3GPP TSG-CN Meeting #26 **NP-040590**
8th – 10th December 2004. Athens, Greece.

Source: **TSG CN WG1**

Title: **CRs to Rel-6 WI "IMS2" for TS 24.229**

Agenda item: **9.1**

Document for: **APPROVAL**

This document contains **14 CRs on Rel-6 Work Item "IMS2"**, that have been agreed by TSG CN WG1 CN#36 meeting and forwarded to TSG CN Plenary meeting #26 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
N1-042085	Reference updates	24.229	730	2	F	6.4.0	IMS2	Rel-6
N1-042117	Clarifications to SigComp	24.229	733	3	F	6.4.0	IMS2	Rel-6
N1-042120	Correction to subclause 5.1.3 of TS 24.229	24.229	734	2	F	6.4.0	IMS2	Rel-6
N1-042084	Correction to subclause 5.1.4.1.2.3 of TS 24.229	24.229	735	1	F	6.4.0	IMS2	Rel-6
N1-041869	Tel-URI related reference updates	24.229	739		C	6.4.0	IMS2	Rel-6
N1-042086	Throttling	24.229	741	1	C	6.4.0	IMS2	Rel-6
N1-041881	Editorial correction resulting from CR665	24.229	742		D	6.4.0	IMS2	Rel-6
N1-041882	Unprotected REGISTER corrections	24.229	743		F	6.4.0	IMS2	Rel-6
N1-042087	Corrections to text on receiving SDP offer in 200 (OK) response	24.229	744	1	F	6.4.0	IMS2	Rel-6
N1-042088	Privacy corrections	24.229	745	1	F	6.4.0	IMS2	Rel-6
N1-042105	P-Charging-Vector syntax	24.229	747	2	F	6.4.0	IMS2	Rel-6
N1-042106	Unavailability of the access-network-charging-info when the session is established without SBLP	24.229	752	2	F	6.4.0	IMS2	Rel-6
N1-042089	SIP messages carrying the access-network-charging-info for sessions without preconditions	24.229	753	1	F	6.4.0	IMS2	Rel-6
N1-042090	Network-initiated deregistration for multiple UEs sharing the same user public identity and for the old contact information of a roaming UE registered in a new network	24.229	755	1	F	6.4.0	IMS2	Rel-6

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-041869

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **739** ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Tel-URI related reference updates
Source:	⌘	Nokia
Work item code:	⌘	IMS2
Date:	⌘	07/11/2004
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:	⌘	RFC 2916 is obsoleted by RFC 3761, and the internet draft http://www.ietf.org/internet-drafts/draft-ietf-iptel-rfc2806bis-09.txt was approved by the IESG.
Summary of change:	⌘	References to obsoleted RFCs replaced
Consequences if not approved:	⌘	Reference to obsoleted RFCs (RFC2806, RFC 2916) in TS.
Clauses affected:	⌘	2

	Y	N			
Other specs affected: ⌘	X		Other core specifications	⌘	22.228, 23.228
		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=======

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 2806 (April 2000): "URLs for Telephone Calls".~~

[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 2916 (September 2000): "E.164 number and DNS".~~

[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] draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)"

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

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

[58] draft-ietf-sip-session-timer-13 (January 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] draft-ietf-sip-referredby-05 (March 2004): "The SIP Referred-By Mechanism".

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

[60] draft-ietf-sip-replaces-05 (February 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

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

[61] draft-ietf-sip-join-03 (February 2004): "The Session Inititation Protocol (SIP) "Join" Header".

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

[62] 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.

[70] draft-ietf-sip-publish-02 (January 2004): "Session Initiation Protocol (SIP) Extension for Presence Publication".

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

[71] draft-niemi-sipping-event-throttle-00 (October 2003): "Session Initiation Protocol (SIP) Event Notification Throttles".

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

[72] draft-ietf-simple-winfo-package-05 (January 2003): "A Session Initiation Protocol (SIP) Event Template-Package for Watcher Information".

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

[74] draft-ietf-simple-presence-10 (January 2003): "A Presence Event Package for the Session Initiation Protocol (SIP)".

