the Request-URI equals to the saved value of the Request-URI. If there is no match, then:

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

   b) forward the request based on the Request-URI and skip the following steps;

   If there is a match, then continue with the further steps;

9) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B];

10) 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. Furthermore, the S-CSCF shall:

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

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

      - if the fork directive in the Request Disposition header was set to "no-fork", the contact with the highest qvalue parameter shall be used when building the Request-URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally what contact address to be used when building the Request-URI; otherwise

      - fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF determine the contact address to be used when building the Request-URI as directed by the Request Disposition header as described in RFC 3841 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

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

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

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

12) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header ~~and apply the same privacy mechanism to the P-Access-Network-Info header~~;

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

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

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

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;

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

~~4) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header; and~~

5) in case the response is sent towards the originating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

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

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

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

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

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

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

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. ~~In case the response is sent towards the originating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).~~

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

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

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

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. ~~In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).~~

**3GPP TSG–CN1 Meeting #37**
**Sydney, Australia, 14th to 18th February 2005**

***Tdoc*** **⌘N1-050288**

*CR-Form-v7*

# CHANGE REQUEST

⌘ **23.218 CR 74** ⌘**rev** **1** ⌘ Current version: **6.2.0** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | |
|---|---|---|---|
| ***Title:*** ⌘ | Default handling | | |
| ***Source:*** ⌘ | Orange | | |
| ***Work item code:*** ⌘ | IMS2 | ***Date:*** ⌘ | 17/02/2005 |
| ***Category:*** ⌘ | **F** | ***Release:*** ⌘ | REL-6 |
| | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use one of the following releases:*<br>*2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)* |

| | |
|---|---|
| ***Reason for change:*** ⌘ | In TS 23.218 section 5.2 about Service interaction, it is stated:<br>If the S-CSCF can not reach the Application Server, the S-CSCF shall apply the default handling associated with the trigger. This default handling shall be :<br>- to continue verifying if the triggers of lower priority in the list match; or<br>- to abandon verification of matching of the triggers of lower priority in the list; and to release the dialogue.<br>In TS 29.228 section B2 about Service profile, it is stated:<br>Default Handling determines whether the dialog should be released if the Application Server could not be reached or not; it is of type enumerated and can take the values: SESSION_CONTINUED or SESSION_TERMINATED.<br>Consequently, default handling should be taken into account in all stage 3 specifications. |
| ***Summary of change:*** ⌘ | In section 6.9.2.2, it is removed that<br>"Use of the default handling procedure by the AS is not supported in this version of this specification." |
| ***Consequences if not approved:*** | Inconsistency within TS 23.218 and between TS 29.228 and 23.218 |

| | | | | |
|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ 6.9.2.2 | | | |
| | Y | N | | |
| ***Other specs affected:*** | ⌘ X | | Other core specifications | ⌘ TS 24.229 (CR801, CR803) |
| | | X | Test specifications | |
| | | X | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | |

## How to create CRs using this form:

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

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

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

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

*** FIRST MODIFICATION ***

### 6.9.2.2 Default handling

The default handling procedure indicates whether to abandon matching of lower priority triggers and to release the dialogue, or to continue the dialogue and trigger matching.

~~Use of the default handling procedure by the AS is not supported in this version of this specification.~~

*** END OF MODIFICATION ***

**3GPP TSG–CN1 Meeting #37**
**Sydney, Australia, 14th to 18th February 2005**

***Tdoc* ⌘N1-050297**

*CR-Form-v7*

# CHANGE REQUEST

⌘ **24.229 CR 821** ⌘**rev** **1** ⌘ Current version: **6.5.1** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | |
|---|---|---|---|
| ***Title:*** | ⌘ Handling topmost Route header at the P-CSCF | | |
| ***Source:*** | ⌘ Vodafone | | |
| ***Work item code:*** | ⌘ IMS2 | ***Date:*** ⌘ | 10/01/2005 |
| ***Category:*** | ⌘ **F** | ***Release:*** ⌘ | REL-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

***Reason for change:*** ⌘ It is specified in RFC 3261 that when performing the request containing a Router header field, the proxy shall inspect the URI in the topmost Route header field value. If it indicates this proxy, the proxy removes it from the Route header field (this route node has been reached).

In Section 5.2.6.3, removing its own SIP URI from the topmost Route header is not explicitly specified, when the P-CSCF receives a request from the UE for a dialog or for a standalone transaction with a Route header containing the P-CSCF's own SIP URI on the topmost.

On the contrary, in Section 5.2.6.4, removing its own SIP URI from the topmost Route header is explicitly specified, when the P-CSCF receives a request destined to the UE for a dialog or for a standalone transaction with a Route header containing the P-CSCF's own SIP URI on the topmost.

Therefore, the handling the topmost Route header is inconsistent specified Section 5.2.6.3 and Section 5.2.6.4.

***Summary of change:*** ⌘ Deleting the sentences "remove its own SIP URI from the topmost Route header value" in Section 5.2.6.4.

***Consequences if not approved:*** ⌘ Inconsistent specification.

***Clauses affected:*** ⌘ 5.2.6.3, 5.2.6.4

***Other specs affected:*** ⌘

| Y | N | | |
|---|---|---|---|
| | X | Other core specifications | ⌘ |
| | X | Test specifications | |
| | X | O&M Specifications | |

***Other comments:*** ⌘

**How to create CRs using this form:**

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

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

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

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

*** CHANGE ***

### 5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a~~s~~ P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more then one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

~~When the P-CSCF receives a request for a dialog or a request for a standalone transaction from the UE, and the request contains a Route header, in which the SIP URI in the topmost Route header field value indicates the SIP URI of this P-CSCF, the P-CSCF shall remove its own SIP URI from the topmost Route header, prior to forwarding the request.~~

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

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;

2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

3) add its own SIP URI to the top of the Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address;

4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

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

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

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

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

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

2) store the list of Record-Route headers from the received response;

3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

4) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

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

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

1) verify if the request relates to a dialog in which the originator of the request is involved:

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog;

3) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

4) add its own SIP URI to the top of Record-Route header. The P-CSCF SIP URI is built in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address; and

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

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

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

1) store the list of Record-Route headers from the received response;

2) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

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

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and

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

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

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

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

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. The P-CSCF will not forward the request. No other actions are required;

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the Route header value in the request with the stored list of Record-Route headers for the same dialog; and

3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and

2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

### 5.2.6.4 Requests terminated by the UE

~~When the P-CSCF receives a request for a dialog or a request for a standalone transaction destined for the UE, and the request contains a Route header, in which the SIP URI in the topmost Route header field value indicates the SIP URI of this P-CSCF, the P-CSCF shall remove its own SIP URI from the topmost Route header, prior to forwarding the request.~~

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

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

1~~2~~) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

2~~3~~) if the request is an INVITE request, save a copy of the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

3~~4~~) add its own SIP URI to the top of the list of Record-Route headers and save the list. The P-CSCF SIP URI is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

4~~5~~) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

5~~6~~) store the values received in the P-Charging-Function-Addresses header;

6~~7~~) remove and store the icid parameter received in the P-Charging-Vector header; and

7~~8~~) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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

1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;

2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

    a) discard the response; or

    b) replace the Via header values with those received in the request;

3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

    a) discard the response; or

    b) replace the Record-Route header values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.

    If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and

5) if the response corresponds to an INVITE request, save the Contact and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

    a) discard the response; or

    b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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

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

1~~2~~) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

    a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

    b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2~~3~~) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter; and

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

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

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

3) remove and store the icid parameter received in the P-Charging-Vector header; and

4) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request; and

2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from the P-Called-Party-ID header of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].

2) remove and store the icid parameter from P-Charging-Vector header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

*** END OF CHANGE ***

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050299**
**Sydney, Australia, 14-18 February 2004**

was **Tdoc N1-050234**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **848** | ⌘**rev** | **1** | ⌘ | Current version: | **6.5.1** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Removal of I-CSCF normative requirement on Cx interface | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 06/02/05 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | Subclause 5.3.2.2 of 24.229 contains a normative requirement relating to the Cx inferface protocol. The Cx interface is in the scope of 29.228 and 29.229. |
| ***Summary of change:*** | ⌘ | The normative requirement is downgraded to a note. |
| ***Consequences if not approved:*** | ⌘ | Out of scope normative material in the specification. Therefore possible that CN4 change requirements and make inconsistent specifications. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.3.2.2 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

**How to create CRs using this form:**

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

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

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

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

### 5.3.2.2 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 404 (Not Found) response to the UE.

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

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

NOTE: The I-CSCF will discard any later arriving (pending) Cx answer message from the HSS.

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050315**
***was tdoc N1-050183***

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.247** | **CR** | **10** | ⌘**rev** | **2** | ⌘ | Current version: | **6.0.1** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Removing CPCP from 24.247 | | |
| ***Source:*** | ⌘ | Nokia | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 03/02/05 |
| ***Category:*** | ⌘ | **C** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | As agreed during last CN plenary, BFCP and CPCP will be removed due to these protocols are not being stabel in IETF. |
| ***Summary of change:*** | ⌘ | BFCP and CPCP and all related references are removed. |
| ***Consequences if not approved:*** | ⌘ | `Instabitiliy of Stage 3, CN1 specification not in-line with CN decision.` |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 1, 10 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

# 1 Scope

The present document provides the protocol details for the messaging service within the IP Multimedia CN Subsystem (IMS) based on the Session Initiation Protocol (SIP), the Session Description Protocol (SDP) and~~,~~ the Message Session Relay Protocol (MSRP)~~ and the Conference Policy Control Protocol (CPCP)~~. The document covers immediate messaging, session based messaging and session-based messaging conferences, as described in TS 22.340.

Where possible the present document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of SIP, SDP and ~~,~~ MSRP~~ and other protocols~~, either directly, or as modified by 3GPP TS 24.229.

The present document is applicable to Application Servers (ASs) , Media Resource Function Controllers (MRFCs), Media Resource Function Processors (MRFPs)  and to User Equipment (UE) providing messaging capabilities.

This document does not cover the signalling between a MRFC and a MRFP.

# 10 Void~~Protocol for data manipulation at the Ut reference point~~

## ~~10.1 Introduction~~

## ~~10.2 Functional entities~~

### ~~10.2.1 User Equipment (UE)~~

~~For the purpose of SIP based conferences, the UE may implement the role of a XCAP client as described in subclause 10.3.1.~~

~~The UE shall implement HTTP digest AKA (see RFC 3310 [X]) and it shall initiate a bootstrapping procedure with the bootstrapping server function located in the home network, as described in 3GPP TS 24.109 [YY].~~

~~The UE shall acquire the subscriber's certificate from PKI portal by using a bootstrapping procedure, as described in 3GPP TS 24.109 [YY].~~

~~The UE shall implement Transport Layer Security (TLS) (see RFC 2246 [Y]). The UE shall be able to authenticate the authentication proxy based on the received certificate during TLS handshaking phase.~~

### ~~10.2.2 Media Resource Function Controller (MRFC)~~

~~As the function split between the MRFC and the AS is out of scope of the present document, the procedures for the MRFC are described together with those for the AS in subclause 10.2.3.~~

### ~~10.2.3 Application Server (AS)~~

~~The AS shall implement the role of a XCAP server as described in subclause 10.3.2. As the function split between the AS and the MRFC is out of scope of the present document, only the procedures are described for a combined AS and MRFC. The AS and MRFC may either be collocated, or interoperate using a proprietary protocol and a proprietary functional split.~~

~~For the purpose of SIP-based conferences, the AS/MRFC shall act as a XCAP Server, as described in subclause 10.3.2.~~

~~The AS/MRFC may implement the role of a privileged user as described in subclause 7.3.1.~~

~~If there is no authentication proxy in the network, then the AS/MRFC shall:~~

- ~~implement the role of a network application function, as described in 3GPP TS 24.109 [YY];~~
- ~~support HTTP digest authentication and certificate authentication; and~~
- ~~implement TLS (see RFC 2246 [Y]).~~

~~Editor's Note: It needs to be clarified what physical entities can contain the Authentication Proxy and its relationship with the IMS architecture. Documentation for the case of a separate authentication proxy may need to be provided.~~

## ~~10.3 Role~~

### ~~10.3.1 XCAP client~~

~~A XCAP client shall support the manipulation of some or all of the conferencing policy data elements that are defined in draft-ietf-xcon-cpcp-xcap [Z]..The XCAP client shall comply with the requirement as specified for a privileged user role in subclause 5.3.1 in TS 24.147 [10].~~

### ~~10.3.2 XCAP Server~~

~~The XCAP server shall comply with the requirement as specified for a conference policy server role in subclause 5.3.1 in TS 24.147 [10].~~

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050316**
**Sydney, Australia, 14-18 February 2005**

*CR-Form-v7.1*

# CHANGE REQUEST

|  |  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.247** | **CR** | **11** | ⌘**rev** | **1** | ⌘ | Current version: | **6.0.1** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

|  |  |  |
|---|---|---|
| ***Title:*** | ⌘ | Corrections to Message Session Flows to align with draft-ietf-simple-message-sessions-09 |
| ***Source:*** | ⌘ | RIM |
| ***Work item code:*** | ⌘ | IMS2    ***Date:*** ⌘ 02/15/2005 |
| ***Category:*** | ⌘ | **F**    ***Release:*** ⌘ Rel-6 |

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

*Use one of the following releases:*

|  |  |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

|  |  |  |
|---|---|---|
| ***Reason for change:*** | ⌘ | Current example flows in Annex A are not conformant to draft-ietf-simple-message-sessions-09 and are not aligned with the stage 2 flows in TS 23.228. There is also an empty subclause in Annex A because no session based messaging conferencing flows are provided. |
| ***Summary of change:*** | ⌘ | Flows updated to align with TS 23.228, reflect sequence, protocol primitives and information elements as defined in draft-ietf-simple-message-sessions-09 and reference to draft-ietf-simple-message-sessions updated from 06 to 09. Session based messaging conferencing flows are also provided. |
| ***Consequences if not approved:*** | ⌘ | Confusion for implementors and potential for incompatibility problems. |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, Annex A |  |  |  |
|  |  | **Y** | **N** |  |  |
| ***Other specs affected:*** | ⌘ |  | **X** | Other core specifications | ⌘ |
|  |  |  | **X** | Test specifications |  |
|  |  |  | **X** | O&M Specifications |  |
| ***Other comments:*** | ⌘ |  |  |  |  |

**How to create CRs using this form:**

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

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

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

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

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "3G Vocabulary".

[2] 3GPP TS 22.228: " Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".

[3] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model; Stage 2".

[4] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[5] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[7] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".

[8] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[9] draft-ietf-simple-message-sessions-~~06~~09.txt (~~May~~ October 2004): "The Message Session Relay Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[10] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[11] 3GPP TS 22.340: "IP Multimedia System (IMS) messaging; Stage 1".

# Annex A (informative): Example signalling flows of messaging service operation

Editor's note: draft-ietf-simple-message-sessions-09.txt contains a TBD for IANA registration of a default MSRP port number to assist with Firewall traversal. This default port number will be assigned by IANA at publication. When the RFC is published the Annex A flow examples need to be updated to show use of the default port number in the a=path attribute and the to-path and from-path headers. Current value in the examples is 3402 and this should be replaced by the IANA assigned default port in both offer and answer.

# A.1 Scope of signalling flows

This annex gives examples of signalling flows for conferencing within the IP Multimedia CN Subsystem (IMS) based on the Session Initiation Protocol (SIP), SIP Events, the Session Description Protocol (SDP) and other protocols.

These signalling flows provide detailed signalling flows, which expand on the overview information flows provided in 3GPP TS 23.228 [6].

# A.2 Introduction

## A.2.1 General

## A.2.2 Key required to interpret signalling flows

The key to interpret signalling flows specified in 3GPP TS 24.228 [4] subclause 4.1 applies with the additions specified below.

In order to differentiate between messages for SIP and MSRP, the following notation is used:

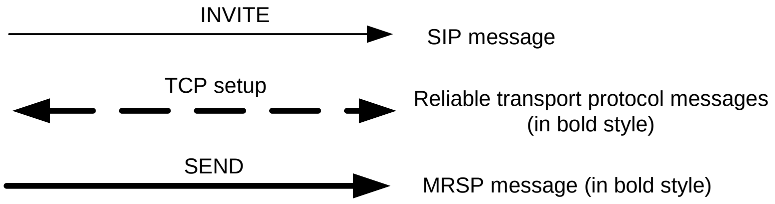

INVITE
SIP message
TCP setup
Reliable transport protocol messages (in bold style)
SEND
MRSP message (in bold style)

**Figure A.2.2-1: Signalling flow notation**

# A.3 Signalling flows demonstrating immediate messaging

The signalling flow for immediate messaging is shown in subclause 10.6 of 3GPP TS 24.228 [4].

# A.4 Signalling flows demonstrating session-based messaging

# A.4.1 Introduction

This subclause provides signalling flows for session-based messaging, established both with and without preconditions.

How the signalling flow for session-based messaging looks like depends on the following:

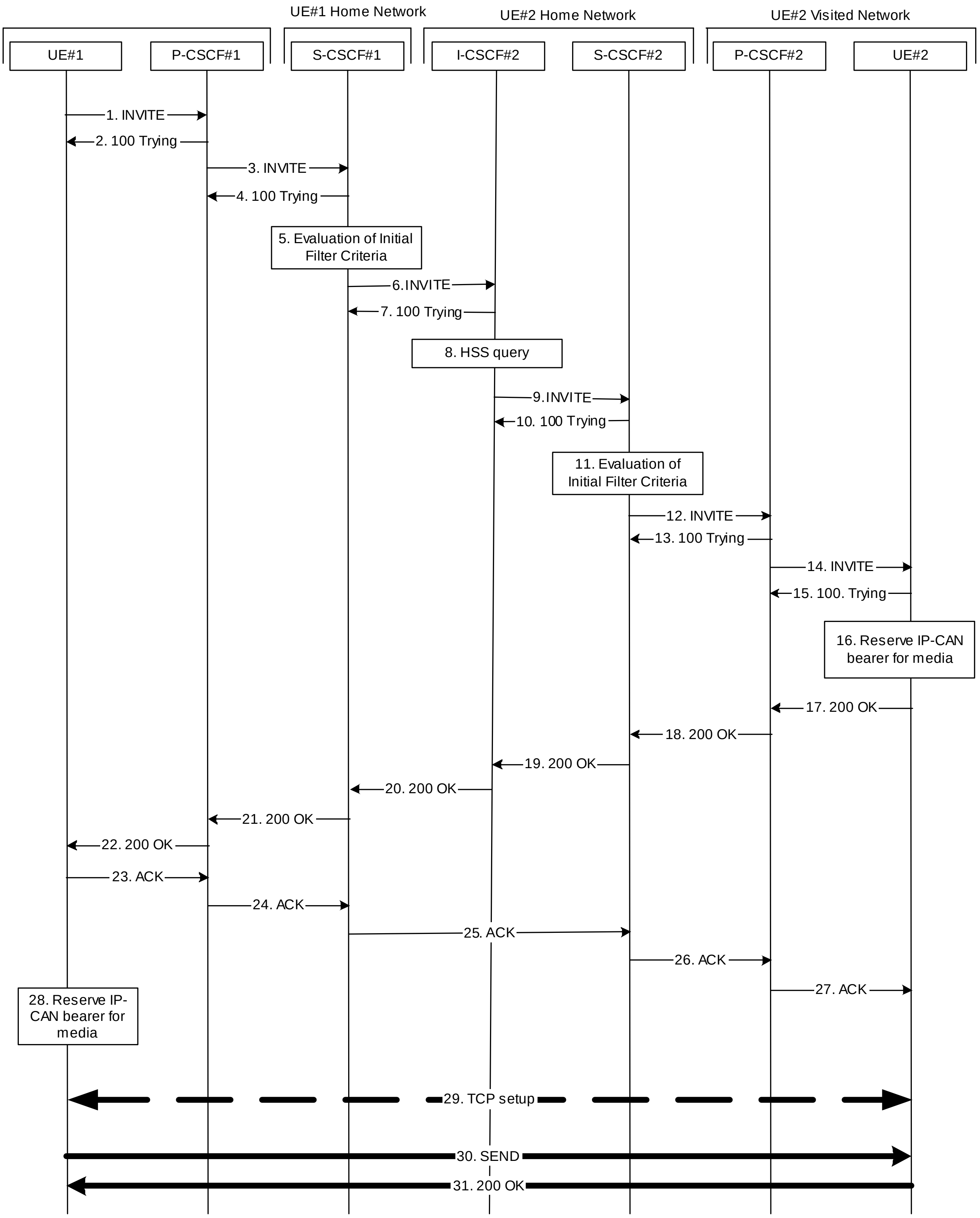
a) at what point in time the IP-CAN for the media component (MSRP) is set up; or

b) whether preconditions and reliable provisional responses are used or not.

# A.4.2 Establishing a session for session-based messaging without preconditions

Figure A.4.2-1 shows the establishment of an MSRP session between two users without the usage of preconditions and reliable provisional responses as well as the first message being sent over the established connection.

It is assumed that both the originating UE and terminating UE are using an IP-CAN with a separate bearer for SIP signalling which means that each UE needs to reserve a new IP-CAN bearer for the message session media component prior to sending the first MSRP message.


UE#1 Home Network
UE#2 Home Network
UE#2 Visited Network
UE#1
P-CSCF#1
S-CSCF#1
I-CSCF#2
S-CSCF#2
P-CSCF#2
UE#2
1. INVITE
2. 100 Trying
3. INVITE
4. 100 Trying
5. Evaluation of Initial Filter Criteria
6.INVITE
7. 100 Trying
8. HSS query
9.INVITE
10. 100 Trying
11. Evaluation of Initial Filter Criteria
12. INVITE
13. 100 Trying
14. INVITE
15. 100. Trying
16. Reserve IP-CAN bearer for media
17. 200 OK
18. 200 OK
19. 200 OK
20. 200 OK
21. 200 OK
22. 200 OK
23. ACK
24. ACK
25. ACK
26. ACK
27. ACK
28. Reserve IP-CAN bearer for media
29. TCP setup
30. SEND
31. 200 OK

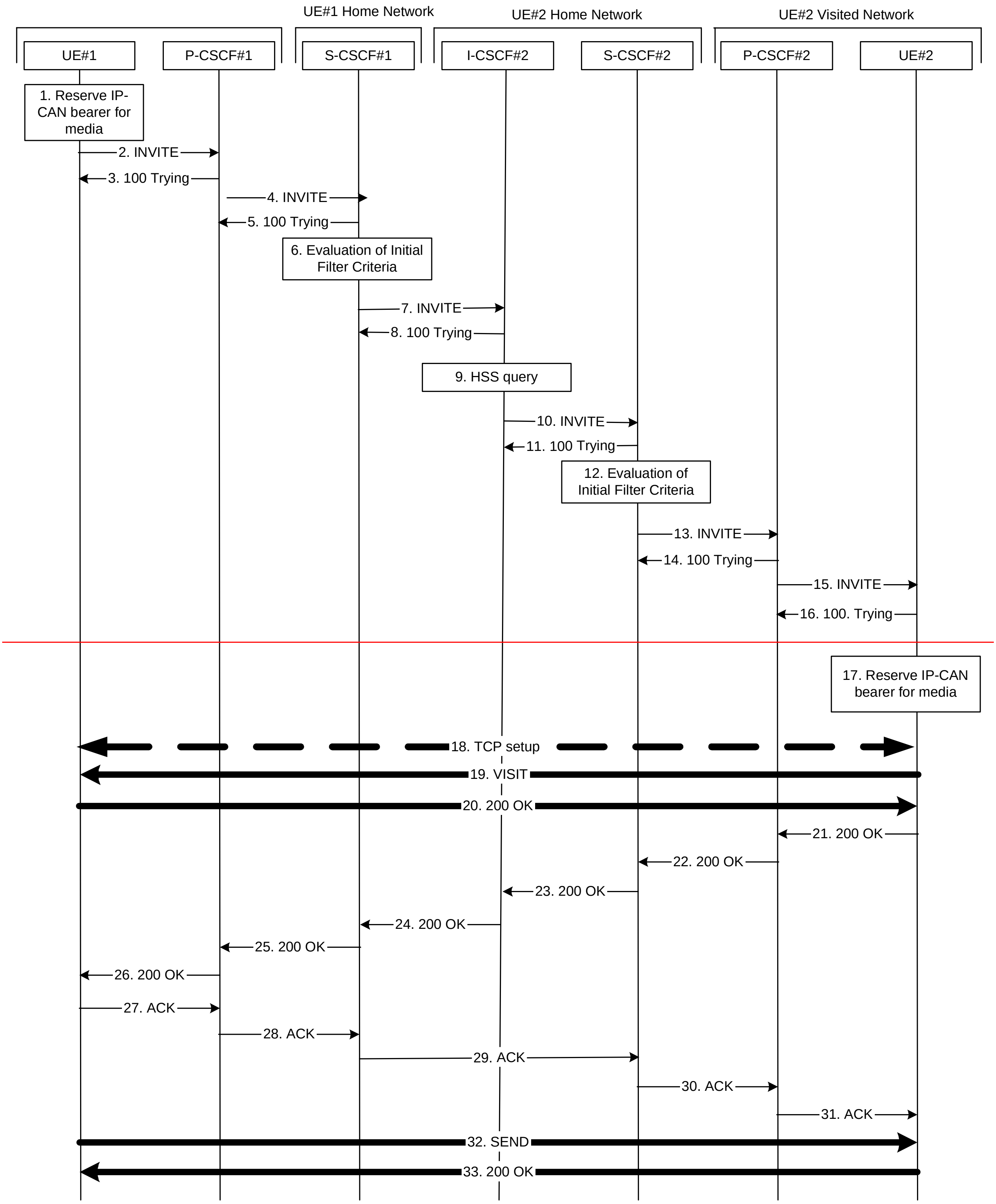


**Figure A.4.2-1: Establishment of MSRP session**

The details of the signalling flows are as follows:

~~1. Reserve IP-CAN bearer for media~~

~~The originating UE wants to initiate a session-based message session with the terminating UE. The originating UE reserves an IP-CAN bearer for the message session media component.~~

**~~2~~1. INVITE request (UE#1 to P-CSCF#1) - see example in table A.4.2-~~2~~1**

The originating UE wants to initiate a session-based message session with the terminating UE. The originating UE creates a local MSRP URL, which can be used for the communication between the two user agents. It builds a SDP Offer containing the generated MSRP URL and assigns a local port number for the MSRP communication.

**Table A.4.2-~~2~~1: INVITE request (UE#1 to P-CSCF#1)**

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
   port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd~~my.msrp.dummy.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
a=max-size:131072
```

**SDP** The SDP contains a set of content types supported by UE#1 and desired by the user at UE#1 for this session in the accept-types attribute and indicates the maximum size message that can be receieved by UE#1 in the max-size attribute.

**~~3~~2. 100 (Trying) response (P-CSCF#1 to UE#1) - see example in table A.4.2-~~3~~2**

The P-CSCF responds to the INVITE request with a 100 (Trying) response provisional response.

**Table A.4.2-~~3~~2: 100 (Trying) response (P-CSCF#1 to UE#1)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

**~~4~~3. INVITE request (P-CSCF#1 to S-CSCF#1) - see example in table A.4.2-~~4~~3**

The INVITE request is forwarded to the S-CSCF.

**Table A.4.2-~~4~~3: INVITE request (P-CSCF#1 to S-CSCF#1)**

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:orig@scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length: (…)

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

**~~5~~4. 100 (Trying) response (S-CSCF#1 to P-CSCF#1) - see example in table A.4.2-~~5~~4**

The S-CSCF responds to the INVITE request with a 100 (Trying) response provisional response.

**Table A.4.2-~~5~~4: 100 (Trying) response (S-CSCF#1 to P-CSCF#1)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

**~~6~~5. Evaluation of initial filter criteria**

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias.

**~~7~~6. INVITE request (S-CSCF#1 to I-CSCF#2) - see example in table A.41-~~7~~6**

S-CSCF#1 forwards the INVITE request to the I-CSCF#2.

### Table A.4.2-~~7~~6: INVITE request (S-CSCF#1 to I-CSCF#2)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length: (...)

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

### ~~8~~7. 100 (Trying) response (I-CSCF#2 to S-CSCF#1) - see example in table A.4.2-~~8~~ 7

I-CSCF#2 sends a 100 (Trying) response provisional response to S-CSCF#1.

### Table A.4.2-~~8~~7: 100 (Trying) response (I-CSCF#2 to S-CSCF#1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### ~~9~~8. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

### ~~10~~9. INVITE request (I-CSCF#2 to S-CSCF#2) – see example in table A.4.2-~~10~~9

I-CSCF#2 forwards the INVITE request to the S-CSCF#2 that will handle the session termination.

### Table A.4.2-~~10~~9: INVITE request (I-CSCF#2 to S-CSCF#2)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:scscf2.home2.net;lr>
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length:

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

~~11~~10. **100 (Trying) response (S-CSCF#2 to I-CSCF#2) – see example in table A.4.2-~~11~~10**

S-CSCF#2 responds to the INVITE request with a 100 (Trying) response provisional response.

### Table A.4.2-~~11~~10: 100 (Trying) response (S-CSCF#2 to I-CSCF#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

~~12~~11. **Evaluation of initial filter criterias**

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias.

~~13~~12. **INVITE request (S-CSCF#2 to P-CSCF#2) – see example in table A.4.2-~~13~~12**

S-CSCF#2 forwards the INVITE request, as determined by the termination procedure. S-CSCF#2 remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE.

### Table A.4.2-~~13~~12: INVITE request (S-CSCF#2 to P-CSCF#2)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>,
   <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (…)

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

### ~~14~~13. 100 (Trying) response (P-CSCF#2 to S-CSCF#2) – see example in table A.4.2-~~14~~13

S-CSCF#2 receives a 100 (Trying) response provisional response to the INVITE request.

### Table A.4.2-~~14~~13: 100 (Trying) response (P-CSCF#2 to S-CSCF#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### ~~15~~14. INVITE request (P-CSCF#2 to UE#2) – see example in table A.4.2-~~15~~14

P-CSCF#2 forwards the INVITE request to the terminating UE.

### Table A.4.2-~~15~~14: INVITE request (P-CSCF#2 to UE#2)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 65
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>,
   <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
P-Called-Party-ID:
Content-Type:
Content-Length: (...)

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

**~~16~~15. 100 (Trying) response (UE#2 to P-CSCF#2) – see example in table A.4.2-~~16~~15**

The terminating UE sends a 100 (Trying) response provisional response to P-CSCF#2.

### Table A.4.2-~~16~~15: 100 (Trying) response (UE#2 to P-CSCF#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

**~~17~~16. Reserve IP-CAN bearer for media**

The terminating UE accepts the message session. The terminating UE reserves an IP-CAN bearer for the message session media component.

~~**18. TCP setup**~~

~~The terminating UE establishes a TCP connection using the IP-CAN bearers established in step 1 and step 17 to the host address and the port as specified in the MSRP URL received in the SDP Offer from the originating UE.~~

~~**19. MSRP VISIT request (UE#1 to UE#2) – see example in table A.4.2-19**~~

~~The terminating UE sends an MSRP VISIT request using the established TCP connection.~~

### ~~Table A.4.2-19: MSRP VISIT request (UE to UE)~~

```
~~MSRP VISIT~~
~~Boundary: dkei38sd~~
~~To-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271~~
~~From-path:msrp://[5555::eee:fff:aaa:bbb]:3333/s234167~~
~~TR-ID: 2810~~
~~Message-ID: 2810~~
~~-------dkei38sd$~~
```

~~**Boundary:** Boundary string used to terminate message~~

~~**To-path:** The sender's remote path~~

~~**From-path:** The sender's local URL~~

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

~~**Message-ID:** A unique message ID for MSRP message.~~

~~**Closing:** Same boundary string as well as Continuation-Flag~~

~~20. **MSRP 200 (OK) response (UE#2 to UE#1) – see example in table A.4.2-20**~~

~~The originating UE that acts as an MSRP host returns an MSRP 200 (OK) response to the MSRP VISIT request using the established TCP connection.~~

### ~~Table A.4.2-20: 200 (OK) response (UE#2 to UE#1)~~

```
~~MSRP 200 OK~~
~~Boundary: wej28su~~
~~To-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271~~
~~From-path:msrp://[5555::eee:fff:aaa:bbb]:3333/s234167~~
~~TR-ID: 2810~~
~~-------wej28su$~~
```

~~**TR-ID:** The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

~~21~~17. **200 (OK) response (UE#2 to P-CSCF#2) – see example in table A.4.2-~~21~~17**

After reserving an IP-CAN bearer for the message session media component ~~the receipt of the the MSRP 200 (OK) response to the MSRP VISIT request,~~ the terminating UE sends a 200 (OK) response for the INVITE request containing SDP that indicates that the terminating UE has accepted the message session and listens on the MSRP TCP port returned in the path attribute in the answer for a TCP SETUP from the originating UE.~~successfully visited to the originating UE~~.

**Table A.4.2-~~21~~17: 200 (OK) response (UE#2 to P-CSCF#2)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>>, <sip:scscf2.home2.net;lr>,
   <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
Privacy: none
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933617 IN IP6 5555::eee:fff:aaa:bbb~~aaa:bbb:ccc:ddd~~
s=-
c=IN IP6 5555::eee:fff:aaa:bbb~~my.MSRP.dummy.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:text/plain text/html message/cpim
a=path:msrp://[5555::eee:fff:aaa:bbb]:~~3333~~3402/s234167;tcp
a=max-size:65536
```

**SDP** The SDP contains the set of offered content types supported by UE#2 and desired by the user at UE#2 for this session in the accept-types attribute and indicates the maximum size message that can be receieved by UE#2 in the max-size attribute.

### ~~22~~18. 200 (OK) response (P-CSCF#2 to S-CSCF#2) – see example in table A.4.2-~~22~~18

P-CSCF#2 forwards the 200 (OK) response to S-CSCF#2.

**Table A.4.2-~~22~~18: 200 (OK) response (P-CSCF#2 to S-CSCF#2)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity: John Smith" <sip:user2_public1@home2.net>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

## ~~23~~19. 200 (OK) response (S-CSCF#2 to I-CSCF#2) – see example in table A.4.2-~~23~~19

S-CSCF#2 forwards the 200 (OK) response to I-CSCF#2.

**Table A.4.2-~~23~~19: 200 (OK) response (S-CSCF#2 to I-CSCF#2)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
   term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
   ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

## ~~24~~20. 200 (OK) response (I-CSCF#2 to S-CSCF#1) – see example in table A.4.2-~~24~~20

I-CSCF#2 forwards the 200 (OK) response to S-CSCF#1.

**Table A.4.2-~~24~~20: 200 (OK) response (I-CSCF#2 to S-CSCF#1)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy: none
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~25~~21. 200 (OK) response (S-CSCF#1 to P-CSCF#1) – see example in table A.4.2-~~25~~21

S-CSCF#1 forwards the 200 (OK) response to P-CSCF#1.

**Table A.4.2-~~25~~21: 200 (OK) response (S-CSCF#1 to P-CSCF#1)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~26~~22. 200 (OK) response (P-CSCF#1 to UE#1) – see example in table A.4.2-~~26~~22

P-CSCF#1 forwards the 200 (OK) response to the originating UE.

### Table A.4.2-~~26~~22: 200 (OK) response (P-CSCF#1 to UE#1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>,
   <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~27~~23. ACK request (UE#1 to P-CSCF#1) – see example in table A.4.2-~~27~~23

The UE responds to the 200 (OK) response with an ACK request sent to the P-CSCF#1.

### Table A.4.2-~~27~~23: ACK request (UE#1 to P-CSCF#1)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>,
   <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 ACK
Content-Length: 0
```

### ~~28~~24. ACK request (P-CSCF#1 to S-CSCF#1) – see example in table A.4.2-~~28~~24

The P-CSCF#1 forwards the ACK request to S-CSCF#1.

### Table A.4.2-~~28~~24: ACK request (P-CSCF#1 to S-CSCF#1)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### ~~29~~25. ACK request  (S-CSCF#1 to S-CSCF#2) - see example in table A.4.2-~~29~~25

The S-CSCF#1 forwards the ACK request to the the S-CSCF#2.

### Table A.4.2-~~29~~25: ACK request (S-CSCF#1 to S-CSCF#2)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### ~~30~~26. ACK request (S-CSCF#2 to P-CSCF#2) – see example in table A.4.2-~~30~~26

S-CSCF#1 forwards the ACK request to P-CSCF#2.

### Table A.4.2-~~30~~26: ACK request (S-CSCF#2 to P-CSCF#2)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### ~~31~~27. ACK request (P-CSCF#2 to UE#2) – see example in table A.4.2.~~31~~27

P-CSCF#2 forwards the ACK request to the terminating UE.

### Table A.4.2-~~31~~27: ACK request (P-CSCF#2 to UE#2)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 66
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### 28. Reserve IP-CAN bearer for media

The originating UE reserves an IP-CAN bearer for the message session media component.

### 29. TCP setup

The originating UE establishes a TCP connection using the IP-CAN bearers established in step 16 and step 28 to the host address and the port as specified in the MSRP URL received in the SDP Answer from the terminating UE.

### 30~~2~~. MSRP SEND request (UE#1 to UE#2) – see example in table A.4.2-30~~2~~

The originating UE sends the first message over the MSRP session with an MSRP SEND request using the established TCP connection.

**Table A.4.2-30~~2~~: MSRP SEND request (UE#1 to UE#2)**

```
MSRP d93kswow SEND
~~Boundary: d93kswow~~
To-path:msrp://[5555::eee:fff:aaa:bbb]:~~3333~~3402/s234167;tcp
From-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
~~TR-ID: 8822~~
Message-ID: 8822
Byte-Range: 1-77/77
Content-Type: "text/plain"