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

[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.

=======END OF CHANGE=======

3GPP TSG-CN1 Meeting #36 **Tdoc N1-041881**
Seoul, Korea, 15-19 November 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **742** ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Editorial correction resulting from CR665
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	06/11/2004
Category:	⌘	**D**
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:	⌘	During CN1#35, CR665 to 24.229 in N1-041372 → NP-040381 was accepted. The change was slightly out of alignment with the items in the previous bullet items in the same list, and this change corrects it.
Summary of change:	⌘	Minor editorial changes to subclause 5.1.1.3, item g, to adjust it to same format as previous items.
Consequences if not approved:	⌘	Specification text poorly structured

Clauses affected:	⌘	5.1.1.3

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

Other comments: ⌘

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

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

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

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

5.1.1.3 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 users 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 initiaial registratioin 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 ~~that contains~~ 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.

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-041882

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **743** ⌘ **rev** **-** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Unprotected REGISTER corrections
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	06/11/2004
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:	⌘	CR699r1 approved at CN1#35 (in N1-041629 → NP-040385) introduced the text "When the S-CSCF receives a new unprotected registration request for an already registered public user identity". It is the P-CSCF that recognises that any message is protected or unprotected, and the only way the S-CSCF has knowledge of this condition is by virtue of a signalling indication. A previous CR corrected other text in 24.229 in respect of this error, and this new occurrence also needs to be corrected. Additionally, there is no longer sufficient separation of the condition in this paragraph and that in the subsequent paragraph.
Summary of change:	⌘	Text "When the S-CSCF receives a new unprotected registration request for an already registered public user identity" amended to "Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no". Additional condition added to subsequent paragraph "which is not for an already registered public user identity linked to the same private user identity,"
Consequences if not approved:	⌘	Specification is imprecise, and inconsistent with terminology in the remainder of the document.

Clauses affected:	⌘	5.4.1.2.1			
		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.

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

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

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

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", 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 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

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

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

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042084

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **735** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction to subclause 5.1.4.1.2.3 of TS 24..229
Source:	⌘	LM Ericsson
Work item code:	⌘	IMS2
Date:	⌘	29/10/2004
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:	⌘	Alignment with CR 453. The present procedure is unnecessarily complex. The procedure also leads to more complex charging analysis, since the 200 (OK) either is sent too early or sent from the incorrect user.
Summary of change:	⌘	The proposal aligns the fall back case with the non precondition session set-up procedure. The 200 (OK) response is not sent until the resources has been reserved and the call has been accepted by the termination user. No additional INVITE needs to be sent.
Consequences if not approved:	⌘	1) Unnecessarily complex procedure. 2) Unnecessarily complex charging analysis.

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.

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

~~Editor's Note: It needs to be investigated whether the solution proposed in this subclause (for the case when an UE outside the IMS calls an IMS UE) is covered by the solution given in subclause 5.1.4.1.3. In that case the resource reservation would be initiated when the initial INVITE is received, and the 200 (OK) for the initial INVITE would then be sent after the related resources have been reserved and the called user has accepted the call.~~

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 ~~either~~ the preconditions extension as described in RFC 3312 [30] ~~or the reliable provisional responses extension defined in RFC 3262 [27]~~, the UE shall:

1)~~1)~~ ~~if the INVITE request includes the "100rel" option-tag in the Supported header field value, answer with~~ send none or more provisional response(s) (eg. 183 Session Progress); and~~a~~ ~~183 (Session Progress) response and include the "100rel" option-tag in the Require header field in the response; or~~

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

~~2) if the INVITE request does not include the "100rel" option-tag in the Supported header field value, providing that the user accepts the session establishment, answer with a 200 (OK) response; and~~

~~3) in any of the above cases, set each of the media streams in inactive mode in SDP as described in subclause 6.1 in this specification; and~~

~~4) initiate the regular resource reservation mechanisms, as described in subclause 9.2.5.~~

~~When the above INVITE transaction has successfully complete, and when the local resource reservation procedure has complete, the UE shall create and forward a re-INVITE request which shall include:~~