those are my principles. If you don't like them I have others – Groucho Marx.
-------d93kswow$
```

~~**Boundary:** Boundary string used to terminate message~~

**To-path:** The sender’s remote path

**From-path:** The sender’s local URL

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

**Message-ID:** A unique message ID for MSRP message.

**Byte-Range:** The Byte Range for this message.

**Content-Type:** The format of the body of the request.

~~**Closing:** Same boundary string as well as Continuation-Flag~~

~~33~~31. **MSRP 200 (OK) response (UE#2 to UE#1) – see example in table A.4.2-~~33~~31**

The terminating UE acknowledges the reception of the MSRP SEND request with an MSRP 200 (OK) response using the established TCP connection.

**Table A.4.2-~~33~~31: MSRP 200 (OK) response (UE#2 to UE#1)**

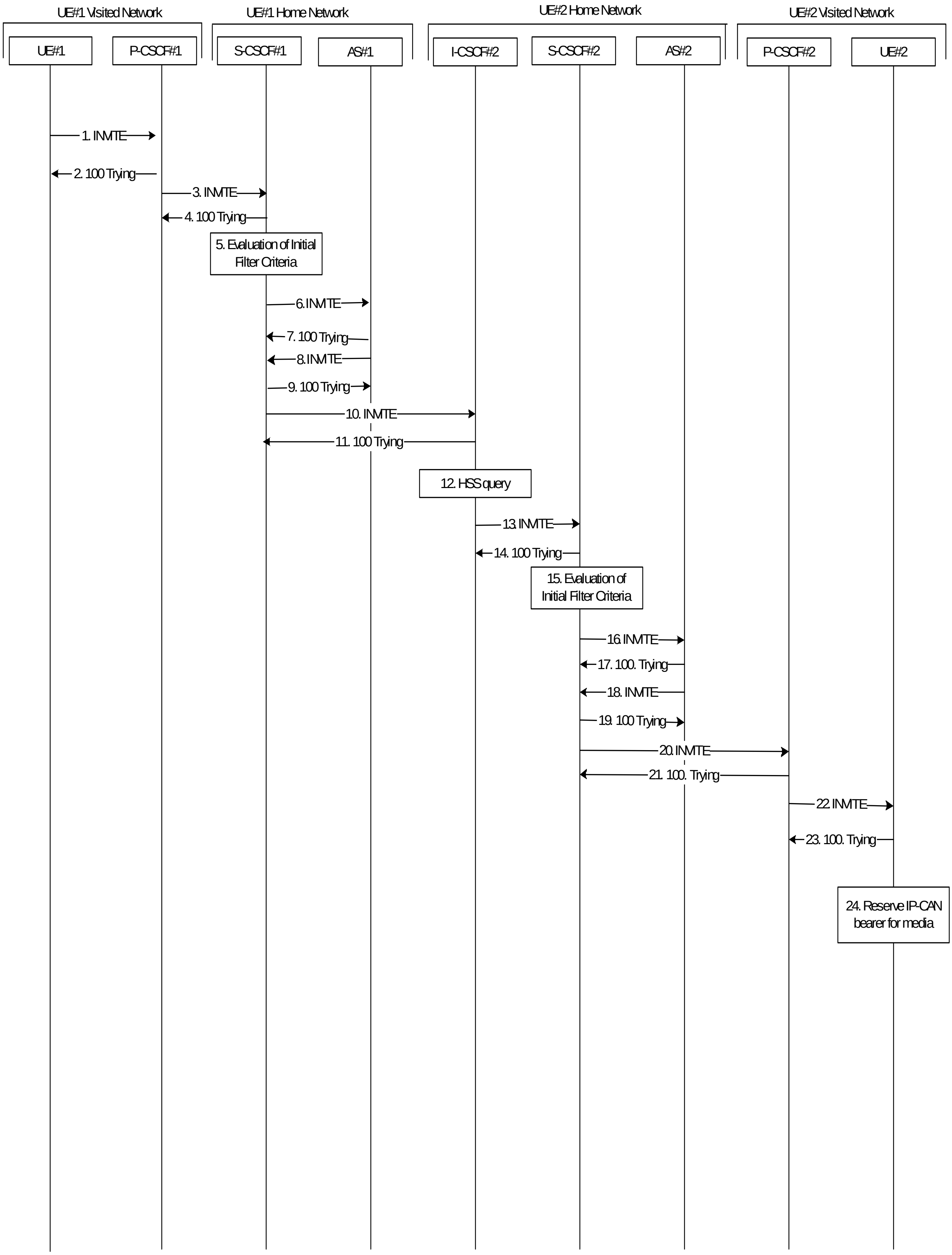
```
MSRP d93kswow 200 OK
~~Boundary: 839s9ed~~
To-path:msrp://[5555::eee:fff:aaa:bbb]:3333/s234167;tcp
From-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
~~TR-ID: 8822~~
-------d93kswow~~839s9ed~~$
```

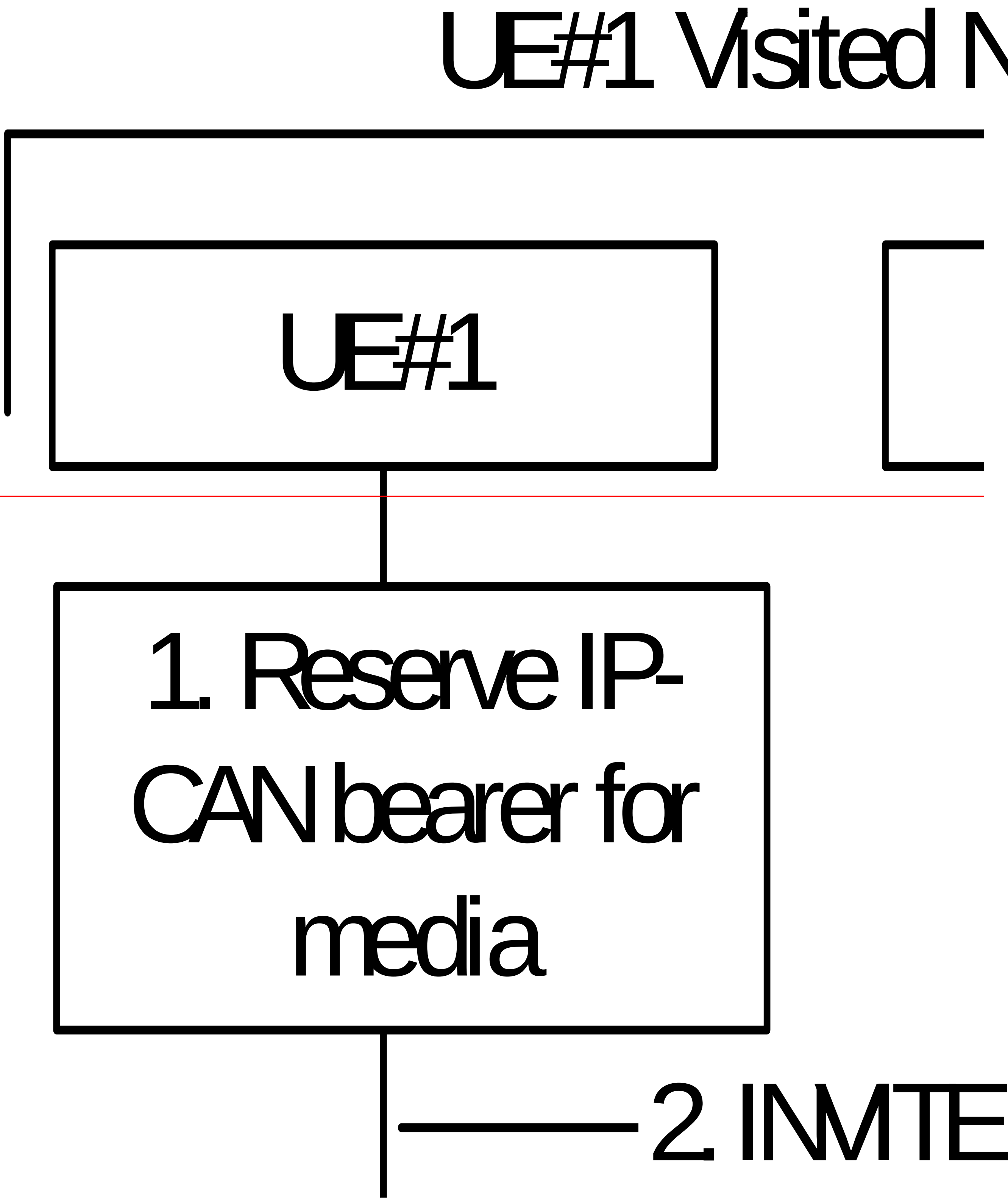
~~**TR-ID:** The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

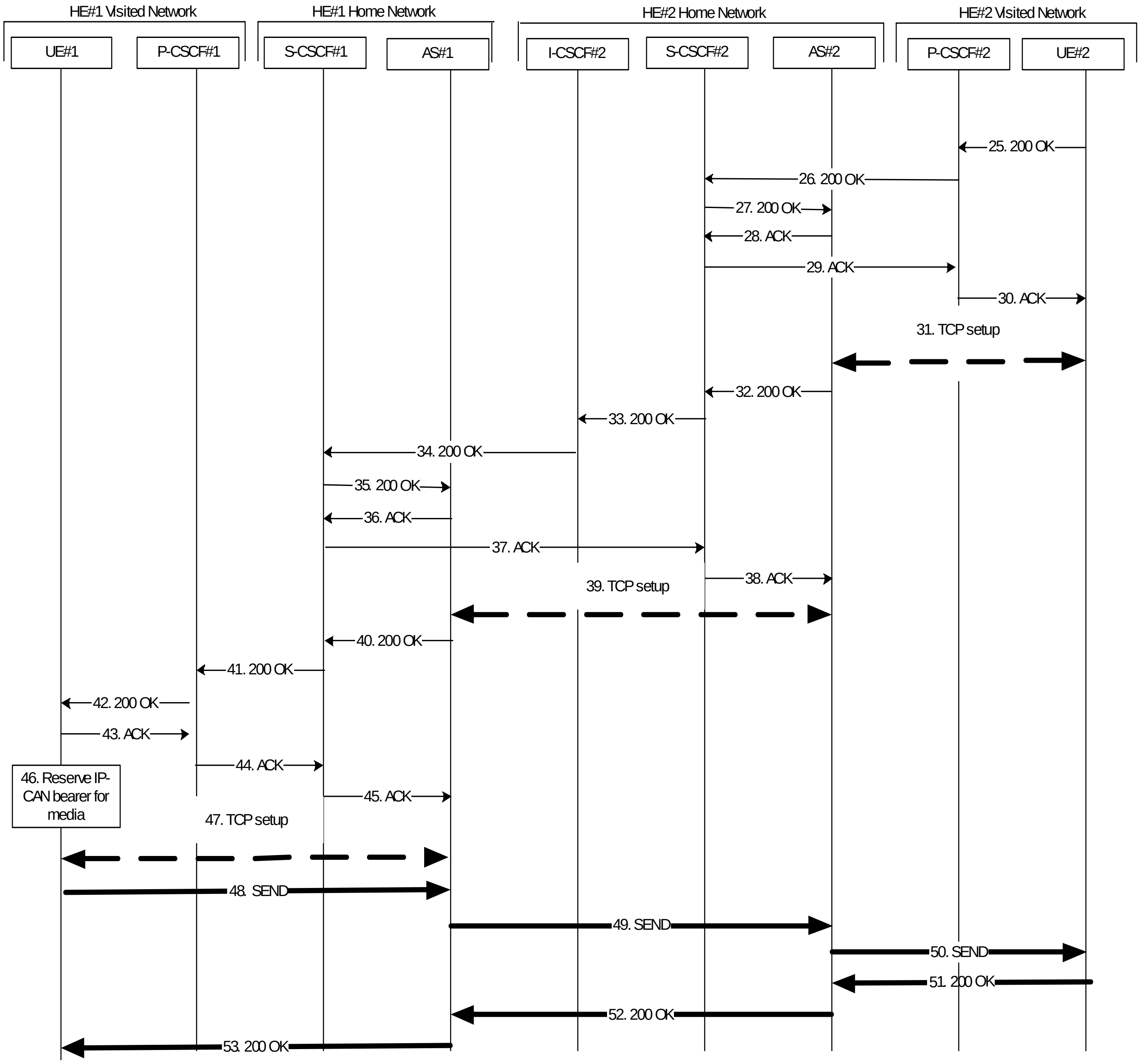
## A.4.3 Establishing a session for session-based messaging with Intermediate Nodes

Figure A.4.3-1 shows the establishment of a MSRP session between two users with intermediate nodes being added to the signalling path as well as the first message being sent over the established connection.

It is assumed that both the originating UE and terminating UE are using an IP-CAN with a separate bearer for SIP signalling which means that each UE needs to reserve a new IP-CAN bearer for the message session media component.


UE#1 Visited Network
UE#1 Home Network
UE#2 Home Network
UE#2 Visited Network
UE#1
P-CSCF#1
S-CSCF#1
AS#1
I-CSCF#2
S-CSCF#2
AS#2
P-CSCF#2
UE#2
1. INVITE
2. 100 Trying
3. INVITE
4. 100 Trying
5. Evaluation of Initial Filter Criteria
6. INVITE
7. 100 Trying
8. INVITE
9. 100 Trying
10. INVITE
11. 100 Trying
12. HSS query
13. INVITE
14. 100 Trying
15. Evaluation of Initial Filter Criteria
16. INVITE
17. 100. Trying
18. INVITE
19. 100 Trying
20. INVITE
21. 100. Trying
22. INVITE
23. 100. Trying
24. Reserve IP-CAN bearer for media


UE#1 Visited N
UE#1
1. Reserve IP-CAN bearer for media
2. INVITE


HE#1 Visited Network
HE#1 Home Network
HE#2 Home Network
HE#2 Visited Network
UE#1
P-CSCF#1
S-CSCF#1
AS#1
I-CSCF#2
S-CSCF#2
AS#2
P-CSCF#2
UE#2
25. 200 OK
26. 200 OK
27. 200 OK
28. ACK
29. ACK
30. ACK
31. TCP setup
32. 200 OK
33. 200 OK
34. 200 OK
35. 200 OK
36. ACK
37. ACK
38. ACK
39. TCP setup
40. 200 OK
41. 200 OK
42. 200 OK
43. ACK
44. ACK
45. ACK
46. Reserve IP-CAN bearer for media
47. TCP setup
48. SEND
49. SEND
50. SEND
51. 200 OK
52. 200 OK
53. 200 OK

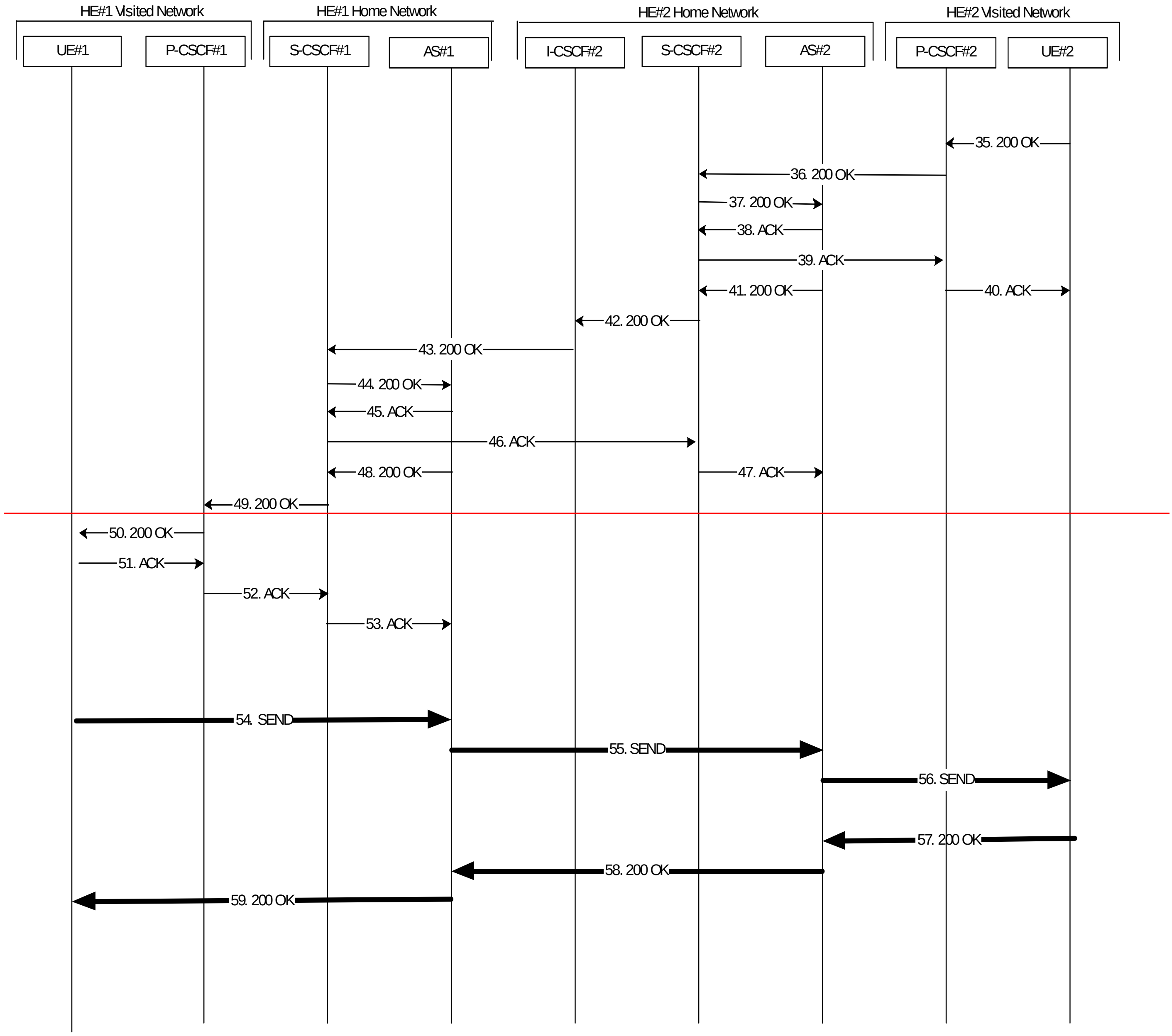


**Figure A.4.3-1: Establishment of MSRP session with Intermediate Nodes**

Editor's Note: It is FFS if the labelling of the intermediate nodes should be AS or AS/MRFC/MRFP.

The details of the signalling flows are as follows:

~~1. Reserve IP-CAN bearer for media~~

~~The originating UE#1 wants to initiate a session-based message session with the terminating UE#2. UE#1 reserves an IP-CAN bearer for the message session media component.~~

~~2~~1. **INVITE request (UE#1 to P-CSCF#1) - see example in table A.4.3-~~2~~1**

The originating UE#1 wants to initiate a session-based message session with the terminating UE#2. UE#1 creates a local MSRP URL, which can be used for the communication between the two user agents. It builds a SDP Offer containing the generated MSRP URL and assigns a local port number for the MSRP communication.

### Table A.4.3-~~2~~1: INVITE request (UE#1 to P-CSCF#1)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi=87654321; port1=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd~~my.msrp.dummy.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
a=max-size:131072
```

**SDP** The SDP contains the set of content types supported by UE#1 and desired by the user at UE#1 for this session in the accept-types attribute and indicates the maximum size message that can be receieved by UE#1 in the max-size attribute.

~~3~~2. **100 (Trying) response (P-CSCF#1 to UE#1) - see example in table A.4.3-~~3~~2**

The P-CSCF responds to the INVITE request with a 100 (Trying) response provisional response.

### Table A.4.3-~~3~~2: 100 (Trying) response (P-CSCF#1 to UE#1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

~~4~~3. **INVITE request (P-CSCF#1 to S-CSCF#1) - see example in table A.4.3-~~4~~3**

The INVITE request is forwarded to the S-CSCF.

**Table A.4.3-~~4~~3: INVITE request (P-CSCF#1 to S-CSCF#1)**

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:orig@scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length: (…)

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

### ~~5~~4. 100 (Trying) response (S-CSCF#1 to P-CSCF#1) - see example in table A.4.3-~~5~~4

The S-CSCF responds to the INVITE request with a 100 (Trying) response provisional response.

**Table A.4.3-~~5~~4: 100 (Trying) response (S-CSCF#1 to P-CSCF#1)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### ~~6~~5. Evaluation of initial filter criterias

S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criterias. For sip:user1_public1@home1.net S-CSCF#2 has origination initial filter criteria with service points of interest of Method = INVITE request and SDP m= 'message' and 'msrp' protocol that informs the S-CSCF to route the INVITE request to the AS sip:as1.home1.net.

### ~~7~~6. INVITE request (S-CSCF#1 to AS#1) - see example in table A.4.3-~~7~~6

S-CSCF#1 forwards the INVITE request to the AS#1.

### Table A.4.3-~~7~~6: INVITE request (S-CSCF#1 to AS#1)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Route: <sip:as1.home1.net;lr>, <sip:cb03a0s09a2sdfglkj490333@scscf1.home1.net;lr>
Record-Route: <sip:orig@scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
   ecf=[5555::1ff:2ee:3dd:4ee]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length: (...)

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

### ~~8~~7. 100 (Trying) response (AS#1 to S-CSCF#1) - see example in table A.4.3-~~8~~ 7

AS#1 sends a 100 (Trying) response provisional response to S-CSCF#1.

### Table A.4.3-~~8~~7: 100 (Trying) response (AS#1 to S-CSCF#1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### ~~9. TCP setup~~

~~AS#1 establishes a TCP connection using the IP-CAN bearers established in step 1 to the host address and port as specified in the MSRP URL received in the SDP Offer from the originating UE#1.~~

### ~~10~~8. INVITE request (AS#1 to S-CSCF#1) - see example in table A.4.3-~~10~~8

AS#1 sends a new INVITE request to the S-CSCF#1 with the session attribute containing a unique URL for the AS#1 to receive media on.

### Table A.4.3-~~10~~8: INVITE request (AS#1 to S-CSCF#1)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP as1.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 70
Route: <sip:cb03a0s09a2sdfglkj490333@scscf1.home1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=323551024"
Privacy: none
From: <sip:user1_public1@home1.net>; tag=234567
To: <sip:user2_public1@home2.net>
Call-ID: s09a233cbsdfglkj490303a0
Cseq: 278 INVITE
Contact: <sip:[7777::eee:ddd:ccc:aaa]>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (...)

v=0
o=- 2987933620 2987933620 IN IP6 7777::eee:ddd:ccc:aaa
s=-
c=IN IP6 7777::eee:ddd:ccc:aaa~~as1.home1.net.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222371;tcp
a=max-size:65536
```

**SDP** The SDP contains the set of offered content types allowed by the policy of network home1 in the accept-types attribute and indicates the maximum size message that can be receieved by UE#1 and allowed by the policy of network home1 in the max-size attribute.

**~~11~~9. 100 (Trying) response (S-CSCF#1 to AS#1) - see example in table A.4.3-~~11~~ 9**

S-CSCF#1 sends a 100 (Trying) response provisional response to AS#1.

### Table A.4.3-~~11~~9: 100 (Trying) response (S-CSCF#1 to AS#1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP as1.home1.net;branch=z9hG4bK240f34.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

**~~12~~10. INVITE request (S-CSCF#1 to I-CSCF#2) – see example in table A.4.3-~~12~~10**

S-CSCF#1 forwards the INVITE request to the I-CSCF#2. As the S-CSCF#1 does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

### Table A.4.3-~~12~~10: INVITE request (S-CSCF#1 to I-CSCF#2)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 69
Record-Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=323551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length:

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

**~~13~~11. 100 (Trying) response (I-CSCF#2 to S-CSCF#1) - see example in table A.4.3-~~13~~ 11**

I-CSCF#2 sends a 100 (Trying) response provisional response to S-CSCF#1.

### Table A.4.3-~~13~~11: 100 (Trying) response (I-CSCF#1 to S-CSCF#1)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

**~~14~~12. Cx: User Location Query procedure**

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

**13~~5~~. INVITE request (I-CSCF#2 to S-CSCF#2) – see example in table A.4.3-~~15~~13**

I-CSCF#2 forwards the INVITE request to the S-CSCF#2 that will handle the session termination.

**Table A.4.3-~~15~~13: INVITE request (I-CSCF#2 to S-CSCF#2)**

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 68
Route: <sip:scscf2.home2.net;lr>
Record-Route:
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length:

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

NOTE: The I-CSCF does not add itself to the Record-Route header, as it has no need to remain in the signalling path once the session is established.

~~16~~14. **100 (Trying) response (S-CSCF#2 to I-CSCF#2) – see example in table A.4.3-~~16~~14**

S-CSCF#2 responds to the INVITE request with a 100 (Trying) response provisional response.

**Table A.4.3-~~16~~14: 100 (Trying) response (S-CSCF#2 to I-CSCF#2)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

~~17~~15. **Evaluation of initial filter criterias**

S-CSCF#2 validates the service profile of this subscriber and evaluates the initial filter criterias. For sip:user2_public1@home2.net S-CSCF#2 has termination initial filter criteria with service points of interest of Method = INVITE request and SDP m = 'message' and 'msrp' protocol that informs the S-CSCF to route the INVITE request to the AS sip:as2.home2.net.

~~18~~16. **INVITE request (S-CSCF#2 to AS#2) – see example in table A.4.3-~~18~~16**

S-CSCF#2 forwards the INVITE request to AS#2

### Table A.4.3-~~18~~16: INVITE request (S-CSCF#2 to AS#2)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 67
Route: <sip:as2.home2.net;lr>,<sip:s09a233cbsdfglkj490303a0@scscf2.home2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
P-Charging-Function-Addresses: ccf=[6666::b99:c88:d77:e66]; ccf=[6666::a55:b44:c33:d22];
   ecf=[6666::1ff:2ee:3dd:4ee]; ecf=[6666::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length: (…)

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

~~19~~17. **100 (Trying) response (AS#2 to S-CSCF#2) – see example in table A.4.3-~~19~~17**

S-CSCF#2 receives a 100 (Trying) response provisional response to the INVITE request.

### Table A.4.3-~~19~~17: 100 (Trying) response (AS#2 to S-CSCF#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

~~20. **TCP setup**~~

~~AS#2 establishes a TCP connection to the host address and port as specified in the MSRP URL received in the SDP Offer from the AS#1.~~

~~21~~18. **INVITE request (AS#2 to S-CSCF#2) – see example in table A.4.3-~~21~~18**

AS#2 sends a new INVITE request to the S-CSCF#2 with the session attribute containing a unique URL for the AS#2 to receive media on.

### Table A.4.3-~~21~~18: INVITE request (AS#2 to S-CSCF#2)

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP as2.home2.net;branch=z9hG4bK348923.1
Max-Forwards: 70
Route: <sip:s09a233cbsdfglkj490303a0@scscf2.home2.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=423551024"
Privacy: none
From: <sip:user1_public1@home1.net>; tag=7871654
To: <sip:user2_public1@home2.net>
Call-ID: 0s09glkj4903a2sdf33cb03a
Cseq: 210 INVITE
Contact: <sip:[9999::ccc:aaa:bbb:ddd]>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933630 2987933630 IN IP6 9999::ccc:aaa:bbb:ddd
s=-
c=IN IP6 9999::ccc:aaa:bbb:ddd~~as2.home2.net.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317121;tcp
a=max-size:32768
```

**SDP** The SDP contains the set of offered content types allowed by the policy of network home2 in the accept-types attribute and indicates the maximum size message that can be receieved by UE#1 and allowed by the policy of network home2 in the max-size attribute.

### ~~22~~19. 100 (Trying) response (S-CSCF#2 to AS#2) – see example in table A.4.3-~~22~~19

S-CSCF#2 receives a 100 (Trying) response provisional response to the INVITE request.

### Table A.4.3-~~22~~19: 100 (Trying) response (S-CSCF#2 to AS#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP as2.home2.net;branch=z9hG4bK348923.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### ~~23~~20. INVITE request (S-CSCF#2 to P-CSCF#2) – see example in table A.4.3-~~23~~20

S-CSCF#2 forwards the INVITE request, as determined by the termination procedure. S-CSCF#2 remembers (from the registration procedure) the UE Contact address and the next hop CSCF for this UE.

**Table A.4.3-~~23~~20: INVITE request (S-CSCF#2 to P-CSCF#2)**

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
Max-Forwards: 69
Route: <sip:pcscf2.visited2.net;lr>
Record-Route: <sip:scscf2.home2.net;lr>
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (…)

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

~~24~~21. **100 (Trying) response (P-CSCF#2 to S-CSCF#2) – see example in table A.4.3-~~24~~21**

S-CSCF#2 receives a 100 (Trying) response provisional response to the INVITE request.

**Table A.4.3-~~24~~21: 100 (Trying) response (P-CSCF#2 to S-CSCF#2)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

22~~5~~. **INVITE request (P-CSCF#2 to UE#2) – see example in table A.4.3-22~~5~~**

P-CSCF#2 forwards the INVITE request to the terminating UE.

### Table A.4.3-22~~5~~: INVITE request (P-CSCF#2 to UE#2)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
Max-Forwards: 68
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
P-Called-Party-ID:
Content-Type:
Content-Length: (...)

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

23~~6~~. **100 (Trying) response (UE#2 to P-CSCF#2) – see example in table A.4.3-23~~6~~**

UE#2 sends a 100 (Trying) response provisional response to P-CSCF#2.

### Table A.4.3-23~~6~~: 100 (Trying) response (UE#2 to P-CSCF#2)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

24~~7~~. **Reserve IP-CAN bearer for media**

The terminating UE#2 accepts the message session and. UE#2 reserves an IP-CAN bearer for the message session media component.

~~28. **TCP setup**~~

~~UE#2 establishes a TCP connection using the IP-CAN bearers established in step 27 to the host address and port as specified in the MSRP URL received in the SDP Offer from AS#2.~~

~~29. **MSRP VISIT request (UE#2 to AS#2) – see example in table A.4.3-29**~~

~~UE#2 sends a MSRP VISIT request to AS#2 using the established TCP connection.~~

### ~~Table A.4.3-29: MSRP VISIT request (UE#2 to AS#2)~~

```
~~MSRP VISIT~~
~~Boundary: 194sy2s~~
~~To-path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317121~~
~~From-path: msrp:// [5555::eee:fff:aaa:bbb]:3335/s417121~~
~~TR-ID: 2810~~
~~Message-ID: 2810~~
~~-------194sy2s$~~
```

~~**Boundary:** Boundary string used to terminate message~~

~~**To-path:** The sender's remote path~~

~~**From-path:** The sender's local URL~~

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

~~**Message-ID:** A unique message ID for MSRP message.~~

~~**Closing:** Same boundary string as well as Continuation-Flag~~

30. ~~**MSRP VISIT request (AS#2 to AS#1) – see example in table A.4.3-30**~~

~~AS#2 sends a MSRP VISIT request to AS#1 using the established TCP connection.~~

~~**Table A.4.3-30: MSRP VISIT request (AS#2 to AS#1)**~~

```
~~MSRP VISIT~~
~~Boundary: 948qa2q~~
~~To-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222371~~
~~From-path: msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317122~~
~~TR-ID: 1730~~
~~ Message-ID: 1730~~
~~-------948qa2q$~~
```

~~**Boundary:** Boundary string used to terminate message~~

~~**To-path:** The sender's remote path~~

~~**From-path:** The sender's local URL~~

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

~~**Message-ID:** A unique message ID for MSRP message.~~

~~**Closing:** Same boundary string as well as Continuation-Flag.~~

31. ~~**MSRP VISIT request (AS#1 to UE#1) – see example in table A.4.3-31**~~

~~AS#1 sends a MSRP VISIT request to UE#1 using the established TCP connection.~~

~~**Table A.4.3-31: MSRP VISIT request (AS#1 to UE#1)**~~

```
~~MSRP VISIT~~
~~Boundary: i3hd83h~~
~~To-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271~~
~~From-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222372~~
~~TR-ID: 1380~~
~~Message-ID: 1380~~
~~-------- i3hd83h$~~
```

~~**Boundary:** Boundary string used to terminate message~~

~~**To-path:** The sender's remote path~~

~~**From-path:** The sender's local URL~~

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

~~**Message-ID:** A unique message ID for MSRP message.~~

~~**Closing:** Same boundary string as well as Continuation-Flag~~

### ~~32. MSRP 200 (OK) response (UE#1 to AS#1) – see example in table A.4.3-32~~

~~UE#1 that acts as a MSRP host returns a MSRP 200 (OK) response to the MSRP VISIT request using the established TCP connection.~~

**~~Table A.4.3-32: MSRP 200 (OK) response (UE#1 to AS#1)~~**

```
~~MSRP 200 OK~~
~~Boundary: 3hdk39f~~
~~To-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271~~
~~From-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222372~~
~~TR-ID: 1380~~
~~-------3hdk39f$~~
```

~~**TR-ID:** The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

### ~~33. MSRP 200 (OK) response (AS#1 to AS#2) – see example in table A.4.3-33~~

~~AS#1 returns a MSRP 200 (OK) response the MSRP VISIT request to AS#2 using the established TCP connection.~~

**~~Table A.4.3-33: MSRP 200 (OK) response (AS#1 to AS#2)~~**

```
~~MSRP 200 OK~~
~~Boundary: 9sne4lk~~
~~To-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222371~~
~~From-path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317122~~
~~TR-ID: 1730~~
~~-------9sne4lk$~~
```

~~**TR-ID:** The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

### ~~34. MSRP 200 (OK) response (AS#2 to UE#2) – see example in table A.4.3-34~~

~~AS#2 returns a MSRP 200 (OK) response to the MSRP VISIT request to UE#2 using the established TCP connection.~~

**~~Table A.4.3-34: MSRP 200 (OK) response (AS#2 to UE#2)~~**

```
~~MSRP (…) 200 OK~~
~~Boundary: skjf93j~~
~~To:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317121~~
~~From:[5555::eee:fff:aaa:bbb]:3335/s417121~~
~~TR-ID: 2810~~
~~-------skjf93j$~~
```

~~**TR-ID:** The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

### ~~35~~25. 200 (OK) response (UE#2 to P-CSCF#2) – see example in table A.4.3-~~35~~25

After reserving an IP-CAN bearer for the message session media component~~the receipt of the MSRP 200 (OK) response to the MSRP VISIT request~~, the terminating UE#2 sends a 200 (OK) response for the INVITE request containing SDP that indicates that UE#2 has ~~successfully visited AS#2.~~ accepted the message session and listens on the MSRP TCP port returned in the path attribute in the answer for a TCP SETUP from AS#2..

### Table A.4.3-~~35~~25: 200 (OK) response (UE#2 to P-CSCF#2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>
Privacy: none
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From: <sip:user1_public1@home1.net>tag=7871654
To: <sip:user2_public1@home2.net>;tag=999456
Call-ID: 0s09glkj4903a2sdf33cb03a
Cseq: 210 INVITE
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933630298793363O IN IP6 5555::eee:fff:aaa:bbb~~5555::aaa:bbb:ccc:ddd~~
s=-
c=IN IP6 5555::eee:fff:aaa:bbb~~my.MSRP.dummy.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:text/plain text/html message/cpim
a=path:msrp://[5555::eee:fff:aaa:bbb]:~~3335~~3402/s417121;tcp
a=max-size:65536
```

**SDP** The SDP contains the set of offered content types supported by UE#2 and desired by the user at UE#2 for this session in the accept-types attribute and indicates the maximum size message that can be receieved by UE#2 in the max-size attribute.

### ~~36~~26. 200 (OK) response (P-CSCF#2 to S-CSCF#2) – see example in table A.4.3-~~36~~26

P-CSCF#2 forwards the 200 (OK) response to S-CSCF#2.

### Table A.4.3-~~36~~26: 200 (OK) response (P-CSCF#2 to S-CSCF#2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=423551024"
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~37~~27. 200 (OK) response (S-CSCF#2 to AS#2) – see example in table A.4.3-~~37~~27

S-CSCF#2 forwards the 200 (OK) response to AS#2.

**Table A.4.3-~~37~~27: 200 (OK) response (S-CSCF#2 to AS#2)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP as2.home2.net;branch=z9hG4bK348923.1
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=423551024"; orig-ioi=home1.net;
   term-ioi=home2.net
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~38~~28. ACK request (AS#2 to S-CSCF#2) – see example in table A.4.3-~~38~~28

AS#2 generates a new ACK request and sends it to S-CSCF#2.

**Table A.4.3-~~38~~28: ACK request (AS#2 to S-CSCF#2)**

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP as2.home2.net;branch=z9hG4bK348923.1
Max-Forwards: 70
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:user1_public1@home1.net>;tag=7871654
To: <sip:user2_public1@home2.net>;tag=2217770
Call-ID: 0s09glkj4903a2sdf33cb03a
Cseq: 210 ACK
Content-Length: 0
```

### ~~39~~29. ACK request (S-CSCF#2 to P-CSCF#2) – see example in table A.4.3-~~39~~29

S-CSCF#1 forwards the ACK request to P-CSCF#2.

**Table A.4.3-~~39~~29: ACK request (S-CSCF#2 to P-CSCF#2)**

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
Max-Forwards: 69
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### ~~40~~30. ACK request (P-CSCF#2 to UE#2) – see example in table A.4.3.~~40~~30

P-CSCF#2 forwards the ACK request to UE#2.

### Table A.4.3-~~40~~30: ACK request (P-CSCF#2 to UE#2)

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK361k21.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   as2.home2.net;branch=z9hG4bK348923.1
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Content-Length:
```

31. **TCP setup**

AS#2 establishes a TCP connection using the IP-CAN bearers established in step 24 to the host address and port as specified in the MSRP URL received in the SDP Answer from UE#2.

~~41~~32. **200 (OK) response (AS#2 to S-CSCF#2) – see example in table A.4.3-3~~41~~2**

AS#2 generates a 200 (OK) response to S-CSCF#2.

### Table A.4.3-3~~41~~2: 200 (OK) response (AS#2 to S-CSCF#2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK764z87.1, SIP/2.0/UDP
   icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Record-Route: <sip:scscf2.home2.net;lr>, <sip:scscf1.home1.net;lr>
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=323551024"
From: <sip:user1_public1@home1.net>tag=234567
To: <sip:user2_public1@home2.net>;tag=98989823
Call-ID: s09a233cbsdfglkj490303a0
CSeq: 278 INVITE
Contact: <sip:[9999::ccc:aaa:bbb:ddd]>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933640 2987933640 IN IP6 9999::ccc:aaa:bbb:ddd
s=-
c=IN IP6 9999::ccc:aaa:bbb:ddd~~as2.home2.net.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=~~-~~path:msrp://[9999::ccc:aaa:bbb:ddd]:~~3333~~3402/s317122;tcp
a=max-size:32768
```

**SDP** The SDP contains the set of answered content types supported by UE#2 in the accept-types attribute and indicates the maximum size message that can be receieved by UE#2 and allowed by the policy of network home2 in the max-size attribute.

3~~42~~3. **200 (OK) response (S-CSCF#2 to I-CSCF#2) – see example in table A.4.3-3~~42~~3**

S-CSCF#2 forwards the 200 (OK) response to I-CSCF#2.

### Table A.4.3-3~~42~~3: 200 (OK) response (S-CSCF#2 to I-CSCF#2)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
Privacy:
P-Charging-Vector: icid-value"AyretyU0dm+6O2IrT5tAFrbHLso=323551024"; orig-ioi=home1.net;
   term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[6666::b99:c88:d77:e66]; ccf=[6666::a55:b44:c33:d22];
   ecf=[6666::1ff:2ee:3dd:4ee]; ecf=[6666::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~43~~34. 200 (OK) response (I-CSCF#2 to S-CSCF#1) – see example in table A.4.3-~~43~~34

I-CSCF#2 forwards the 200 (OK) response to S-CSCF#1.

### Table A.4.3-~~43~~34: 200 (OK) response (I-CSCF#2 to S-CSCF#1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Record-Route:
P-Asserted-Identity:
Privacy: none
P-Charging-Vector:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~44~~35. 200 (OK) response (S-CSCF#1 to AS#1) – see example in table A.4.3-~~44~~35

S-CSCF#1 forwards the 200 (OK) response to AS#1.

### Table A.4.3-~~44~~35: 200 (OK) response (S-CSCF#1 to AS#1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP as1.home1.net;branch=z9hG4bK240f34.1
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector:
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
   ecf=[5555::1ff:2ee:3dd:4ee]; ecf=[5555::6aa:7bb:8cc:9dd]
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
Content-Type:
Content-Length:

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

### ~~45~~36. ACK request (AS#1 to S-CSCF#1) - see example in table A.4.3-~~45~~36

AS#1 generates an ACK request and sends it to S-CSCF#1.

### Table A.4.3-~~45~~36: ACK request (AS#1 to S-CSCF#1)

```
ACK sip:[9999::ccc:aaa:bbb:ddd] SIP/2.0
Via: SIP/2.0/UDP as1.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 70
Route: <sip:scscf1.home1.net;lr>, <sip:scscf2.home2.net;lr>
From: <sip:user1_public1@home1.net>; tag=234567
To: <sip:user2_public1@home2.net>;tag=98989823
Call-ID: s09a233cbsdfglkj490303a0
Cseq: 278 ACK
Content-Length: 0
```

### ~~46~~37. ACK request (S-CSCF#1 to S-CSCF#2) - see example in table A.4.3-~~46~~37

The S-CSCF#1 forwards the ACK request to S-CSCF#2.

### Table A.4.3-~~46~~37: ACK request (S-CSCF#1 to S-CSCF#2)

```
ACK sip:[9999::ccc:aaa:bbb:ddd] SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP as1.home1.net;branch=
   z9hG4bK240f34.1
Max-Forwards: 69
Route: <sip:scscf2.home2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### ~~47~~38. ACK request (S-CSCF#2 to AS#2) - see example in table A.4.3-~~47~~38

The S-CSCF#2 forwards the ACK request to the AS#2.

### Table A.4.3-~~47~~38: ACK request (S-CSCF#2 to AS#2)

```
ACK sip:[9999::ccc:aaa:bbb:ddd] SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
   as1.home1.net;branch=z9hG4bK240f34.1
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Content-Length:
```

**39. TCP setup**

AS#1 establishes a TCP connection to the host address and port as specified in the MSRP URL received in the SDP Answer from the AS#2.

**~~48~~40. 200 (OK) response (AS#1 to S-CSCF#1) – see example in table A.4.3-~~48~~40**

AS#1 generates a 200 (OK) response and sends it to S-CSCF#1~~.~~

### Table A.4.3-~~48~~40: 200 (OK) response (AS#1 to S-CSCF#1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
CSeq: 127 INVITE
Contact: <sip:[7777::eee:ddd:ccc:aaa]>
Allow:
Content-Type:
Content-Length:

v=0
o=- 2987933642 2987933642 IN IP6 7777::eee:ddd:ccc:aaa
s=-
c=IN IP6 7777::eee:ddd:ccc:aaa~~as1.home1.net.URL~~
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222372;tcp
a=max-size:32768
```

**SDP** The SDP contains the set of answered content types supported by UE#2 in the accept-types attribute and indicates the maximum size message that can be receieved by UE#2 and allowed by the policy of network home1 in the max-size attribute.

**~~49~~41. 200 (OK) response (S-CSCF#1 to P-CSCF#1) – see example in table A.4.3-~~49~~41**

S-CSCF#1 forwards the 200 (OK) response to P-CSCF#1.

### Table A.4.3-~~49~~41: 200 (OK) response (S-CSCF#1 to P-CSCF#1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
Privacy:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
Content-Type:
Content-Length:

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

**~~50~~42. 200 (OK) response (P-CSCF#1 to UE#1) – see example in table A.4.3-~~50~~42**

P-CSCF#1 forwards the 200 (OK) response to UE#1

### Table A.4.3-~~50~~42: 200 (OK) response (P-CSCF#1 to UE#1)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
CSeq:
Require:
Contact:
Allow:
Content-Type:
Content-Length:

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

**~~51~~43. ACK request (UE#1 to P-CSCF#1) – see example in table A.4.3-~~51~~43**

The UE responds to the 200 (OK) response with an ACK request sent to the P-CSCF#1.

**Table A.4.3-~~51~~43: ACK request (UE#1 to P-CSCF#1)**

```
ACK sip:[7777::eee:ddd:ccc:aaa] SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>;tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 ACK
Content-Length: 0
```

~~52~~44. **ACK request (P-CSCF#1 to S-CSCF#1) – see example in table A.4.3-~~52~~44**

The P-CSCF#1 forwards the ACK request to the S-CSCF#1.

**Table A.4.3-~~52~~44: ACK request (P-CSCF#1 to S-CSCF#1)**

```
ACK sip:[7777::eee:ddd:ccc:aaa] SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
P-Access-Network-Info:
Route: <sip:scscf1.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

~~53~~45. **ACK request (S-CSCF#1 to AS#1) - see example in table A.4.3-~~53~~45**

The S-CSCF#1 forwards the ACK request to AS#1.

**Table A.4.3-~~53~~45: ACK request (S-CSCF#1 to AS#1)**

```
ACK sip:[7777::eee:ddd:ccc:aaa] SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Content-Length:
```

46. **Reserve IP-CAN bearer for media**

UE#1 reserves an IP-CAN bearer for the message session media component.

47. **TCP setup**

Originating UE#1 establishes a TCP connection using the IP-CAN bearers established in step 46 to the host address and port as specified in the MSRP URL received in the SDP Answer from AS#1.

~~54~~48. **MSRP SEND (UE#1 to AS#1) – see example in table A.4.3-~~54~~48**

The originating UE sends the first message over the MSRP session with a MSRP SEND request using the established TCP connection.

### Table A.4.3-~~54~~48: MSRP SEND (UE#1 to AS#1)

```
MSRP 34kjf94 SEND
~~Boundary: 34kjf94~~
To-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222372;tcp
From-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
~~TR-ID: 8822~~
Message-ID: 8822
Byte-Range: 1-89/89
Content-Type: "text/plain"

I will never be a member of a club that accepts people like me as members – Groucho Marx.
-------34kjf94$
```

~~**Boundary:** Boundary string used to terminate message.~~

**To-path:** The sender's remote path.

**From-path:** The sender's local URL.

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

**Message-ID:** A unique message ID for MSRP message.

**Byte-Range:** The Byte Range for this message.

**Content-Type:** The format of the body of the request.

~~**Closing:** Same boundary string as well as Continuation-Flag.~~

~~55~~49. **MSRP SEND (AS#1 to AS#2) – see example in table A.4.3-~~55~~49**

AS#1 forwards the first MSRP SEND request to AS#2 over the MSRP session using the established TCP connection.

### Table A.4.3-~~55~~49: MSRP SEND (AS#1 to AS#2)

```
MSRP shfsoi3 SEND
~~Boundary: shfsoi3~~
To-path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317122;tcp
From-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222371;tcp
~~TR-ID: 2832~~
Message-ID: 2832
Byte-Range: 1-89/89
Content-Type: "text/plain"

I will never be a member of a club that accepts people like me as members – Groucho Marx.
-------shfsoi3$
```

~~**Boundary:** Boundary string used to terminate message.~~

**To-path:** The sender's remote path.

**From-path:** The sender's local URL.

~~**TR-ID:** A unique transaction ID for this MSRP transaction.~~

**Message-ID:** A unique message ID for MSRP message.

**Byte-Range:** The Byte Range for this message.

**Content-Type:** The format of the body of the request.

~~**Closing:** Same boundary string as well as Continuation-Flag.~~

50~~6~~. **MSRP SEND (AS#2 to UE#2) – see example in table A.4.3-~~56~~50**

AS#2 forwards the first MSRP SEND request to UE#2 over the MSRP session using the established TCP connection.

### Table A.4.3-~~56~~50: MSRP SEND (AS#2 to UE#2)

```
MSRP 2oid4sf SEND
~~Boundary: 2oid4sf~~
To-path:msrp://[5555::eee:fff:aaa:bbb]:3335/s417121;tcp
From-path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317121;tcp
~~TR-ID: 3311~~
Message-ID: 3311
Byte-Range: 1-89/89
Content-Type: "text/plain"

I will never be a member of a club that accepts people like me as members – Groucho Marx.
-------2oid4sf$
```

~~**Boundary:**~~ ~~Boundary string used to terminate message.~~

**To-path:** The sender's remote path.

**From-path:** The sender's local URL.

~~**TR-ID:**~~ ~~A unique transaction ID for this MSRP transaction.~~

**Message-ID:** A unique message ID for MSRP message.

**Byte-Range:** The Byte Range for this message.

**Content-Type:** The format of the body of the request.

~~**Closing:**~~ ~~Same boundary string as well as Continuation-Flag.~~

51~~7~~. **MSRP 200 (OK) response (UE#2 to AS#2) – see example in table A.4.3-~~57~~51**

The receiving UE#2 acknowledges the reception of the MSRP SEND request with a MSRP 200 (OK) response sent using the established TCP connection.

### Table A.4.3-51~~7~~: MSRP 200 (OK) response (UE#2 to AS#2)

```
MSRP 2oid4sf 200 OK
~~Boundary: 2j32ri3~~
To-path:msrp://[5555::eee:fff:aaa:bbb]:3335/s417121;tcp
From-path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317121;tcp
~~TR-ID: 3311~~
--------2oid4sf~~2j32ri3~~$
```

~~**TR-ID:**~~ ~~The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

52~~8~~. **MSRP 200 (OK) response (AS#2 to AS#1) – see example in table A.4.3-52~~8~~**

AS#2 acknowledges the reception of the MSRP SEND request with a MSRP 200 (OK) response to AS#1 using the established TCP connection.

### Table A.4.3-52~~8~~: MSRP 200 (OK) response (AS#2 to AS#1)

```
MSRP shfsoi3 200 OK
~~Boundary: wnhus9o~~
To-path:msrp://[9999::ccc:aaa:bbb:ddd]:3333/s317122;tcp
From-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222371;tcp
~~TR-ID: 2832~~
------- hfsoi3~~wnhus9o~~$
```

~~**TR-ID:**~~ ~~The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

~~59~~53. **MSRP 200 (OK) response (AS#1 to UE#1) – see example in table A.4.3-~~59~~53**

AS#1 acknowledges the reception of the MSRP SEND request with a MSRP 200 (OK) response to UE#1 sent using the established TCP connection.

**Table A.4.3-~~59~~53: MSRP 200 (OK) response (AS#1 to UE#1)**

```
MSRP 34kjf94 200 OK
~~Boundary: 3is09wh~~
To-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222372;tcp
To-path:msrp://[7777::eee:ddd:ccc:aaa]:3927/s222372;tcp
~~TR-ID: 8822~~
-------34kjf94~~3is09wh~~$
```

~~**TR-ID:** The transaction ID for this MSRP transaction, as received in the related MSRP request.~~

## A.4.4 Establishing a session for session-based messaging with preconditions

This signalling flow is not provided as it is the same as the session establishment flows with preconditions in 3GPP TS 24.228 [4] except that the SDP contents are for setting up MSRP sessions over TCP rather than RTP sessions over UDP.

# A.5 Flows demonstrating session-based messaging conferences

## A.5.1 User connecting into a messaging conference

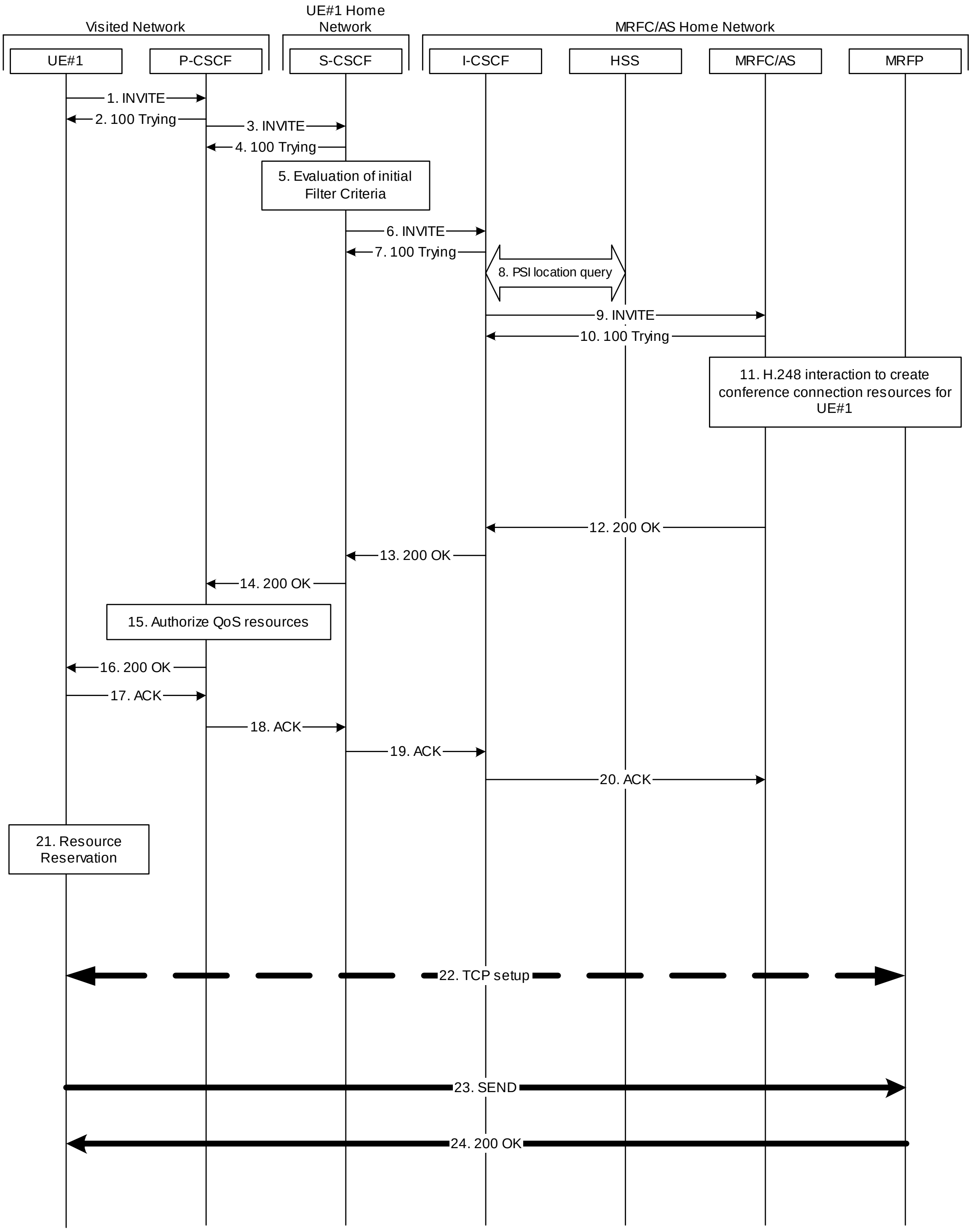


**Figure A.5.1-1: User connecting into a messaging conference - network MRFC/AS is not located in user's home network - conference URI resolved by the terminating home network**

Figure A.5.1-1 shows an user calling into a messaging conference by using a conference URI. The focus of that conference is at a MRFC/AS which are located in another network. The conference URI in this example cannot be resolved by the originating home network. In this example Service Based Local Policy and Media Authorisation is applied in the visited network.

The details of the flows are as follows:

### 1. INVITE request (UE to P-CSCF) - see example in table A.5.1-1

A UE wants to join a messaging conference. For this purpose the UE is aware of the related conference URI that was obtained by means outside the present document (e.g. via other protocols, such as http).

The originating UE creates a local MSRP URL, which can be used for communication for the messaging conference. It builds a SDP Offer containing the generated MSRP URL and assigns a local port number for the MSRP communication.

The UE sends the INVITE request to the P-CSCF.

**Table A.5.1-1: INVITE request (UE to P-CSCF)**

```
INVITE sip:conference1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Preferred-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:conference1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321;
   port-c=8642; port-s=7531
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
a=max-size:131072
```

**SDP** The SDP contains a set of content types supported by UE#1 and desired by the user at UE#1 for this session in the accept-types attribute and indicates the maximum size message that can be receieved by UE#1 in the max-size attribute.

### 2. 100 (Trying) response (P-CSCF to UE) - see example in table A.5.1-2

The P-CSCF responds to the INVITE request (1) with a 100 (Trying) response provisional response.

**Table A.5.1-2: 100 (Trying) response (P-CSCF to UE)**

```
SIP/2.0 100 (Trying) response
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### 3. INVITE request (P-CSCF to S-CSCF) - see example in table A.5.1-3

The P-CSCF forwards the INVITE request to the S-CSCF.