~~1) the From, To, Call-ID headers as per a re-INVITE request;~~

~~2) a Supported header containing the "preconditions" and "100rel" option-tags, in addition to other supported option-tags; and~~

~~3) SDP in which the media streams previously set in inactive mode are set to active mode, according to the procedures described in subclause 6.1 in this specification.~~

3GPP TSG-CN1 Meeting #36 **Tdoc N1-042085**
Seoul, Korea, 15-19 November 2004

was Tdoc N1-041825, Tdoc N1-042003

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **730** ⌘**rev** **2** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Reference updates
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	27/10/2004
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: ⌘ A number of IETF draft references created in the release 6 version of the specification have now been published or revised. It is appropriate to refer to the published version, or to the latest revised version as internet drafts become obsolete and disappear from availability. All revisions have been checked for technical impact.

Summary of change: ⌘
- draft-ietf-sip-callerprefs-10 is revised to RFC 3841 – no technical impact.
- draft-ietf-sip-session-timer-13 is revised to draft-ietf-sip-session-timer-15 – no technical impact, one reference made more specific to be consistent with rest of document.
- draft-ietf-sip-referredby-05 is revised to RFC 3892 – no technical impact.
- draft-ietf-sip-replaces-05 is revised to RFC 3891 – no technical impact.
- draft-ietf-sip-callee-caps-03 is revised to RFC 3840 – no technical impact. However one reference in 5.4.3.3 is to the wrong document, it should be to RFC 3841, and this has been corrected.
- draft-ietf-sip-publish-02 is published as RFC 3903 – no technical impact. Some subclause references are changed and status-code name is revised.
- draft-ietf-simple-winfo-package now published as RFC 3857 – no technical impact.
- draft-ietf-simple-presence now published as RFC 3856 – no technical impact.
- draft-ietf-sip-join-03 is published as RFC 3911 – no technical impact.

Consequences if not approved:	⌘	Obsolete references in release 6 version of specification.

Clauses affected:	⌘	2, 5.1.3.1.2.1, 5.2.7.3, 5.3.2.1, 5.4.3.3, 5.4.4.1, 5.6.2, 5.7.3, 5.7.4, A.2.1.4.1, A.2.1.4.10A, A.2.2.4.1, A.2.2.4.10A			
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.

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] RFC 2806 (April 2000): "URLs for Telephone Calls".

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

[24] RFC 2916 (September 2000): "E.164 number and DNS".

[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] ~~draft-ietf-sip-callerprefs-10~~ RFC 3841 (~~October 2003~~August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)"

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

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

[58] draft-ietf-sip-session-timer-15~~3~~ (~~January~~ 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] ~~draft-ietf-sip-referredby-05~~RFC 3892 (~~March~~ September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".

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

[60] ~~draft-ietf-sip-replaces-05~~RFC 3891 (~~February~~ September 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

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

[61] ~~draft-ietf-sip-join-03~~RFC 3911 (~~February~~ October 2004): "The Session Inititation Protocol (SIP) "Join" Header".

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

[62] ~~draft-ietf-sip-callee-caps-03~~RCF 3840 (~~December 2003~~August 2004): "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.~~

[70] ~~draft-ietf-sip-publish-04~~2RFC 3903 (~~January May~~ October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP) ~~Extension for Presence Publication~~".

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

[71] draft-niemi-sipping-event-throttle-00 (October 2003): "Session Initiation Protocol (SIP) Event Notification Throttles".

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

[72] ~~draft-ietf-simple-winfo-package-05~~RFC 3857 (~~January 2003~~August 2004): "A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)~~A Session Initiation Protocol (SIP) Event Template-Package for Watcher Information~~".

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

[74] ~~draft-ietf-simple-presence-10~~RFC 3856 (~~January 2003~~August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

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

[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.

PROPOSED CHANGE

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.

The UE may also indicate that the 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 ~~draft-ietf-sip-callerprefs-10~~RFC 3841 [56B].

NOTE 1: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE may 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.

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] and proceed with the procedures described in subclause 5.1.3.2 and subclause 6.1.

PROPOSED CHANGE

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer~~-12~~ [58] clause 8.

NOTE 1: 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 in order to make it work.