**Table A.5.1-3: INVITE request (P-CSCF to S-CSCF)**

```
INVITE sip:conference1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:orig@scscf1.home1.net;lr>
Record-Route: <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Allow:
Content-Type:
Content-Length: (…)

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

### 4. 100 (Trying) response (S-CSCF to P-CSCF) - see example in table A.5.1-4

The S-CSCF responds to the INVITE request (3) with a 100 (Trying) response provisional response.

**Table A.5.1-4: 100 (Trying) response (S-CSCF to P-CSCF)**

```
SIP/2.0 100 (Trying) response
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### 5. Evaluation of initial filter criteria

The S-CSCF validates the service profile of this subscriber and evaluates the initial filter criteria.

### 6. INVITE request (S-CSCF to I-CSCF) - see example in table A.5.1-6

The S-CSCF performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator does not desire to keep their internal configuration hidden, the S-CSCF forwards the INVITE request directly to the I-CSCF in the destination network.

As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

**Table A.5.1-6: INVITE request (S-CSCF to I-CSCF)**

```
INVITE sip:conference1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "John Doe" <sip:user1_public1@home1.net>, <tel:+358-50-4821437>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Require:
Contact:
Content-Type:
Content-Length: (...)

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

## 7. 100 (Trying) response (I-CSCF to S-CSCF) - see example in table A.5.1-7 (related to table A.5.1-6)

The I-CSCF responds to the INVITE request (6) with a 100 (Trying) response provisional response.

**Table A.5.1-7: 100 (Trying) response (MRFC/AS to S-CSCF)**

```
SIP/2.0 100 (Trying) response
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

## 8. Public service identity (PSI) location query

The I-CSCF sends a query to the HSS to find out the MRFC/AS at which the conference has been created. The HSS responds with the address of the MRFC/AS at which the conference is hosted. The HSS responds with the address of the MRFC/AS.

For detailed message flows see 3GPP TS 29.228 [11].

### 9. INVITE request (I-CSCF to MRFC/AS) - see example in table A.5.1-9

I-CSCF forwards the INVITE request to the MRFC/AS that was resolved during the PSI location query (8). The I-CSCF does not re-write the Request URI.

**Table A.5.1-9: INVITE request (I-CSCF to MRFC/AS)**

```
INVITE sip:conference1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy:
From:
To:
Call-ID:
Cseq:
Contact:
Content-Type:
Content-Length: (...)

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

### 10. 100 (Trying) response (MRFC/AS to I-CSCF) - see example in table A.5.1-10 (related to table A.5.1-9)

The MRFC/AS responds to the INVITE request (9) with a 100 (Trying) response provisional response.

**Table A.5.1-10: 100 (Trying) response (MRFC/AS to I-CSCF)**

```
SIP/2.0 100 (Trying) response
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### 11. H.248 interaction to create conference connection resources for UE#1

MRFC initiates a H.248 interaction to create an connection point for UE#1 in MRFP.

### 12. 200 (OK) response (MRFC/AS to I-CSCF) - see example in table A.5.1-12 (related to table A.5.1-9)

The MRFC/AS sends a 200 (OK) response for the INVITE request containing SDP that indicates that the MRFC/AS has accepted the message session and listens on the MSRP TCP port returned in the path attribute in the answer for a TCP SETUP from the originating UE. The MRFC/AS sends a 200 (OK) response final response to the INVITE request (9) to the I-CSCF.

**Table A.5.1-12: 200 (OK) response (MRFC/AS to I-CSCF)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
P-Asserted-Identity: "Conference Server" <sip:mrfc1.home2.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
   term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
   ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy: none
From:
To: <sip:conference1@home2.net>; tag=314159
Call-ID:
CSeq:
Contact: <sip:conference1@home2.net>;isfocus
Allow-Events: conference
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933623 2987933623 IN IP6 5555::aaa:bbb:ccc:ddd
s=-
c=IN IP6 5555::aaa:bbb:ccc:ddd
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[9999:: aaa:bbb:ccc:ddd]:3402/s317122;tcp
a=max-size:32768
```

**SDP** The SDP contains a set of offered content types supported by the MRFC/AS for this session in the accept-types attribute and indicates the maximum size message that can be receieved by the MRFC/AS in the max-size attribute.

### 13. 200 (OK) response (I-CSCF to S-CSCF) - see example in table A.5.1-13

The I-CSCF sends a 200 (OK) response final response along the signalling path back to the S-CSCF.

**Table A.5.1-13: 200 (OK) response (I-CSCF to S-CSCF)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
   term-ioi=home2.net
Privacy:
From:
To:
Call-ID:
CSeq:
Contact:
Allow-Events:
Allow:
Content-Type:
Content-Length:

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

### 14. 200 (OK) response (S-CSCF to P-CSCF) - see example in table A.5.1-14

The S-CSCF sends a 200 (OK) response final response along the signalling path back to the P-CSCF.

**Table A.5.1-14: 200 (OK) response (S-CSCF to P-CSCF)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route:
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
   ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
CSeq:
Contact:
Allow-Events:
Allow:
Content-Type:
Content-Length:

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

### 15. Authorize QoS Resources

The P-CSCF authorizes the resources necessary for this session.

### 16. 200 (OK) response (P-CSCF to UE) - see example in table A.5.1-16

The P-CSCF forwards the 200 (OK) response final response including the media authorisation token to the session originator.

**Table A.5.1-16: 200 (OK) response (P-CSCF to UE)**

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Record-Route: <sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>
P-Asserted-Identity:
Privacy:
P-Media-Authorization:
   0020000100100101706466322e76697369746564322e6e6574000c020139425633303732
From:
To:
Call-ID:
CSeq:
Contact:
Allow-Events:
Allow:
Content-Type:
Content-Length:
```

### 17. ACK request (UE to P-CSCF) - see example in table A.5.1-17

The UE starts the media flow for this session, and responds to the 200( OK) response (16) with an ACK request sent to the P-CSCF.

**Table A.5.1-17: ACK request (UE to P-CSCF)**

```
ACK sip:conference1@home2.net:2342 SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:scscf1.home1.net;lr>
From: <sip:user1_public1@home1.net>; tag=171828
To: <sip:conference1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 ACK
Content-Length: 0
```

### 18. ACK request (P-CSCF to S-CSCF) - see example in table A.5.1-18

The P-CSCF forwards the ACK request to the S-CSCF.

**Table A.5.1-18: ACK request (P-CSCF to S-CSCF)**

```
ACK sip:conference1@home2.net:2342 SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 69
Route: <sip:scscf1.home1.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### 19. ACK request (S-CSCF to I-CSCF) - see example in table A.5.1-19

The S-CSCF performs an analysis of the destination address, and determines the network operator to whom the destination subscriber belongs. Since the originating operator does not desire to keep their internal configuration hidden, the S-CSCF forwards the ACK request directly to the I-CSCF in the destination network.

As the S-CSCF does not know whether the I-CSCF at home2.net is a loose router or not, it does not introduce a Route header.

**Table A.5.1-19: ACK request (S-CSCF to I-CSCF)**

```
ACK sip:conference1@home2.net:2342 SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### 20. ACK request (I-CSCF to MRFC/AS) - see example in table A.5.1-20

I-CSCF forwards the ACK request to the MRFC/AS that was resolved during the PSI location query (8). The I-CSCF does not re-write the Request URI.

**Table A.5.1-20: ACK request (I-CSCF to MRFC/AS)**

```
ACK sip:conference1@home2.net:2342 SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
   scscf1.home1.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   pcscf1.visited1.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKnashds7
Max-Forwards: 67
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### 21. Reserve IP-CAN bearer for media

The UE reserves an IP-CAN bearer for the message session media component.

### 22. TCP setup

Originating UE establishes a TCP connection using the IP-CAN bearers established in step 21to the host address and port as specified in the MSRP URL received in the SDP Answer from MRFC/AS.

### 23. MSRP SEND request (UE to MRFP) – see example in table A.5.1-23

The originating UE sends the first me.ssage over the MSRP session with an MSRP SEND request using the established TCP connection.

**Table A.5.1-23: MSRP SEND request (UE to MRFP)**

```
MSRP a97ghjut SEND
To-path:msrp://[9999::ccc:aaa:bbb:ddd]:3402/s317122;tcp
From-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
Message-ID: 9972
Byte-Range: 1-77/77
Content-Type: "text/plain"
those are my principles. If you don't like them I have others – Groucho Marx.
-------a97ghjut$
```

**To-path:** The sender’s remote path

**From-path:** The sender’s local URL

**Message-ID:** A unique message ID for MSRP message.

**Byte-Range:** The Byte Range for this message.

**Content-Type:** The format of the body of the request.

### 24. MSRP 200 (OK) response (MRFP to UE) – see example in table A.5.1-24

The MRFP acknowledges the reception of the MSRP SEND request with an MSRP 200 (OK) response using the established TCP connection.

**Table A.5.1-24: MSRP 200 (OK) response (MRFP to UE)**

```
MSRP a97ghjut 200 OK
To-path:msrp://[9999::ccc:aaa:bbb:ddd]:3402/s317122;tcp
From-path:msrp://[5555::aaa:bbb:ccc:ddd]:3402/s111271;tcp
-------a97ghjut$
```

## A.5.2 MRFC/AS invites a user to a messaging conference

Figure A.5.2-1 shows an MRFC/AS inviting a user to a messaging conference. The invitation is sent as a result of user1@home1.net sending a REFER request to the MRFC/AS. The MRFC/AS is located in a different network than user's S-CSCF. The flows for inviting a user to a conference using REFER are shown in TS 24.147 [10]. In this example Service Based Local Policy and Media Authorisation is applied in the visted network.

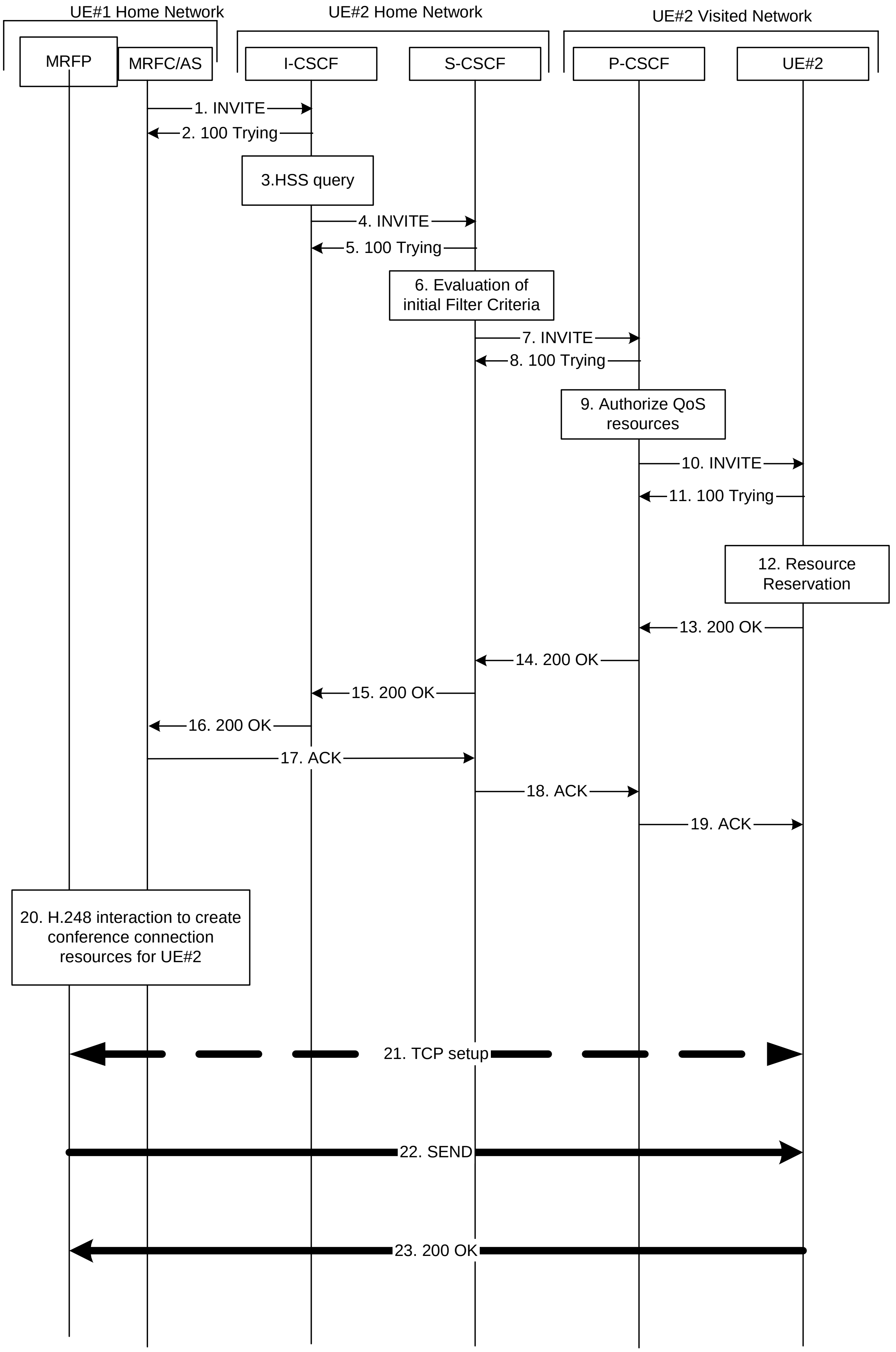

UE#1 Home Network
UE#2 Home Network
UE#2 Visited Network
MRFP
MRFC/AS
I-CSCF
S-CSCF
P-CSCF
UE#2
1. INVITE
2. 100 Trying
3.HSS query
4. INVITE
5. 100 Trying
6. Evaluation of initial Filter Criteria
7. INVITE
8. 100 Trying
9. Authorize QoS resources
10. INVITE
11. 100 Trying
12. Resource Reservation
13. 200 OK
14. 200 OK
15. 200 OK
16. 200 OK
17. ACK
18. ACK
19. ACK
20. H.248 interaction to create conference connection resources for UE#2
21. TCP setup
22. SEND
23. 200 OK

**Figure A.5.2-1: MRFC/AS inviting a user to a messaging conference - MRFC/AS routes directly to I-CSCF**

The details of the flows are as follows:

### 1. INVITE request (MRFC/AS to I-CSCF) - see example in table A.5.2-1

In this example, the MRFC/AS is capable of resolving the terminating users I-CSCF address for this request. As a result of a DNS query, it has received the address of the I-CSCF as the next hop.

The MRFC/AS invites a user to a messaging conference as it received a REFER request from another user.

The MRFC/AS creates a local MSRP URL, which can be used for communication for the messaging conference. It builds a SDP Offer containing the generated MSRP URL and assigns a local port number for the MSRP communication. In this example Service Based Local Policy and Media Authorisation is applied in the visited network.

**Table A.5.2-1: INVITE request (MRFC/AS to I-CSCF)**

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 70
P-Asserted-Identity: <sip:conference1@mrfc1.home1.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
Privacy: none
From: <sip:conference1@mrfc1.home1.net>;tag=171828
To: <sip:user2_public1@home2.net>
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 INVITE
Referred-By: <sip:user1_public1@home1.net>
Contact: <sip:conference1@mrfc1.home1.net>;isfocus
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Allow-Events: conference
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933615 2987933615 IN IP6 5555::abc:def:abc:def
s=-
c=IN IP6 5555::abc:def:abc:def
t=0 0
m=message 9999 msrp *
a=accept-types:message/cpim text/plain text/html
a=path:msrp://[5555::abc:def:abc:def]:3402/s111271;tcp
a=max-size:32768
```

**SDP** The SDP contains a set of content types supported by the MRFC/AS for this session in the accept-types attribute and indicates the maximum size message that can be receieved by the MRFC/AS in the max-size attribute.

### 2. 100 (Trying) response (I-CSCF to MRFC/AS) - see example in table A.5.2-2

The I-CSCF responds to the INVITE request with a 100 (Trying) provisional response.

**Table A.5.2-2: 100 (Trying) response (I-CSCF to MRFC/AS)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP conference1@mrfc1.home1.net;branch=z9hG4bK23273846
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### 3. Cx: User Location Query procedure

The I-CSCF sends a query to the HSS to find out the S-CSCF of the called user. The HSS responds with the address of the current S-CSCF for the terminating subscriber.

For detailed message flows see 3GPP TS 29.228[11].

4. **INVITE request (I-CSCF to S-CSCF) - see example in table A.5.2-4**

The INVITE request is forwarded to the S-CSCF.

**Table A.5.2-4: INVITE request (I-CSCF to S-CSCF)**

```
INVITE sip:user2_public1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 69
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
From:
To:
Call-ID:
Cseq:
Referred-By:
Contact:
Allow:
Allow-Events:
Content-Type:
Content-Length: (…)

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

5. **100 (Trying) response (S-CSCF to I-CSCF) - see example in table 6.2.2.2-5**

The S-CSCF responds to the INVITE request (3) with a 100 (Trying) provisional response.

**Table 6.2.2.2-5: 100 (Trying) response (S-CSCF to I-CSCF)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

6. **Evaluation of initial filter criteria**

The S-CSCF validates the service profile of this subscriber and evaluates the initial filter criteria.

7. **INVITE request (S-CSCF to P-CSCF) - see example in table A.5.2-7**

S-CSCF remembers (from registration procedures) the contact address of UE#2 and determines the P-CSCF assigned for UE#2 and routes message there.

### Table A.5.2-7: INVITE request (S-CSCF to P-CSCF)

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 68
Record-Route: <sip:scscf1.home1.net;lr>
P-Asserted-Identity:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
Cseq:
Referred-By:
Contact:
Allow:
Allow-Events:
P-Called-Party-ID: <sip:user2_public1@home2.net>
Content-Type:
Content-Length: (...)

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

### 8. 100 (Trying) response (P-CSCF to S-CSCF) - see example in table A.5.2-8

The P-CSCF responds to the INVITE request (6) with a 100 (Trying) provisional response.

### Table A.5.2-8: 100 (Trying) response (P-CSCF to S-CSCF)

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### 9. Authorize QoS resources

The P-CSCF authorizes the resources necessary for this session.

### 10. INVITE request (P-CSCF to UE#2) - see example in table A.5.2-10

P-CSCF forwards the request to UE#2 including the Media Authorisation token.

**Table A.5.2-10: INVITE request (P-CSCF to UE#2)**

```
INVITE sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK240f34.1 SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 67
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>
P-Asserted-Identity:
Privacy:
P-Media-Authorization: 0020000100100101706466312e686f6d65312e6e6574000c02013331533134363231
From:
To:
Call-ID:
Cseq:
Referred-By:
Contact:
Allow:
Allow-Events:
P-Called-Party-ID:
Content-Type:
Content-Length: (...)

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

### 11. 100 (Trying) response (UE#2 to P-CSCF) - see example in table A.5.2-11

UE#2 responds to the INVITE request (10) with a 100 (Trying) provisional response.

**Table A.5.2-11: 100 (Trying) response (UE#2 to P-CSCF)**

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK240f34.1 SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

### 12. Resource reservation

After determining the media streams, UE#2 initiates the reservation procedures for the resources needed for this session.

### 13. 200 (OK) response (UE#2 to P-CSCF) - see example in table A.5.2-13 (related to table A.5.2-10)

After reserving an IP-CAN bearer for the message session media componentthe receipt of the MSRP 200 (OK) response to the MSRP VISIT request, the terminating UE#2 sends a 200 (OK) response for the INVITE request containing SDP that indicates that UE#2 has successfully visited AS#2. accepted the message session and listens on the MSRP TCP port returned in the path attribute in the answer for a TCP SETUP from the MRFC/AS.

### Table A.5.2-13: 200 (OK) response (UE#2 to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Record-Route: <sip:pcscf2.visited2.net:5088;lr;comp=sigcomp>, <sip:scscf2.home2.net;lr>
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Privacy: none
From:
To: <sip:user2_public1@home2.net>; tag=314159
Call-ID:
CSeq: 127 INVITE
Contact: <sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp>
Content-Length:0
Allow: INVITE, ACK, CANCEL, BYE, PRACK, UPDATE, REFER, MESSAGE, SUBSCRIBE, NOTIFY
Content-Type: application/sdp
Content-Length: (…)

v=0
o=- 2987933623 2987933623 IN IP6 5555::eee:fff:aaa:bbb
s=-
c=IN IP6 5555::eee:fff:aaa:bbb
t=0 0
m=message 9999 msrp *
a=accept-types:text/plain text/html message/cpim
a=path:msrp://[5555::eee:fff:aaa:bbb]:3402/s417121;tcp
a=max-size:65536
```

**SDP** The SDP contains a set of offered content types supported by UE#2 and desired by the user at UE#2 for this session in the accept-types attribute and indicates the maximum size message that can be receieved by UE#2 in the max-size attribute.

## 14. 200 (OK) response (P-CSCF to S-CSCF) - see example in table A.5.2-14

The P-CSCF forwards the 200 (OK) response to the S-CSCF.

### Table A.5.2-14: 200 (OK) response (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Record-Route: <sip:pcscf2.visited2.net;lr>, <sip:scscf2.home2.net;lr>
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>
P-Access-Network-Info:
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### 15. 200 (OK) response (S-CSCF to I-CSCF) - see example in table A.5.2-15

The S-CSCF sends a 200 (OK) response final response along the signalling path back to I-CSCF.

### Table A.5.2-15: 200 (OK) response (S-CSCF to I-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP icscf2.home2.net;branch=z9hG4bK241d17.2, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Record-Route:
P-Asserted-Identity: "John Smith" <sip:user2_public1@home2.net>, <tel:+1-212-555-2222>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net;
   term-ioi=home2.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
   ecf=[5555::1ff:2ee:3dd:4cc]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### 16. 200 (OK) response (I-CSCF to MRFC/AS) - see example in table A.5.2-16

The I-CSCF forwards the 200 (OK) response final response to the session originator.

### Table 6.2.2.2-16: 200 (OK) response (I-CSCF to MRFC/AS)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP mrfc1.home1.net;branch=z9hG4bK23273846
Record-Route:
P-Asserted-Identity:
Privacy:
From:
To:
Call-ID:
CSeq:
Contact:
Allow:
Content-Type:
Content-Length:

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

### 17. ACK request (MRFC/AS to S-CSCF) - see example in table A.5.2-17

The MRFC/AS responds to the 200 (OK) response (16) with an ACK request sent to the S-CSCF.

**Table A.5.2-17: ACK request (MRFC/AS to S-CSCF)**

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 70
Route: <sip:scscf2.home2.net;lr>, <sip:pcscf2.visited2.net;lr>
From: <sip:conference1@mrfc1.home1.net>; tag=171828
To: <sip:user2_public1@home2.net>;tag=314159
Call-ID: cb03a0s09a2sdfglkj490333
Cseq: 127 ACK
Content-Length: 0
```

### 18. ACK request (S-CSCF to P-CSCF) - see example in table A.5.2-18

The S-CSCF forwards the ACK request to the P-CSCF.

**Table A.5.2-18: ACK request (S-CSCF to P-CSCF)**

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 69
Route: <sip:pcscf2.visited2.net;lr>
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### 19. ACK request (P-CSCF to UE#2) - see example in table A.5.2-19

The P-CSCF forwards the ACK request to the UE#2.

**Table A.5.2-19: ACK request (P-CSCF to UE#2)**

```
ACK sip:[5555::eee:fff:aaa:bbb]:8805;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf2.visited2.net:5088;comp=sigcomp;branch=z9hG4bK240f34.1, SIP/2.0/UDP
   scscf2.home2.net;branch=z9hG4bK332b23.1, SIP/2.0/UDP
   mrfc1.home1.net;branch=z9hG4bK23273846
Max-Forwards: 68
From:
To:
Call-ID:
Cseq:
Content-Length:
```

### 20. H.248 interaction to create conference connection resources for UE#2

MRFC initiates a H.248 interaction to create an connection point for UE#2 in MRFP.

### 21. TCP setup

MRFP establishes a TCP connection using the IP-CAN bearers established in step 12 to the host address and port as specified in the MSRP URL received in the SDP Answer UE#2.

### 22. MSRP SEND request (MRFP  to UE#2) – see example in table A.5.1-22

The MRFP sends the first me.ssage over the MSRP session with an MSRP SEND request using the established TCP connection.

### Table A.5.1-22: MSRP SEND request (MRFP to UE#2)

```
MSRP y56hkseg SEND
To-path:msrp://[5555::eee:fff:aaa:bbb]:3402/s417121;tcp
From-path:msrp://[5555::abc:def:abc:def]:3402/s111271;tcp
Message-ID: 10568
Byte-Range: 1-89/89
Content-Type: "text/plain"
I will never be a member of a club that accepts people like me as members – Groucho Marx.
-------y56hkseg$
```

**To-path:** The sender's remote path

**From-path:** The sender's local URL

**Message-ID:** A unique message ID for MSRP message.

**Byte-Range:** The Byte Range for this message.

**Content-Type:** The format of the body of the request.

23. **MSRP 200 (OK) response (UE#2 to MRFP) – see example in table A.5.1-23**

The terminating UE acknowledges the reception of the MSRP SEND request with an MSRP 200 (OK) response using the established TCP connection.

### Table A.5.1-23: MSRP 200 (OK) response (UE#2 to MRFP)

```
MSRP y56hkseg 200 OK
To-path:msrp://[5555::eee:fff:aaa:bbb]:3402/s417121;tcp
From-path:msrp://[5555::abc:def:abc:def]:3402/s111271;tcp
-------y56hkseg$
```

**3GPP TSG-CN1 Meeting #37** **Tdoc N1-050318**
**Sydney, Australia, 14-18 February 2005**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.247** | **CR** | **8** | ⌘**rev** | **1** | ⌘ | Current version: | **6.0.1** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Alignment between TS TS 23.228/ TS 22.340 and TS 24.247 for immediate messaging | | |
| ***Source:*** | ⌘ | LM Ericsson | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 02/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |
| | | *Use one of the following categories:*<br>**F** *(correction)*<br>**A** *(corresponds to a correction in an earlier release)*<br>**B** *(addition of feature),*<br>**C** *(functional modification of feature)*<br>**D** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use one of the following releases:*<br>*Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | In TS 23.228 it is stated IMS users shall be able to send a single immediate message to multiple recipients, as specified in 3GPP TS 22.340 [29a]. The following means are supported to achieve this:<br>- A PSI identifying a new group is created in the appropriate Application Server, and members are added to this group (e.g. by the user via the Ut interface or by the operator via O&M mechanisms). Immediate messages addressed to this PSI will be routed to the AS hosting the PSI, and this AS shall create and send immediate messages addressed to a group member of the group identified by the PSI. |
| ***Summary of change:*** | ⌘ | An AS in the form of  a list server is defined. The possibilty for the sending participant to use a PSI to address a group of participan is added. The relevant procedure section is added for the list server, |
| ***Consequences if not approved:*** | ⌘ | Misalignment with TS 22.340 and TS 23.228. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 5.2.2, 5.2.3 and 5.3 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs Affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |

|  |  |
|---|---|
| ***Other comments:*** ⌘ |  |

## How to create CRs using this form:

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

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

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

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

FIRST CHANGE

### 5.2.2 Application Server (AS)

As the functional split between the AS and the MRFC is out of scope of the present document, the procedures are described for a combined AS and MRFC. The AS and MRFC may either be collocated, or interoperate using a proprietary protocol and a proprietary functional split.

For the purpose of ~~immediate~~ page mode messaging, an Application Server may implement the role of a List Server as described in subclause 5.3.2. An Application Server may implement the role of a Participant as described in subclause 5.3.1.

### 5.2.3 Media Resource Function Controller (MRFC)

As the function split between the MRFC and the AS is out of scope of the present document, the procedures for the MRFC are described together with those for the AS in subclause 5.2.2.

LAST CHANGE

## 5.3 Role

### 5.3.1 Participant

#### 5.3.1.1 General

For the purpose of page-mode messaging a participant will send a page-mode message using a SIP MESSAGE request as defined in RFC 3428 [8] to another participant.

#### 5.3.1.2 Sending of an immediate message

When sending an page-mode message to another participant or to a list server, the participant shall construct and send a MESSAGE request in accordance with RFC 3428 [8] and subclause 5.1.2A.1 of 3GPP TS 24.229 [5].

The Request URI shall either be:

- the URI of the other participant; or
- a PSI identifying a group.

#### 5.3.1.3 Receiving an immediate message

Upon receipt of a MESSAGE request, the participant shall perform the procedures as described in RFC 3428 [8] and subclause 5.1.2A.2 of 3GPP TS 24.229 [5].

NOTE: A MESSAGE request can be used for applications other than immediate messaging (e.g. 3GPP TS 23.228 [6] subclause 5.4.9), and the handling of received MESSAGE requests for such applications is outside the scope of this specification.

## 5.3.2 List Server

### 5.3.2.1 List server originating case

In addition to the procedure specified in 5.3.2.2 the list server shall follow the procedures of 3GPP TS 24.229 [5] subclause 5.7.3 when acting as an originating UA.

The PSI is used to address a predefined list of URIs.

The list server shall send a MESSAGE request to each of the entries in the predefined UPI list. For each of MESSAGE requests the list server shall set:

a) the Request URI and the To header to the URI of one of the entries of the distribution list;

b) include the P-Charging-Vector header including:

1) the value of the icid parameter if available; and

2) the value of the orig-ioi parameter if available;

c) include the P-Charging-Function-Addresses header as received in the MESSAGE request or, if the P-Charging-Function-Addresses header was not received in the MESSAGE request, indicate the values applicable for the list server in the P-Charging-Function-Addresses header; and

d) include the P-Asserted Identity header and Privacy header with the values as received in the MESSAGE request;

The handling of the 200 (OK) response shall be in accordance with 3GPP TS 24.229 [5].

### 5.3.2.2 List server terminating case

Upon receipt of a MESSAGE request that includes a PSI in the request URI the list server shall:

1) check if the PSI is allocated to a predefined URI list and rejects the request in accordance with RFC 3261 [7] if it is not allocated. The following actions in this subclause shall only be performed if the distribution list URI is allocated;

2) verify the identity of the user as described in subclause 5.7.1.4 of 3GPP TS 24.229 [5] and authorize the request as described in subclause 5.7.1.5 of 3GPP TS 24.229 [5]. The following actions in this subclause shall only be performed if the request can be authorized;

3) create a 202 (Accepted) response. The response shall be in accordance with the procedures of 3GPP TS 24.229 [5] subclause 5.7.1.2 in relation to the contents of the P-Charging-Function-Addresses header and the P-Charging-Vector header; and :

a) include the P-Charging-Vector header including:

i) the value of the icid parameter as received in the MESSAGE request;

ii) the value of the orig-ioi parameter as received in the MESSAGE request; and

iii) the term-ioi parameter, indicating the network of the list server; and

b) include the P-Charging-Function-Addresses header as received in the MESSAGEl request or, if the P-Charging-Function-Addresses header was not received in the MESSAGE request, indicate the values applicable for the list server in the P-Charging-Function-Addresses header; and

4) send the 202 (Accepted) response.

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050321**

**was Tdoc N1-050062**

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **24.141 CR 034** ⌘**rev** **1** ⌘ Current version: **6.2.0** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | | |
|---|---|---|---|---|---|
| ***Title:*** | ⌘ | Resolution of references to 24.228 | | | |
| ***Source:*** | ⌘ | Lucent Technologies | | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** | ⌘ | 04/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** | ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | It has been agreed at CN1#36 and at CN#26 that a release 6 version of 24.228 will not be created. 3GPP TS 23.218 makes a number of references to 24.228, which by default are supposed to be to the release 6 version.<br>Depending on the nature of the reference, a number of resolutions are possible, ranging from deleting all the references, making the reference specific to release 5, or reproducing the referenced material in the referencing specification.<br>For 24.241 it is considered that the making of a reference specific to release 5 is the most appropriate. That is therefore the proposal in this CR.<br>There is also an editor's note that makes a reference to 24.228. This editor's note exists because the equivalent mapping to the Cx interface is not performed in 24.228 (it relates to a PSI in a SUBSCRIBE request). The proposal here is to resolve the editor's note. |
| ***Summary of change:*** | ⌘ | All references to 24.228 are made specific to release 5.<br>The editor's note in subclause A.3.3.2 is replaces by the appropriate Cx interface mapping. |
| ***Consequences if not approved:*** | ⌘ | Invalid references will exist in the specificiation. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2, A.3.3.2 |
| | | **Y** **N** |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ | |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

## 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.141: "Presence Service; Stage 1".

[3] 3GPP TS 23.002: "Network architecture".

[4] 3GPP TS 23.141: "Presence service; Architecture and functional description; Stage 2".

[5] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[7] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[8] 3GPP TS 24.228 Release 5: "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[9] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[10] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[11] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[12] IETF RFC 2664 (1999): "FYI on Questions and Answers - Answers to Commonly asked New Internet User Questions".

[13] IETF RFC 2246 (1999): "The TLS Protocol Version 1.0".

[14] IETF RFC 2387 (August 1998): "The MIME Multipart/Related Content-type".

[15] IETF RFC 2616 (June 1999): "Hypertext Transfer Protocol -- HTTP/1.1".

[15A] IETF RFC 2617 (June 1999): " HTTP Authentication: Basic and Digest Access Authentication".

[16] IETF RFC 2778 (2000): "A Model for Presence and Instant Messaging".

[17] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[18] IETF RFC 3263 (June 2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[19] IETF RFC 3265 (March 2002): "Session Initiation Protocol (SIP)-Specific Event Notification".

[20] IETF RFC 3310 (2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[21] IETF RFC 3863 (August 2004): "Presence Information Data Format (PIDF)".

[22] draft-ietf-simple-event-list-05 (October 2004): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[23] IETF RFC 3903 (October 2004): " Session Initiation Protocol (SIP) for Event State Publication".

[24] draft-ietf-simple-partial-notify-03 (October 2004): "Partial Notification of Presence Information".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[25] draft-ietf-simple-prescaps-ext-02 (October 2004): "User Agent Capability Extension to Presence Information Data Format (PIDF)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[26] draft-ietf-simple-rpid-04 (October 2004): "RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[27] IETF RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[28] IETF RFC 3857 (August 2004): "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)".

[29] IETF RFC 3858 (August 2004): "An Extensible Markup Language (XML) Based Format for Watcher Information".

[30] draft-ietf-simple-filter-format-03 (October 2004): "An Extensible Markup Language (XML) Based Format for Event Notification Filtering".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[31] draft-ietf-simple-event-filter-funct-03 (October 2004): "Functional Description of Event Notification Filtering".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[32] draft-ietf-simple-cipid-03 (July 2004): "CIPID: Contact Information in Presence Information Data Format".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[33] draft-ietf-simple-xcap-04 (October 2004): "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[34] draft-ietf-simple-xcap-pidf-manipulation-usage-02 (October 2004): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[35] draft-ietf-simple-presence-rules-01 (October 2004): "Presence Authorization Rules".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[36] draft-ietf-simple-xcap-list-usage-04 (October 2004): "An Extensible Markup Language (XML) Format for Representing Resource Lists".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[37] draft-ietf-geopriv-pidf-lo-03 (September 2004): "A Presence-based GEOPRIV Location Object Format".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[38] draft-ietf-simple-partial-pidf-format-02 (October 2004): "Presence Information Data Format (PIDF) Extension for Partial Presence".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[39] draft-ietf-simple-xcap-package-02 (July 2004): "An Extensible Markup Language (XML) Document Format for Indicating Changes in XML Configuration Access Protocol (XCAP) Resources".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[40] draft-ietf-sip-content-indirect-mech-05 (October 2004): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[41] draft-rosenberg-simple-common-policy-caps-01 (July 2004): "An Extensible Markup Language (XML) Representation for Expressing Policy Capabilities".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[42] draft-rosenberg-simple-pres-policy-caps-01 (July 2004): "An Extensible Markup Language (XML) Representation for Expressing Presence Policy Capabilities".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[43] draft-ietf-sipping-config-framework-05 (October 2004): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[44] draft-ietf-simple-presence-data-model-01 (October 2004): "A Data Model for Presence".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[45] draft-ietf-simple-partial-publish-01 (October 2004): "Partial Publication of Presence Information".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

PROPOSED CHANGE

### A.3.3.2 Watcher subscribing to a resource list, UE in visited network - successful subscription

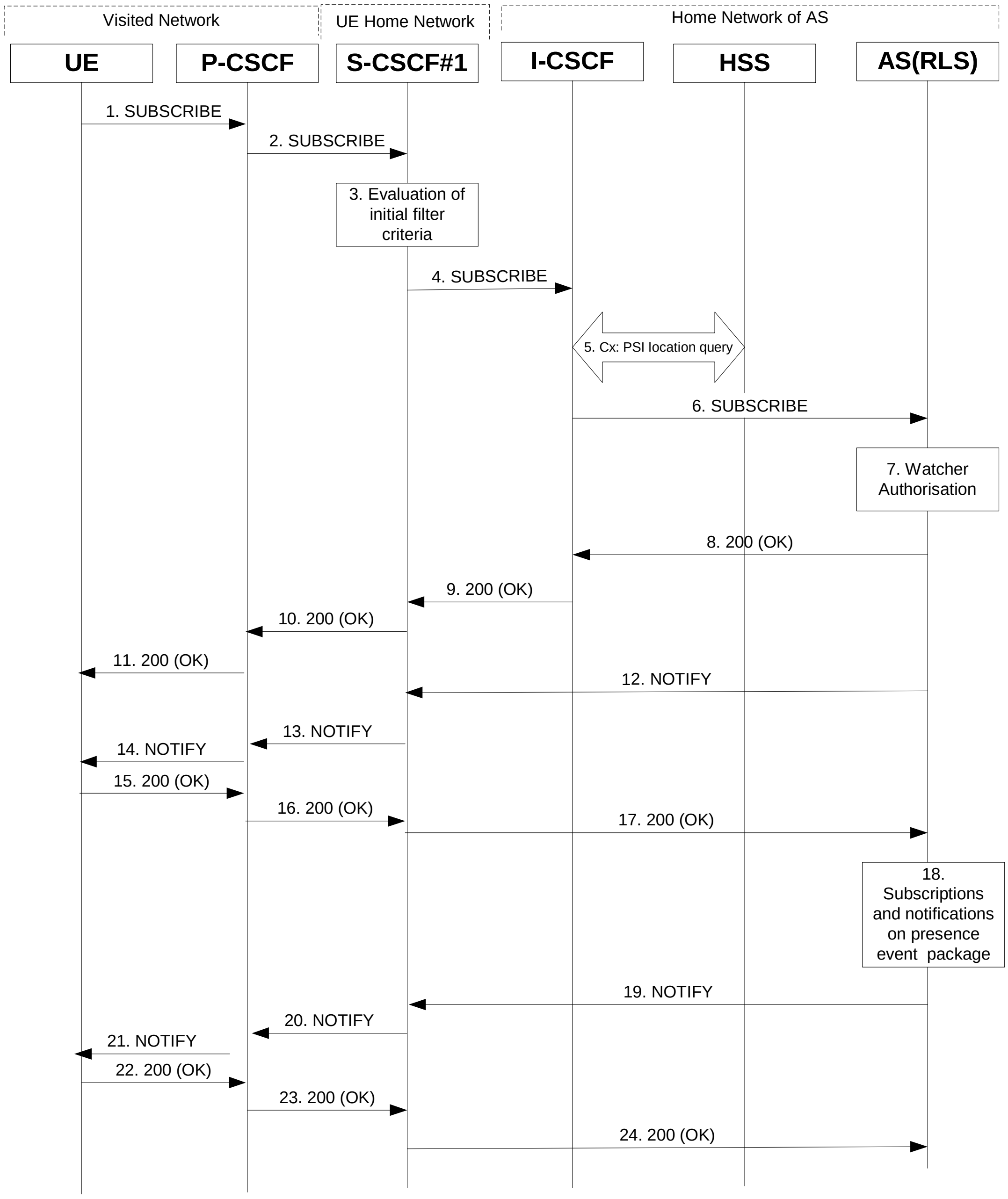


**Figure A.3.3.2-1 Watcher subscribing to resource list**

Figure A.3.3.2-1 shows a watcher subscribing to resource list event notification. The details of the signalling flows are as follows:

1. **SUBSCRIBE request (UE to P-CSCF) - see example in table A.3.3.2-1**

   A watcher agent in a UE wishes to watch a number of presentities, or certain presence information of these presentities. The list of presentities are identified by a SIP URI. In order to initiate a subscription to the RLS, the UE generates a SUBSCRIBE request indicating support for 'eventlist', together with an indication of the length of time this periodic subscription should last.

**Table A.3.3.2-1: SUBSCRIBE request (UE to P-CSCF)**

```
SUBSCRIBE sip:user2_list1@home2.net SIP/2.0
Via: SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKehuefdam
Max-Forwards: 70
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
Route: <sip:pcscf1.visited1.net:7531;lr;comp=sigcomp>, <sip:orig@scscf1.home1.net;lr>
P-Preferred-Identity: <sip:user1_public1@home1.net>
Privacy: none
From: <sip:user1_public1@home1.net>;tag=31415
To: <sip:user2_list1@home1.net>
Call-ID: b89rjhnedlrfjflslj40a222
CSeq: 123 SUBSCRIBE
Require: sec-agree
Proxy-Require: sec-agree
Security-Verify: ipsec-3gpp; q=0.1; alg=hmac-sha-1-96; spi-c=98765432; spi-s=87654321; port-
      c=8642; port-s=7531
Event: presence
Supported: eventlist
Expires: 7200
Accept: application/pidf+xml, application/rlmi+xml, multipart/related
Contact: <sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp>
Content-Length: 0
```

**Request-URI:** SIP URI of the resource list representing the collection of public user identities whose events the subscriber subscribes to.

**Event:** This field is populated with the value "presence" to specify the use of the presence package.

**Accept:** This field is populated with the value "application/pidf+xml", "application/rlmi+xml" and "multipart/related" indicating that the UE supports the eventlist extension additionally to PIDF.

**Supported:** This field is populated with the value 'eventlist' to specify the support for the eventlist extension.

**To:** Same as the Request-URI.

2. **SUBSCRIBE request (P-CSCF to S-CSCF) - see example in table A.3.3.2-2**

   The P-CSCF looks up the serving network information for the public user identity that was stored during the registration procedure. The SUBSCRIBE request is forwarded to S-CSCF#1. A Route header is inserted into SUBSCRIBE request. The information for the Route header is taken from the service route determined during registration.

### Table A.3.3.2-2: SUBSCRIBE request (P-CSCF to S-CSCF)

```
SUBSCRIBE sip:user2_list1@home2.net SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net;branch=z9hG4bK120f34.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKehuefdam
P-Access-Network-Info:
Route: <sip:orig@scscf1.home1.net;lr>
Max-Forwards: 69
P-Asserted-Identity: <sip:user1_public1@home1.net>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"
Privacy:
Record-Route: <sip:pcscf1.visited1.net;lr>
Route: <sip:scscf1.home1.net;lr>
From:
To:
Call-ID:
CSeq:
Event:
Supported:
Expires:
Accept:
Contact:
Content-Length:
```

3. **Evaluation of initial filter criteria**

   S-CSCF#1 validates the service profile of this subscriber and evaluates the initial filter criteria. For this example, assume no application server involvement.