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

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

NOTE 2: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

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

The P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header in the first request or response originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF e.g., after the local resource reservation is complete. Typically, this first response is a 180 (Ringing) or 200 (OK) response if the remote UA supports the "integration of resource management in SIP" extension, or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

PROPOSED CHANGE

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-ID 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~~-12~~ [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, 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.

PROPOSED 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) 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) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

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

8) if necessary perform the caller preferences to callee capabilities matching according to ~~draft-ietf-sip-caller-preferences~~RFC 3841 [56B~~62~~];

9) 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;

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", forward the request to the contact with the highest qvalue parameter. In case no qvalue parameters were provided, the S-CSCF shall decide locally how to forward the request; 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 shall forward the request as directed by the Request Disposition header as described in ~~draft-ietf-sip-callerprefs-10~~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 INVITE;

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 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 3323 [33].

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, 9, 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) 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;

3) 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

4) in case the response is sent towards the terminating 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 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.

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 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, 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).

PROPOSED CHANGE

5.4.4.1 Initial INVITE

When the S-CSCF receives an INVITE request, either from the served user or destined to the served user, the S-CSCF may require the periodic refreshment of the session to avoid hung states in the S-CSCF. If the S-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer~~-12~~ [58] clause 8.

NOTE: 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.

PROPOSED CHANGE

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. While the next entity may be a MGCF acting as a UA, the BGCF shall not apply the procedures of RFC 3323 [33] relating to privacy. The BGCF shall store the values received in the P-Charging-Function-Addresses header. The BGCF shall 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.

NOTE 1: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

When the BGCF receives an INVITE request, if the BGCF inserts its own Record-Route header, the BGCF may require the periodic refreshment of the session to avoid hung states in the BGCF. If the BGCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer ~~-12~~ [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.

PROPOSED CHANGE

5.7.3 Application Server (AS) acting as originating UA

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions identified in this subclause.

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

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]. The AS may retrieve CCF and/or ECF addresses from HSS on Sh interface.

When an AS acting as an originating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header that is received in any 1xx or 2xx responses to the requests.

The AS may also indicate that the 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 ~~draft-ietf-sip-callerprefs-10~~RFC 3841 [56B].

When sending an initial request on behalf of a PSI that is hosted by the AS, the AS shall insert a Route header pointing to an S-CSCF of the home network of the PSI, if:

- the AS is not able to resolve the next hop address by itself; or
- the operator policy requires it.

NOTE 1: The address of the S-CSCF may be obtained by querying the HSS on the Sh interface or from static configuration.

When sending an initial request on behalf of a public user identity, the AS shall insert a Route header pointing to the S-CSCF where the public user identity on whose behalf the request is generated is registered or hosted (unregistered case).

NOTE 2: The address of the S-CSCF may be obtained either from a previous request terminated by the AS, by querying the HSS on the Sh interface or from static configuration.

For the use of the P-Asserted-Identity by the AS, at least two cases exist:

a) any initial request for a dialog or request for a standalone transaction is generated as if it was originated by the UE on whose behalf the request is generated. In this case the AS shall insert a P-Asserted-Identity representing a public user identity of that UE. The AS shall append the "orig" parameter to the URI of the S-CSCF; and

b) any initial request for a dialog or request for a standalone transaction is generated by an AS supporting a service identified by a PSI. In this case the AS shall insert a P-Asserted-Identity containing the PSI of the AS.

Editor's Note: It needs to be specified that the AS can only add the P-Asserted-Identity when the AS is within the trust domain.

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

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

NOTE 3: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the AS indication of privacy or by network subscription or network policy. Therefore the AS should include the value "Anonymous" whenever privacy is explicitly required.

Editor's note: Is there a need to specify any conditions for the AS choosing to indicate privacy that are generic to all originating AS, or all conditions service specific, and therefore out of the scope of 24.229.

PROPOSED CHANGE

5.7.4 Application Server (AS) acting as a SIP proxy

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

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

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

The AS shall not fork the request if the fork-directive in the Request-Disposition header is set to "no-fork" as described in ~~draft-ietf-sip-callerprefs-10~~RFC 3841 [56B].

An AS acting as a SIP proxy shall propagate any received IM CN subsystem XML message body in the forwarded message.

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] 11.1.1~~3~~	c20	c20	[70] 11.1.1~~3~~	c20	c20
15B	PUBLISH response	[70] 11.1.1~~3~~	c20	c20	[70] 11.1.1~~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] 6.1	c6	c6	[30] 6.2	c6	c6
23	UPDATE response	[30] 6.2	c6	c6	[30] 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.2.1.4.1 Status-codes

Table A.6: Supported status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	n/a	n/a	[26] 21.1.1	m	m
2	180 (Ringing)	[26] 21.1.2	c2	c2	[26] 21.1.2	c1	c1
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c2	c2	[26] 21.1.3	c1	c1
4	182 (Queued)	[26] 21.1.4	c2	c2	[26] 21.1.4	c1	c1
5	183 (Session Progress)	[26] 21.1.5	c1	c1	[26] 21.1.5	c1	c1
6	200 (OK)	[26] 21.2.1			[26] 21.2.1		
7	202 (Accepted)	[28] 8.3.1	c3	c3	[28] 8.3.1	c3	c3
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1		
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2		
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3		
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4		
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5		
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	m	m
14	401 (Unauthorized)	[26] 21.4.2			[26] 21.4.2		
15	402 (Payment Required)	[26] 21.4.3			[26] 21.4.3		
16	403 (Forbidden)	[26] 21.4.4			[26] 21.4.4		
17	404 (Not Found)	[26] 21.4.5			[26] 21.4.5		
18	405 (Method Not Allowed)	[26] 21.4.6			[26] 21.4.6		
19	406 (Not Acceptable)	[26] 21.4.7			[26] 21.4.7		
20	407 (Proxy Authentication Required)	[26] 21.4.8			[26] 21.4.8		
21	408 (Request Timeout)	[26] 21.4.9			[26] 21.4.9		
22	410 (Gone)	[26] 21.4.10			[26] 21.4.10		
22A	412 (Conditional Request Failed~~Precondition Failed~~)	[70] ~~7~~11.2.1	c20	c20	[70] ~~7~~11.2.1	c20	c20
23	413 (Request Entity Too Large)	[26] 21.4.11			[26] 21.4.11		
24	414 (Request-URI Too Large)	[26] 21.4.12			[26] 21.4.12		
25	415 (Unsupported Media Type)	[26] 21.4.13			[26] 21.4.13		
26	416 (Unsupported URI Scheme)	[26] 21.4.14			[26] 21.4.14		
27	420 (Bad Extension)	[26] 21.4.15			[26] 21.4.15		
28	421 (Extension Required)	[26] 21.4.16			[26] 21.4.16		
28A	422 (Session Interval Too Small)	[58] 6	c7	c7	[58] 6	c7	c7
29	423 (Interval Too Brief)	[26] 21.4.17	c4	c4	[26] 21.4.17	m	m
29A	429 (Provide Referrer Identity)	[59] 5	c8	c8	[59] 5	c9	c9
30	480 (Temporarily Unavailable)	[26] 21.4.18			[26] 21.4.18		
31	481 (Call/Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	m	m
32	482 (Loop Detected)	[26] 21.4.20			[26] 21.4.20		
33	483 (Too Many Hops)	[26] 21.4.21			[26] 21.4.21		
34	484 (Address Incomplete)	[26] 21.4.22			[26] 21.4.22		
35	485 (Ambiguous)	[26] 21.4.23			[26] 21.4.23		
36	486 (Busy Here)	[26] 21.4.24			[26] 21.4.24		
37	487 (Request Terminated)	[26] 21.4.25			[26] 21.4.25		
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	m	m
39	489 (Bad Event)	[28] 7.3.2	c3	c3	[28] 7.3.2	c3	c3
40	491 (Request Pending)	[26] 21.4.27			[26] 21.4.27		