4. **SUBSCRIBE request (S-CSCF to I-CSCF) - see example in table A.3.3.2-4**

   S-CSCF#1 performs an analysis of the destination address. As the destination address points to a resource that is in a different network as the S-CSCF, the S-CSCF sends the request to the I-CSCF of home2.net.

### Table A.3.3.2-4: SUBSCRIBE request (S-CSCF to I-CSCF)

```
SUBSCRIBE sip:user2_list1@home2.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
      pcscf1.visited1.net;branch=z9hG4bK120f34.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKehuefdam
Max-Forwards: 68
P-Asserted-Identity: <sip:user1_public1@home1.net>, <tel:+1-212-555-1111>
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net
P-Charging-Function-Addresses: ccf=[5555::b99:c88:d77:e66]; ccf=[5555::a55:b44:c33:d22];
      ecf=[5555::1ff:2ee:3dd:4ee]; ecf=[5555::6aa:7bb:8cc:9dd]
Privacy:
Record-Route: <orig@sip:scscf1.home1.net;lr>, <sip:pcscf1.visited1.net;lr>
From:
To:
Call-ID:
CSeq:
Event:
Supported:
Expires:
Accept:
Contact:
Content-Length:
```

5. **PSI location query**

The I-CSCF sends a query to the HSS to find the RLS where sip:user2_list1@home2.net is hosted. The HSS responds with the address of the RLS.

For detailed message flows see 3GPP TS 29.228 [10].

Table A.3.3.2-5a provides the parameters in the SIP SUBSCRIBE request (flow 4), which are sent to the HSS.

### Table A.3.3.2-5a Cx: User registration status query procedure (I-CSCF to HSS)

| Message source & destination | Cx: Information element name | Information source in SIP SUBSCRIBE | Description |
|---|---|---|---|
| I-CSCF to HSS | User Public Identity | Request-URI: | This information element indicates the PSI of the RLS |

Table A.3.3.2-5b provides the parameters sent from the HSS that need to be mapped to SIP SUBSCRIBE (flow 6) and sent to S-CSCF.

### Table A.3.3.2-5b Cx: User registration status query procedure (HSS to I-CSCF)

| Message source & destination | Cx: Information element name | Mapping to SIP header in SIP SUBSCRIBE | Description |
|---|---|---|---|
| HSS to I-CSCF | S-CSCF name | Route header field | This information indicates the address of the RLS |

~~Editor's Note: More detailed information is needed here, similar to the Cx interface information given in 3GPP TS 24.228 [8].~~

6. **SUBSCRIBE request (I-CSCF to RLS) - see example in table A.3.3.2-6**

The I-CSCF forwards the SUBSCRIBE request to the RLS.

### Table A.3.3.2-6: SUBSCRIBE request (I-CSCF to S-CSCF)

```
SUBSCRIBE sip:user2_list1@home2.net SIP/2.0
Via: SIP/2.0/UDP icscf2_s.home2.net;branch=z9hG4bK871y12.1, SIP/2.0/UDP
      scscf1.home1.net;branch=z9hG4bK344a65.1, SIP/2.0/UDP
      pcscf1.visited1.net;branch=z9hG4bK120f34.1, SIP/2.0/UDP
      [5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp;branch=z9hG4bKehuefdam
Max-Forwards: 67
P-Asserted-Identity:
P-Charging-Vector:
Privacy:
Record-Route:
Route: <sip:rls.home2.net;lr>
From:
To:
Call-ID:
CSeq:
Event:
Supported:
Expires:
Accept:
Contact:
Content-Length:
```

Remainder of subclause not shown

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050322**

**was Tdoc N1-050063**

*CR-Form-v7.1*

# CHANGE REQUEST

⌘ **24.147 CR 020** ⌘**rev** **1** ⌘ Current version: **6.1.0** ⌘

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | | |
|---|---|---|---|---|---|
| ***Title:*** | ⌘ | Resolution of references to 24.228 | | | |
| ***Source:*** | ⌘ | Lucent Technologies | | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** | ⌘ | 04/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** | ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | It has been agreed at CN1#36 and at CN#26 that a release 6 version of 24.228 will not be created. 3GPP TS 23.218 makes a number of references to 24.228, which by default are supposed to be to the release 6 version.<br>Depending on the nature of the reference, a number of resolutions are possible, ranging from deleting all the references, making the reference specific to release 5, or reproducing the referenced material in the referencing specification.<br>For 24.147 it is considered that the making of a reference specific to release 5 is the most appropriate. That is therefore the proposal in this CR. |
| ***Summary of change:*** | ⌘ | All references to 24.228 are made specific to release 5. |
| ***Consequences if not approved:*** | ⌘ | Invalid references will exist in the specificiation. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 2 |

| | | Y | N | | | |
|---|---|---|---|---|---|---|
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ | |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

## PROPOSED CHANGE

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.228: "Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".

[3] 3GPP TS 23.218: "IP Multimedia (IM) session handling; IM call model; Stage 2".

[4] 3GPP TS 24.228 Release 5: "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[5] 3GPP TS 24.229: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[7] IETF RFC 3261 (June 2002): "SIP: Session Initiation Protocol".

[8] draft-ietf-sipping-conferencing-framework-03 (October 2004): "A Framework for Conferencing with the Session Initiation Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[9] draft-ietf-sipping-cc-conferencing-05 (October 2004): "Session Initiation Protocol Call Control - Conferencing for User Agents".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[10] IETF RFC 3265 (June 2002): "Session Initiation Protocol (SIP) - Specific Event Notification".

[11] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[13] IETF RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[14] IETF RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[15] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[16] IETF RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[17] IETF RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) Refer Method".

[18] 3GPP TS 22.141: "Presence service; Stage 1".

[19] draft-ietf-sip-callee-caps-03 (December 2003): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[20] IETF RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[21] IETF RFC 2616 (June 1999): "Hypertext Transfer Protocol - HTTP/1.1".

[22] draft-ietf-simple-xcap-02 (February 2004): "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[23] draft-ietf-xcon-cpcp-01 (October 2004): "The Conference Policy Control Protocol (CPCP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[24] 3GPP TS 33.141: "Presence service; Security".

[25] 3GPP TS 24.109: "Bootstrapping interface (Ub) and Network application function interface (Ua); Protocol details".

[26] IETF RFC 2246 (January 1999): "The TLS Protocol Version 1.0".

[27] IETF RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[28] draft-ietf-xcon-bfcp-02 (October 2004): "The Binary Floor Control Protocol (BFCP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[29] draft-ietf-xcon-conference-policy-privileges-01: "Privileges for Manipulating a Conference Policy".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[30] draft-ietf-xcon-cpcp-xcap-03 (October 2004): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usages for Conference Policy Manipulation and Conference Policy Privileges Manipulation".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[31] draft-ietf-simple-xcap-package-02 (July 2004): " A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents ".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[32] draft-ietf-sipping-config-framework-05 (October 2004): "A Framework for Session Initiation Protocol User Agent Profile Delivery".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050323**

**was Tdoc N1-050064**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.247** | **CR** | **001** | ⌘**rev** | **1** | ⌘ | Current version: | **6.0.1** ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Resolution of references to 24.228 | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 04/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |
| | | *Use one of the following categories:*<br>***F*** *(correction)*<br>***A*** *(corresponds to a correction in an earlier release)*<br>***B*** *(addition of feature),*<br>***C*** *(functional modification of feature)*<br>***D*** *(editorial modification)*<br>Detailed explanations of the above categories can be found in 3GPP TR 21.900. | | *Use one of the following releases:*<br>*Ph2 (GSM Phase 2)*<br>*R96 (Release 1996)*<br>*R97 (Release 1997)*<br>*R98 (Release 1998)*<br>*R99 (Release 1999)*<br>*Rel-4 (Release 4)*<br>*Rel-5 (Release 5)*<br>*Rel-6 (Release 6)*<br>*Rel-7 (Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | It has been agreed at CN1#36 and at CN#26 that a release 6 version of 24.228 will not be created. 3GPP TS 23.218 makes a number of references to 24.228, which by default are supposed to be to the release 6 version.<br>Depending on the nature of the reference, a number of resolutions are possible, ranging from deleting all the references, making the reference specific to release 5, or reproducing the referenced material in the referencing specification.<br>For 24.247 it is considered that the making of a reference specific to release 5 is the most appropriate. That is therefore the proposal in this CR. |
| ***Summary of change:*** | ⌘ | All references to 24.228 are made specific to release 5. |
| ***Consequences if not approved:*** | ⌘ | Invalid references will exist in the specificiation. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 2 | | | | |
| | | **Y** | **N** | | | |
| ***Other specs affected:*** | ⌘ | | **X** | Other core specifications | ⌘ | |
| | | | **X** | Test specifications | | |
| | | | **X** | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

## 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "3G Vocabulary".

[2] 3GPP TS 22.228: " Service requirements for the Internet Protocol (IP) multimedia core network subsystem; Stage 1".

[3] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model; Stage 2".

[4] 3GPP TS 24.228 Release 5: "Signalling flows for the IP multimedia call control based on SIP and SDP; Stage 3".

[5] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP; Stage 3".

[6] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[7] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".

[8] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[9] draft-ietf-simple-message-sessions-06.txt (May 2004): "The Message Session Relay Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[10] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[11] 3GPP TS 22.340: "IP Multimedia System (IMS) messaging; Stage 1”.

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050324**

**was Tdoc N1-050065**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **786** | ⌘**rev** | **1** | ⌘ | Current version: | **6.5.1** | ⌘ |

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

***Proposed change affects:*** UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network ☒

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Cleanups resulting from CR changes for last version | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 26/01/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | Previous CRs have added the usage of the abbreviation QoS to the document, but have not included in the abbreviations clause.<br>CR747 has introduced a couple of instances of "non-session". As it is unclear what a non-session is, these wording have been modified (see. subclauses 4.5.2 and B.4.1).<br>CR738 added a new item to the initial list in subclauses 5.1.1.2, 5.1.1.4, and 5.1.1.6. All these lists are items all essentially of the same word structure, and the new insertions deviated from that.<br>CR734 amended text in the 2nd item (1) of 5.1.3.2.2. This amendment has left the "if required" divorced from the rest of the clause to which it relates, which is a dependency on what is needed from RFC 3261 and RFC 3262.<br>CR709 added a new item (10) (e) to subclause 5.4.1.2.2. To be consistent with the format of the other items in the list, an indefinited article is added to the new text.<br>CR 703 to CN1#36 made changes to the SDP procedures (clause 6), but a small part of this change used terminology that was appropriate for the SIP clauses rather than the SDP clauses, and inconsistent with the terminology used elsewhere in clause 6.<br>CR733 introduced some new abbreviations relating to compression, but they are not included in the abbreviations clause. As in both usages, these are already expanded, the simplest solution is to delete the abbrevation usage and that is what is proposed.<br>CR728 modified text concerning the grouping of media streams in annex B, and |

| | | |
|---|---|---|
| | | now in the specification we are inconsistent when referring to the concept, such that sometimes we just have "grouping" and other times "grouping of media streams" and other times other terminology. An attempt is made to correct this.<br>CR730 updated a number of references to published versions of RFCs, including the event state publication extension in RFC 3903. In doing this, and other previous CRs, the references for the Event header in table A.104A have become misaligned with those for the equivalent proxy table in A.260A. Current references in table A.104A are to RFC 3265, and while this is the same header, it is used in the new context of the PUBLISH request and the new procedures are entirely new. It is therefore considered appropriate to refer only to RFC 3903 here. |
| ***Summary of change:*** | ⌘ | In subclause 3.2, the abbreviation "QoS" is added.<br>In subclause 4.5.2, terminology surrounding non-session is modified.<br>In subclause 5.1.1.2, 5.1.1.4, 5.1.1.6, Via header items are amended to retain the existing word structure of other items, and some alignment has also been performed among the initial articles for other items in the list.<br>In subclause 5.1.3.2.2, the 2nd item (1) is restructured to put the "if required" with the text relating to RFC 3261 and RFC 3262.<br>In subclause 5.4.1.2.2, item (10) (e) an indefinite article is added.<br>In subclause 6.2 and 6.3, some instances of "200 (OK)" are changed to "SDP offer".<br>In subclause 8.1.1 and subclause 8.2.1, delete appearance of abbreviations "(SMS)" and "(DMS)", leaving only expansion. In subclause 6.2, and subclause<br>In table A.104A, references corrected to RFC 3903 [70]<br>B.2.2.5.1A, terminology corrected to "grouping of media streams".<br>In subclause B.4.1, terminology surrounding non-session is modified. |
| ***Consequences if not approved:*** | ⌘ | Consistent terminology and layout improve readability of specification. |

| | | | | | | |
|---|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | 3.2, 4.5.2, 5.1.1.2, 5.1.1.4, 5.1.1.6, 5.1.3.2.2, 5.4.1.2.2, 6.2, 6.3, 8.1.1, 8.2.1, A.21.14.10A, B.2.2.5.1A, B.4.1 | | | | |
| | | Y | N | | | |
| ***Other specs affected:*** | ⌘ | | X | Other core specifications | ⌘ | |
| | | | X | Test specifications | | |
| | | | X | O&M Specifications | | |
| ***Other comments:*** | ⌘ | | | | | |

## How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

## 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 |
| APN | Access Point Name |
| AUTN | Authentication TokeN |
| B2BUA | Back-to-Back User Agent |
| BGCF | Breakout Gateway Control Function |
| c | conditional |
| CCF | Charging Collection Function |
| CDR | Charging Data Record |
| CK | Ciphering Key |
| CN | Core Network |
| CSCF | Call Session Control Function |
| DHCP | Dynamic Host Configuration Protocol |
| DNS | Domain Name System |
| DTD | Document Type Definition |
| ECF | Event Charging Function |
| FQDN | Fully Qualified Domain Name |
| GCID | GPRS Charging Identifier |
| GGSN | Gateway GPRS Support Node |
| GPRS | General Packet Radio Service |
| HSS | Home Subscriber Server |
| i | irrelevant |
| I-CSCF | Interrogating CSCF |
| ICID | IM CN subsystem Charging Identifier |
| IK | Integrity Key |
| IM | IP Multimedia |
| IMS | IP Multimedia core network Subsystem |
| IMS-ALG | IMS Application Level Gateway |
| IMSI | International Mobile Subscriber Identity |
| IOI | Inter Operator Identifier |
| IP | Internet Protocol |
| IP-CAN | IP-Connectivity Access Network |
| IPsec | IP security |
| IPv4 | Internet Protocol version 4 |
| IPv6 | Internet Protocol version 6 |
| ISC | IP multimedia Subsystem Service Control |
| ISIM | IM Subscriber Identity Module |
| m | mandatory |
| MAC | Message Authentication Code |
| MCC | Mobile Country Code |
| MGCF | Media Gateway Control Function |
| MGW | Media Gateway |
| MNC | Mobile Network Code |
| MRFC | Multimedia Resource Function Controller |
| MRFP | Multimedia Resource Function Processor |
| PDP | Packet Data Protocol |
| PLMN | Public Land Mobile Network |
| PSTN | Public Switched Telephone Network |
| n/a | not applicable |
| NAI | Netework Access Identifier |

| | |
|---|---|
| o | optional |
| P-CSCF | Proxy CSCF |
| PDU | Protocol Data Unit |
| PSI | Public Service Identity |
| QoS | Quality of Service |
| RAND | RANDom challenge |
| RES | RESponse |
| RTCP | Real-time Transport Control Protocol |
| RTP | Real-time Transport Protocol |
| S-CSCF | Serving CSCF |
| SDP | Session Description Protocol |
| SIP | Session Initiation Protocol |
| SLF | Subscription Locator Function |
| SQN | SeQuence Number |
| UA | User Agent |
| UAC | User Agent Client |
| UAS | User Agent Server |
| UE | User Equipment |
| UICC | Universal Integrated Circuit Card |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| UDVM | Universal Decompressor Virtual Machine |
| USIM | Universal Subscriber Identity Module |
| x | prohibited |
| XMAC | expected MAC |
| XML | eXtensible Markup Language |

PROPOSED CHANGE

## 4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems. The ICID is used also for session unrelated messages (e.g. SUBSCRIBE request, NOTIFY request, MESSAGE request) for the correlation with CDRs generated among the IM CN subsystem entities.

The first IM CN subsystem entity involved in a ~~dialog (session) or standalone (non-session) method~~ SIP transaction will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. For a dialog relating to a session, this will be performed only on the INVITE request, for all other transactions, it will occur on each SIP request. See 3GPP TS 32.260 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for mobile-originated calls. The I-CSCF will generate an ICID for mobile-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header. The valid duration of the ICIDis specified in 3GPP TS 32.260 [17].

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

The ICID is also passed from the P-CSCF to the IP-CAN via PDF. The interface supporting this operation is outside the scope of this document.

PROPOSED CHANGE

### 5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

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

a) ~~the~~ an Authorization header, with the username field, set to the value of the private user identity;

b) ~~the~~ a From header set to the SIP URI that contains the public user identity to be registered;

c) ~~the~~ a To header set to the SIP URI that contains the public user identity to be registered;

d) ~~the~~ a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) ~~the~~ a Via header ~~containing~~ set to include the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) ~~the~~ an Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: 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 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

f) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

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 (Interval Too Brief) 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 (Interval Too Brief) response.

PROPOSED CHANGE

### 5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) an Authorization header, with the username field set to the value of the private user identity;

b) a From header set to the SIP URI that contains the public user identity to be registered;

c) a To header set to the SIP URI that contains the public user identity to be registered;

d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

e) a Via header ~~containing~~ set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: 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 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

j) the Supported header containing the option tag "path"; and

k) the P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the new expiration time of the registration for this public user identity found in the To header value;

b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

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 (Interval 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 (Interval Too Brief) response.

When the timer F expires at the UE, the UE shall:

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

    a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

    b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

    c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 4: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive initial registration attempts, the UE shall not automatically attempt any further initial registration for an implementation dependant time of at least 30 minutes.

PROPOSED CHANGE

### 5.1.1.6 User-initiated deregistration

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

The UE shall integrity protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

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

a) ~~the~~ an Authorization header, with the username field, set to the value of the private user identity;

b) ~~the~~ a From header set to the SIP URI that contains the public user identity to be deregistered;

c) ~~the~~ a To header set to the SIP URI that contains the public user identity to be deregistered;

d) ~~the~~ a Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;

e) a Via header ~~containing~~ set to include the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

f) ~~the~~ an Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

g) a Request-URI set to the SIP URI of the domain name of the home network; and

h) a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

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

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

PROPOSED CHANGE

#### 5.1.3.1.2.2 Preconditions not supported by remote end

This procedure is initiated upon the reception of a 420 (Bad Extension) response to an initial INVITE request, the response containing the "precondition" option-tag in the Unsupported header field value.

The UE may create a new INVITE request addressed to the same destination as initial INVITE. When creating the new INVITE request, the UE shall:

1) populate the From, To, Call-ID headers and the Request-URI as per the initial INVITE request;

2) include the "precondition" option-tag in the Supported header;

3) set each of the media streams in inactive mode in SDP as described in subclause 6.1 in this specification; and

4) forward the INVITE request as per regular procedures.

Upon receiving a provisional response or final response containing the remote SDP, the UE shall:

1) if required by the regular SIP procedures defined in RFC 3261 [26] and RFC 3262 [27], acknowledge~~, if required,~~ the SIP response~~ as per regular SIP procedures defined in RFC 3261 [26] and RFC 3262 [27]~~; and

2) initiate the regular resource reservation mechanism, as described in subclause 9.2.5.

When the above INVITE transaction is successfully completed, and the local resource reservation procedure is complete, the UE shall create and forward a re-INVITE request including:

1) the From, To, Call-ID headers as per a re-INVITE request; and

2) SDP in which the media streams previously set in inactive mode are set to active (sendrecv, sendonly or recvonly) mode, according to the procedures described in subclause 6.1 in this specification.

PROPOSED CHANGE

#### 5.4.1.2.2 Protected REGISTER

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

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

1) check if the user needs to be reauthenticated.

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

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

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

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

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

2) stop timer reg-await-auth;

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

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

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

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

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

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

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:

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

   b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria(the initial Filter Criteria for the Registered and common parts is stored and the unregisterd part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered);

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

6) bind to each non-barred registered public user identity all registered contact information including all header parameters contained in the Contact header and all associated URI parameters and store information for future use;

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

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

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

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

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

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

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

   a) the list of received Path headers;

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

c) a Service-Route header containing:

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

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

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

e) a Contact header listing all contact addresses for this public user identity.

NOTE 5: There might be other contact addresses available, that other UEs have registered for the same public user identity.

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

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

NOTE 6: If this registration is a reregistration, the Filter Criteria already exists in the local data.

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

PROPOSED CHANGE

## 6.2 Procedures at the P-CSCF

When the P-CSCF receives any SIP request containing an SDP offer, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy, or, based on configuration by the operator of the P-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The P-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specifed in RFC 3261 [26]. The P-CSCF shall order the SDP payload with the most preferred codec listed first. If the SDP offer is encrypted, the P-CSCF may reject the request.

When the P-CSCF receives a SIP response different from 200 (OK) response containing SDP offer, the P-CSCF shall not examine the media parameters in the received SDP offer, but the P-CSCF shall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy), the P-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP payload. If the SDP answer is encrypted, the P-CSCF may reject the succeeding request.

When the P-CSCF receives a 200 (OK) response containing SDP offer, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it shall immediately terminate the session as described in subclause 5.2.8.1.2. If the SDP offer is encrypted, the P-CSCF shall forward the ~~200 (OK)~~ SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.2.8.1.2.

When the P-CSCF receives an initial INVITE request for a terminating session setup or a 183 (Session Progress) response to an INVITE request for an originating session setup, the P-CSCF may modify the SDP according to RFC 3524 [54] to indicate to the UE that particular media stream(s) is grouped according to a local policy. The policy is used to determine whether the P-CSCF will request the UE to keep media stream(s) grouped in different IP-CAN bearers and identify the relation between different media streams and IP-CAN bearers (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

The P-CSCF shall apply and maintain the same policy within the SDP from the initial request or response containing SDP and throughout the complete SIP session. If a media stream is added and grouping ~~apply~~ of media streams to the session, the P-CSCF shall modify the SDP according to RFC 3524 [54] to indicate to the UE that the added media stream(s) will be grouped into either a new group or into one of the existing groups. The P-CSCF shall not indicate re-grouping of media stream(s) within the SDP.

The P-CSCF shall not apply RFC 3524 [54] to the SDP for additional media stream(s), if grouping of media stream(s) was not indicated in the initial INVITE request or 183 (Session Progress) response.