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
41	493 (Undecipherable)	[26] 21.4.28			[26] 21.4.28		
41A	494 (Security Agreement Required)	[48] 2	c5	c5	[48] 2	c6	c6
42	500 (Internal Server Error)	[26] 21.5.1			[26] 21.5.1		
43	501 (Not Implemented)	[26] 21.5.2			[26] 21.5.2		
44	502 (Bad Gateway)	[26] 21.5.3			[26] 21.5.3		
45	503 (Service Unavailable)	[26] 21.5.4			[26] 21.5.4		
46	504 (Server Time-out)	[26] 21.5.5			[26] 21.5.5		
47	505 (Version not supported)	[26] 21.5.6			[26] 21.5.6		
48	513 (Message Too Large)	[26] 21.5.7			[26] 21.5.7		
49	580 (Precondition Failure)	[30] 8			[30] 8		
50	600 (Busy Everywhere)	[26] 21.6.1			[26] 21.6.1		
51	603 (Decline)	[26] 21.6.2	c10	c10	[26] 21.6.2	m	m
52	604 (Does Not Exist Anywhere)	[26] 21.6.3			[26] 21.6.3		
53	606 (Not Acceptable)	[26] 21.6.4			[26] 21.6.4		

c1: IF A.5/9 THEN m ELSE n/a - - INVITE response.
c2: IF A.5/9 THEN o ELSE n/a - - INVITE response.
c3: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c4: IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c5: IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.
c6: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c7: IF A.4/42 AND (A.5/9 OR A.5/23) THEN m ELSE n/a - - the SIP session timer AND (INVITE response OR UPDATE response).
c8: IF A.4/43 AND A.5/17 THEN o ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c9: IF A.4/43 AND A.5/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c10: IF A.4/44 THEN m ELSE o - - the Session Inititation Protocol (SIP) "Replaces" header.
c20: IF A.4/41 THEN m ELSE n/a

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	[28] 8.2.1	m	m	[28] 8.2.1	m	m
15	Expires	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	o (note 1)	o (note 1)	[26] 20.19, [70] ~~7.1.1~~ 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] ~~7~~11.3.2	o	o	[70] ~~7~~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							

Prerequisite A.5/15B - - PUBLISH response

Table A.104C: Supported headers within the PUBLISH response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 24.9	o	o	[26] 24.9	m	m
3	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
4	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
5	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
10	From	[26] 20.20	m	m	[26] 20.20	m	m
11	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
12	Organization	[26] 20.25	o	o	[26] 20.25	o	o
13	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
14	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
15	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
16	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
17	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
18	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
19	Require	[26] 20.32	m	m	[26] 20.32	m	m
20	Server	[26] 20.35	o	o	[26] 20.35	o	o
21	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
22	To	[26] 20.39	m	m	[26] 20.39	m	m
23	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
24	Via	[26] 20.42	m	m	[26] 20.42	m	m
25	Warning	[26] 20.43	o	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c4:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c5:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c6:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c7:	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.						
c8:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c10:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
NOTE:	For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/7 - - 200 (OK)

Table A.104D: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	Expires	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	m	m	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	m	m
4	SIP-Etag	[70] ~~7~~11.3.1	m	m	[70] ~~7~~11.3.1	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.104E: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11OR A.6/12 – 401 (Unauthorized)

Table A.104F: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.104G: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.104H: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.104I: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.104J: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
4	Allow	[26] 20.5	o	o	[26] 20.5	m	m
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.104K: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m
4	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/28 OR A.6/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.104L: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/29 - - 423 (Interval Too Brief)

Table A.104M: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Min-Expires	[26] 20.23, [70] ~~6~~5, 6	m	m	[26] 20.23, [70] ~~6~~5, 6	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.104N: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/39 - - 489 (Bad Event)

Table A.104O: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	m	m
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/15B - - PUBLISH response

Table A.104P: Supported message bodies within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

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] ~~3~~11.1.1	c20	c20	[70] 11.1.1~~3~~	c20	c20
15B	PUBLISH response	[70] 11.1.1~~3~~	c20	c20	[70] 11.1.1~~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] 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] 7	c4	c4	[30] 7	c4	c4
23	UPDATE response	[30] 7	c4	c4	[30] 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.2.2.4.1 Status-codes