The P-CSCF may inspect, if present, the "b=RS" and "b=RR" lines in order to find out the bandwidth allocation requirements for RTCP.

PROPOSED CHANGE

## 6.3 Procedures at the S-CSCF

When the S-CSCF receives any SIP request containing an SDP offer, the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy and users subscription or, based on configuration by the operator of the S-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The S-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26]. If the SDP offer is encrypted, the S-CSCF may reject the request.

When the S-CSCF receives a SIP response different from 200 (OK) response containing SDP offer, the S-CSCF shall not examine the media parameters in the received SDP offer, but the S-CSCFshall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy), the S-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP payload. If the SDP answer is encrypted, the S-CSCF may reject the succeeding request.

When the S-CSCF receives a 200 (OK) response containing SDP offer, the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it shall immediately terminate the session as described in subclause 5.4.5.1.2. If the SDP offer is encrypted, the S-CSCF shall forward the ~~200 (OK)~~ SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.2.8.1.2.

PROPOSED CHANGE

### 8.1.1 SIP compression

The UE shall support SigComp as specified in RFC 3320 [32]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. When the UE will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

Editor’s note: The draft-ietf-rohc-sigcomp-sip-01 [79] can lead to the need for additional changes or clarifications.

The UE shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

The following apply when signalling compression is used:

- State Memory Size ~~(SMS)~~ greater than zero is needed to give room for the UDVM byte code and make dynamic compression possible. A State Memory Size of at least 4096 bytes shall be a minimum value; and
- A Decompression Memory Size ~~(DMS)~~ of at least 8192 bytes should be a minimum value.

PROPOSED CHANGE

### 8.2.1 SIP compression

The P-CSCF shall support SigComp as specified in RFC 3320 [32]. When using SigComp the P-CSCF shall send compressed SIP messages in accordance with RFC 3486 [55]. When the P-CSCF will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

The P-CSCF shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the P-CSCF shall use the dictionary to compress the first message.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

Editor’s note: The draft-ietf-rohc-sigcomp-sip-01 [79] can lead to the need for additional changes or clarifications.

The following apply when signalling compression is used:

- State Memory Size ~~(SMS)~~ greater than zero is needed to give room for the UDVM byte code and make dynamic compression possible. A State Memory Size of at least 4096 bytes shall be a minimum value; and
- A Decompression Memory Size ~~(DMS)~~ of at least 8192 bytes should be a minimum value.

PROPOSED CHANGE

### A.2.1.4.10A PUBLISH method

Editor's note: The base draft does not yet contain an analysis of header usage within this method, and therefore this clause will have to be reviewed and completed when such an analysis is available.

Prerequisite A.5/15A – PUBLISH request

**Table A.104A: Supported headers within the PUBLISH request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | Accept-Contact | [56B] 9.2 | c24 | c24 | [56B] 9.2 | n/a | n/a |
| 2 | Allow | [26] 20.5 | o | o | [26] 20.5 | m | m |
| 3 | Allow-Events | [26] 7.2.2 | c1 | c1 | [26] 7.2.2 | c2 | c2 |
| 4 | Authorization | [26] 20.7 | c3 | c3 | [26] 20.7 | c3 | c3 |
| 5 | Call-ID | [26] 20.8 | m | m | [26] 20.8 | m | m |
| 6 | Call-Info | [26] 20.9 | o | o | [26] 20.9 | o | o |
| 7 | Content-Disposition | [26] 20.11 | o | o | [26] 20.11 | m | m |
| 8 | Content-Encoding | [26] 20.12 | o | o | [26] 20.12 | m | m |
| 9 | Content-Language | [26] 20.13 | o | o | [26] 20.13 | m | m |
| 10 | Content-Length | [26] 20.14 | m | m | [26] 20.14 | m | m |
| 11 | Content-Type | [26] 20.15 | m | m | [26] 20.15 | m | m |
| 12 | Cseq | [26] 20.16 | m | m | [26] 20.16 | m | m |
| 13 | Date | [26] 20.17 | c4 | c4 | [26] 20.17 | m | m |
| 14 | Event | [70] 4, 6~~[28] 8.2.1~~ | m | m | [70] 4, 6~~[28] 8.2.1~~ | m | m |
| 15 | Expires | [26] 20.19, [70] 4, 5, 6 | o (note 1) | o (note 1) | [26] 20.19, [70] 4, 5, 6 | m | m |
| 16 | From | [26] 20.20 | m | m | [26] 20.20 | m | m |
| 17 | In-Reply-To | [26] 20.21 | o | o | [26] 20.21 | o | o |
| 18 | Max-Forwards | [26] 20.22 | m | m | [26] 20.22 | n/a | n/a |
| 19 | MIME-Version | [26] 20.24 | o | o | [26] 20.24 | m | m |
| 20 | Organization | [26] 20.25 | o | o | [26] 20.25 | o | o |
| 21 | P-Access-Network-Info | [52] 4.4 | c15 | c16 | [52] 4.4 | c15 | c17 |
| 22 | P-Asserted-Identity | [34] 9.1 | n/a | n/a | [34] 9.1 | c11 | c11 |
| 23 | P-Called-Party-ID | [52] 4.2 | x | x | [52] 4.2 | c13 | c13 |
| 24 | P-Charging-Function-Addresses | [52] 4.5 | c20 | c21 | [52] 4.5 | c20 | c21 |
| 25 | P-Charging-Vector | [52] 4.6 | c18 | c19 | [52] 4.6 | c18 | c19 |
| 26 | P-Preferred-Identity | [34] 9.2 | c11 | c7 | [34] 9.2 | n/a | n/a |
| 27 | P-Visited-Network-ID | [52] 4.3 | x (note 3) | x | [52] 4.3 | c14 | n/a |
| 28 | Priorità | [26] 20.26 | o | o | [26] 20.26 | o | o |
| 29 | Privacy | [33] 4.2 | c12 | c12 | [33] 4.2 | c12 | c12 |
| 30 | Proxy-Authorization | [26] 20.28 | c5 | c5 | [26] 20.28 | n/a | n/a |
| 31 | Proxy-Require | [26] 20.29 | o | n/a | [26] 20.29 | n/a | n/a |
| 32 | Reason | [34A] 2 | c8 | c8 | [34A] 2 | c8 | c8 |
| 33 | Reject-Contact | [56B] 9.2 | c22 | c22 | [56B] 9.2 | n/a | n/a |
| 33A | Referred-By | [59] 3 | c25 | c25 | [59] 3 | c26 | c26 |
| 34 | Request-Disposition | [56B] 9.1 | c22 | c22 | [56B] 9.1 | n/a | n/a |
| 35 | Reply-To | [26] 20.31 | o | o | [26] 20.31 | o | o |
| 36 | Require | [26] 20.32 | o | o | [26] 20.32 | m | m |
| 37 | Route | [26] 20.34 | m | m | [26] 20.34 | n/a | n/a |
| 38 | Security-Client | [48] 2.3.1 | c9 | c9 | [48] 2.3.1 | n/a | n/a |
| 39 | Security-Verify | [48] 2.3.1 | c10 | c10 | [48] 2.3.1 | n/a | n/a |
| 40 | SIP-If-Match | [70] 11.3.2 | o | o | [70] 11.3.2 | m | m |
| 41 | Subject | [26] 20.36 | o | o | [26] 20.36 | o | o |
| 42 | Supported | [26] 20.37, [26] 7.1 | o | o | [26] 20.37, [26] 7.1 | m | m |
| 43 | Timestamp | [26] 20.38 | c6 | c6 | [26] 20.38 | m | m |
| 44 | To | [26] 20.39 | m | m | [26] 20.39 | m | m |
| 45 | User-Agent | [26] 20.41 | o | o | [26] 20.41 | o | o |
| 46 | Via | [26] 20.42 | m | m | [26] 20.42 | m | m |

c1: IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c7: IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 2).
c10: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c11: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c12: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c13: IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c14: IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c15: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c16: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c17: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c18: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c19: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c20: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c22: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c24: IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c25: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c26: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.

NOTE 1: The strength of this requirement is RECOMMENDED rather than OPTIONAL.
NOTE 2: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented.
NOTE 3: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.

Prerequisite A.5/15A - - PUBLISH request

**Table A.104B: Supported message bodies within the PUBLISH request**

| Item | Header | Sending | | | Receiving | | |
|---|---|---|---|---|---|---|---|
| | | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
| 1 | | | | | | | |

Remainder of subclause not shown

PROPOSED CHANGE

### B.2.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping of media streams. The UE may freely group media streams to PDP context(s) in case no indication of grouping of media streams is received from the P-CSCF.

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, the UE shall:

- either use existing PDP context(s) where another media authorization token is already in use and no indication of ~~media~~ grouping of media streams is required; or
- establish separate PDP context(s) for the media; or

- use an existing PDP context where media authorization token is not in use and no indication of ~~media~~ grouping of media streams is required.

When a UE modifies a PDP context to indicate a new media authorization token:

- either as a result of establishment of an additional SIP session; or
- modification of media streams for an ongoing SIP session;

the UE shall include all media authorization tokens and all flow identifiers for all ongoing SIP sessions that use this particular PDP context.

If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

If either background or interactive QoS class is needed for the media, then the UE does not need to use the authorization token even if it receives one. In this case the UE may reuse an existing PDP context and it does not need to request PDP context modification unless it needs to modify the QoS.

If existing PDP context(s) where another media authorization token is already in use is re-used for the media, or separate PDP context(s) is established for the media, the UE shall proceed as follows:

- when a SIP session is terminated, the media authorization token is no longer valid and the UE shall not include it in future GPRS session management messages. The UE shall send a MODIFY PDP CONTEXT REQUEST message updating the binding information by deleting the media authorization token and the corresponding flow identifiers that are no longer valid. If a SIP session is terminated and no other SIP sessions are using the PDP context, the UE shall either update the binding information as described above or deactivate the PDP context;
- the UE shall transparently pass the media authorization token received from the P-CSCF in a response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message;
- to identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12];
- if the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE; and
- the UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

The encoding of the media authorization token and the flow identifiers within the Traffic Flow Template IE is described in 3GPP TS 24.008 [8].

PROPOSED CHANGE

## B.4.1 P-Charging-Vector header

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

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

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

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

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

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

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

The access network charging information is not included in the P-Charging-Vector for ~~non-session based~~ SIP signalling that is not associated with a session, and may not be available for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.

When the access network charging information is included in the P-Charging-Vector and necessary information is not available from the Go/Gq interface reference points then null or zero values are included.

**3GPP TSG-CN1 Meeting #37**
**Sydney, Australia, 14-18 February 2004**

**Tdoc N1-050326**

was **Tdoc N1-050235**

*CR-Form-v7.1*

# CHANGE REQUEST

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ⌘ | **24.229** | **CR** | **849** | ⌘ **rev** | **1** | ⌘ | Current version: | **6.5.1** | ⌘ |

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

| | | | | |
|---|---|---|---|---|
| ***Proposed change affects:*** | UICC apps⌘ □ | ME ☒ | Radio Access Network □ | Core Network □ |

| | | | | |
|---|---|---|---|---|
| ***Title:*** | ⌘ | Corrections to addition of session set-up not requiring preconditions and reliable transport of provisional responses | | |
| ***Source:*** | ⌘ | Lucent Technologies | | |
| ***Work item code:*** | ⌘ | IMS2 | ***Date:*** ⌘ | 06/02/2005 |
| ***Category:*** | ⌘ | **F** | ***Release:*** ⌘ | Rel-6 |

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

*Use one of the following releases:*

| | |
|---|---|
| *Ph2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |
| *Rel-7* | *(Release 7)* |

***Reason for change:*** ⌘ In CN1#35 a CR was introduced "Addition of session set-up not requiring preconditions and reliable transport of provisional responses" (N1-041632 → NP-040383). During the approval of that CR a number of textual improvements were identified which still need to be made:

1) Discussed in the meeting, two existing subclauses at header level 5 were subdivided, creating a number of subclauses at header level 6. Reasonably simple modifications can keep all this text at header level 5. Indeed, as currently structured, the heading of 5.1.4.1.2.3 is inconsistent with its heading one level up in 5.1.4.1.2, as the higher level heading indicates that all text in this subclause is with preconditions required by the terminating UE, whereas the lower one explicitly precludes it.
2) by using term "preconditions extension" or "preconditions mechanism" with no further explanation we have a discontinuity with the name of the extension in annex A, and no connection of that to mean the entirety of RFC 3312 – precondition is the name of the option-tag rather than the extension. However, rather than change all the usages, an explanatory phrase is inserted at the start of all the appropriate subclauses, and the usage made consistent throughout.
3) References to RFC 3312 are not made at the point where we introduce the extension, but rather inconsistently within the text on some but not all instances.

| | | |
|---|---|---|
| ***Summary of change:*** ⌘ | Structure of subclause 5.1.3.1 and 5.1.4.1 is revised to remove descent to header level 6.<br>Usage of term "precondition mechanism" is properly introduced, and then used consistently throughout.<br>Appropriate references to RFC 3312 are inserted.<br>The headlines were changed to be of consistent wording. | |
| ***Consequences if not approved:*** ⌘ | Inconsistent terminology and confusing structure within document. | |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** ⌘ | 5.1.3.1, 5.1.4.1, 6.1 | | | | |
| | **Y** | **N** | | | |
| ***Other specs affected:*** ⌘ | | **X** | Other core specifications | ⌘ | |
| | | **X** | Test specifications | | |
| | | **X** | O&M Specifications | | |
| ***Other comments:*** ⌘ | If the CR 729, "Incorporation of draft-ietf-sip-rfc3312-update-03.txt" is accepted, the RFC 3312 references in this CR will need some correction, as will that CR, due to interaction. | | | | |

**How to create CRs using this form:**

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

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

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

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

# PROPOSED CHANGE

## 5.1.3.1 Initial INVITE request

### 5.1.3.1.1 General

Subclause 5.1.3.1 describes the procedures when the initial INVITE is sent by the originating UE. The default behaviour using the "integration of resource management and SIP" extension (~~SIP ~~herafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30], and with the request for such a mechanism known as a precondition) is described in subclause 5.1.3.1.2~~.1~~. Session without preconditions may be initiated:

- when the remote node does not support the precondition mechanism, as discovered in subclause 5.1.3.1.3~~2.2~~; or
- when the specifc service does not require the precondition mechanism, as described in subclause 5.1.3.1.4~~3~~.

Editor's Note: The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

The UE may indicate that proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

NOTE 1: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and
2) send a BYE request to this dialog in order to terminate it.

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.

If the UE receives a 488 (Not Acceptable Here) response to an initial INVITE request, the UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 2: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements

### ~~5.1.3.1.2 "Integration of resource management" required by originating UE~~

### 5.1.3.1.2~~.1~~ "Integration of resource management and SIP" required by originating UE~~Preconditions required by originating UE~~

Upon generating an initial INVITE request using preconditions, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement ~~of ~~for the preconditions mechanism and specify it using the Require header mechanism.

When the initial INVITE has been created and forwarded the forthcoming procedures are identical to the procedures described in subclause 5.1.3.1.1.

If the UE receives a 420 (Bad Extension) response to an initial INVITE request with "precondition" option-tag in the Unsupported header field, the UE shall either:

a) abort the session attempt and shall not resend this INVITE request without "precondition" option-tag in the Require header, or

b) try to complete the session by relaxing the requirement on the usage of the ~~"integration of resource management in SIP" extension as described in RFC 3312 [30]~~ precondition mechanism and proceed with the procedures described in subclause 5.1.3.1.3 and subclause 6.1.

### 5.1.3.1.3~~2.2~~ "Integration of resource management and SIP" required by originating UE and ~~Preconditions~~ not supported by ~~remote end~~terminating UE

This procedure is initiated upon the reception of a 420 (Bad Extension) response to an initial INVITE request, the response containing the "precondition" option-tag in the Unsupported header field value.

The UE may create a new INVITE request addressed to the same destination as initial INVITE. When creating the new INVITE request, the UE shall:

1) populate the From, To, Call-ID headers and the Request-URI as per the initial INVITE request;

2) include the "precondition" option-tag in the Supported header;

3) set each of the media streams in inactive mode in SDP as described in subclause 6.1 in this specification in order to prevent the terminating end to send media whereas the resource reservation is not done at the originating side; and

4) forward the INVITE request as per regular procedures.

Upon receiving a provisional response or final response containing the remote SDP, the UE shall:

1) acknowledge, if required, the SIP response as per regular SIP procedures defined in RFC 3261 [26] and RFC 3262 [27]; and

2) initiate the regular resource reservation mechanism, as described in subclause 9.2.5.

When the above INVITE transaction is successfully completed, and the local resource reservation procedure is complete, the UE shall create and forward a re-INVITE request including:

1) the From, To, Call-ID headers as per a re-INVITE request; and

2) SDP in which the media streams previously set in inactive mode are set to active (sendrecv, sendonly or recvonly) mode, according to the procedures described in subclause 6.1 in this specification.

### 5.1.3.1.4~~3~~ "Integration of resource management and SIP" not required by originating UE

This procedure is initiated when the ~~SIP~~ precondition ~~procedure~~ mechanism is not required for a session by the origination UE.

Upon generating the initial INVITE the UE may indicate the support of ~~preconditions~~ the precondition mechanism by including the "precondition" option-tag in the Supported header.

When the initial INVITE has been created and forwarded the forthcoming procedures are identical to the procedures described in subclause 5.1.3.1.1.

PROPOSED CHANGE

## 5.1.4 Call initiation - mobile terminating case

### 5.1.4.1 Initial INVITE request

#### 5.1.4.1.1 General

The handling of incoming initial INVITE requests at the terminating UE is mainly dependant on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (herafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30], and with the request for such a mechanism known as a precondition)~~resource reservation~~; and
- the UEs configuration for the case when the specific service does not require ~~resource reservation~~the precondition mechanism.

Editor's Note: The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires integration of resource management ~~is required~~ either due to the requested service or due to local configuration.

If resource management is required at the terminating UE and:

a) the received INVITE request includes the "precondition" option-tag in the Require header, the terminating UE shall perform the actions as described in subclause 5.1.4.1.2~~.1~~;

b) the received INVITE request does not include the "precondition" option-tag in the Require header and the terminating UE, based on local configuration, requires the usage of ~~preconditions~~ the precondition mechanism in this case, the terminating UE shall perform the actions as described in subclause 5.1.4.1.3~~2.2~~; or

c) the received INVITE request does not include the "precondition" option-tag in the Require header and the terminating UE, based on local configuration, does not require the usage of ~~preconditions~~ the precondition mechanism in this case, the terminating UE shall perform the actions as described in subclause 5.1.4.1.4~~2.3~~.

If resource management is not required by the terminating UE and:

a) the received INVITE request includes the "precondition" option-tag in the Require header, the terminating UE shall perform the actions as described in subclause 5.1.4.1.2~~.1~~, i.e. the terminating UE shall use the precondition mechanism in order to fulfil the requirement of the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Require header, the terminating UE shall perform the actions as described in subclause 5.1.4.1.45~~3~~.

NOTE: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

Editor's Note: The above note needs further investigation.

#### ~~5.1.4.1.2 "Integration of resource management" required by terminating UE~~

#### 5.1.4.1.2~~.1~~ "Integration of resource management and SIP" required by terminating UE and ~~Preconditions~~ used by originating UE

Upon generating the first response to the initial INVITE request that indicated the "precondition" option-tag in the Require header, the UE shall indicate the requirement for reliable provisional responses and specify it using the Require header mechanism.The UE shall send the 200 (OK) response to the initial INVITE request only after the local resource reservation has been completed and the call is accepted by the termination user.

#### 5.1.4.1.3~~2.2~~ "Integration of resource management and SIP" required by terminating UE and ~~Preconditions~~ not used by originating UE ~~but preconditions required by terminating UE~~

Upon receiving an initial INVITE request without the "precondition" option-tag in the Require header, and the ~~preconditions extension~~ preconditions mechanism ~~as described in RFC 3312 [30]~~ is required by the terminating UE, the terminating UE shall generate a 421 (Extension Required) response indicating the required extension in the Require header field value.

#### 5.1.4.1.4~~2.3~~ "Integration of resource management and SIP" ~~Preconditions~~ not ~~used~~ required by ~~originating~~ terminating UE and ~~preconditions~~ not ~~required~~ used by ~~terminating~~ originating UE

Upon receiving an initial INVITE request without containing the "precondition" option-tag in the Require header, if the terminating UE is configured to not use the preconditions ~~extension~~ mechanism~~as described in RFC 3312 [30]~~, the UE shall:

1) send none or more provisional response(s) (eg. 183 Session Progress); and

2) send a 200 (OK) response, when the resources ~~have been reserved~~ are available and the call has been accepted by the terminating user.

#### ~~5.1.4.1.53 "Integration of resource management" not required by terminating UE~~

~~Upon receiving an initial INVITE request without containing the "precondition" option-tag Require headers, and "integration of resource management" is not required by the terminating UE, the terminating UE shall:~~

~~1) send none or more provisional response(s) (eg. 183 Session Progress); and~~

~~2) send 200 (OK) response, when the call is accepted by the terminating user.~~

PROPOSED CHANGE

## 6.1 Procedures at the UE

Usage of SDP by the UE:

1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP payload with the most preferred codec listed first.

3. If the SIP request includes a "precondition" option-tag in the Require header (indicating the requirement for "Integration of resource management and SIP" and hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30]), the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

   If the SIP request does not include the "precondition" option-tag in the Require header, the UE shall not indicate that it mandates local QoS. The UE may indicate its desire for optional local QoS, by including the following preconditions:

   a=des:qos optional local sendrecv

In the case described in subclause 5.1.3.1.3~~2.2~~ in the first SDP offer the UE sends, the UE shall set each media stream in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

NOTE 1: When setting the media streams in the inactive mode, the UE may include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

4. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, and the precondition mechanism is used as described in subclause 5.1.4.1.2~~.1~~, the first 183 (Session Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.

   In the case described in subclause 5.1.4.1.5~~3~~ no specific SDP procedures for integration of resource reservation have to be performed.

   In the case described in subclause 5.1.4.1.4~~2.3~~ in the first SDP answer the UE sends, the UE shall set each media streams in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

   If the UE is setting one or more media streams in active mode, it shall apply the procedures described in draft-ietf-mmusic-sdp-new [39] with respect to setting the direction of media streams.

5. When the UE sends a 183 (Session Progress) response with SDP payload including one or more "m=" media descriptions, if the preconditions ~~extension~~ mechanism ~~as described in RFC 3312 [30]~~ is supported by the calling UE, the called UE shall request confirmation for the result of the resource reservation at the originating end point.

6. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261[26].

7. 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 and the "AS" bandwidth modifier in the SDP.

   If the media line in the SDP indicates the usage of RTP/RTCP, in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP.

   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 [13].

NOTE 2: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer will typically get the value of zero.

8. The UE shall include the MIME subtype "telephone-event" in 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 [23].

9. The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

10. If an IP-CAN bearer is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].

11. If the UE builds SDP for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE may be attempting a session establishment through multiple networks with different policies and potentially may need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.