Table A.164: Supported-status codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	c1	c1	[26] 21.1.1	c2	c2
2	180 (Ringing)	[26] 21.1.2	c3	c3	[26] 21.1.2	c3	c3
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c3	c3	[26] 21.1.3	c3	c3
4	182 (Queued)	[26] 21.1.4	c3	c3	[26] 21.1.4	c3	c3
5	183 (Session Progress)	[26] 21.1.5	c3	c3	[26] 21.1.5	c3	c3
6	200 (OK)	[26] 21.2.1			[26] 21.2.1		
7	202 (Accepted)	[28] 8.3.1	c4	c4	[28] 8.3.1	c4	c4
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1		
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2		
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3		
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4		
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5		
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	i	i
14	401 (Unauthorized)	[26] 21.4.2			[26] 21.4.2		
15	402 (Payment Required)	[26] 21.4.3			[26] 21.4.3		
16	403 (Forbidden)	[26] 21.4.4			[26] 21.4.4		
17	404 (Not Found)	[26] 21.4.5			[26] 21.4.5		
18	405 (Method Not Allowed)	[26] 21.4.6			[26] 21.4.6		
19	406 (Not Acceptable)	[26] 21.4.7			[26] 21.4.7		
20	407 (Proxy Authentication Required)	[26] 21.4.8			[26] 21.4.8		
21	408 (Request Timeout)	[26] 21.4.9			[26] 21.4.9		
22	410 (Gone)	[26] 21.4.10			[26] 21.4.10		
22A	412 (Conditional Request Failed~~Precondition Failed~~)	[70] ~~7~~11.2.1	c20	c20	[70] ~~7~~11.2.1	c20	c20
23	413 (Request Entity Too Large)	[26] 21.4.11			[26] 21.4.11		
24	414 (Request-URI Too Large)	[26] 21.4.12			[26] 21.4.12		
25	415 (Unsupported Media Type)	[26] 21.4.13			[26] 21.4.13		
26	416 (Unsupported URI Scheme)	[26] 21.4.14			[26] 21.4.14		
27	420 (Bad Extension)	[26] 21.4.15			[26] 21.4.15		

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
28	421 (Extension Required)	[26] 21.4.16			[26] 21.4.16		
28A	422 (Session Interval Too Small)	[58] 6	c8	c8	[58] 6	c8	c8
29	423 (Interval Too Brief)	[26] 21.4.17	c5	c5	[26] 21.4.17	c6	c6
29A	429 (Provide Referrer Identity)	[59] 5	c9	c9	[59] 5	c9	c9
30	480 (Temporarily not available)	[26] 21.4.18			[26] 21.4.18		
31	481 (Call /Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	i	i
32	482 (Loop Detected)	[26] 21.4.20			[26] 21.4.20		
33	483 (Too Many Hops)	[26] 21.4.21			[26] 21.4.21		
34	484 (Address Incomplete)	[26] 21.4.22			[26] 21.4.22		
35	485 (Ambiguous)	[26] 21.4.23			[26] 21.4.23		
36	486 (Busy Here)	[26] 21.4.24			[26] 21.4.24		
37	487 (Request Terminated)	[26] 21.4.25			[26] 21.4.25		
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	i	i
39	489 (Bad Event)	[28] 7.3.2	c4	c4	[28] 7.3.2	c4	c4
40	491 (Request Pending)	[26] 21.4.27			[26] 21.4.27		
41	493 (Undecipherable)	[26] 21.4.28			[26] 21.4.28		
41A	494 (Security Agreement Required)	[48] 2	c7	c7	[48] 2	n/a	n/a
42	500 (Internal Server Error)	[26] 21.5.1			[26] 21.5.1		
43	501 (Not Implemented)	[26] 21.5.2			[26] 21.5.2		
44	502 (Bad Gateway)	[26] 21.5.3			[26] 21.5.3		
45	503 (Service Unavailable)	[26] 21.5.4			[26] 21.5.4		
46	504 (Server Time-out)	[26] 21.5.5			[26] 21.5.5		
47	505 (Version not supported)	[26] 21.5.6			[26] 21.5.6		
48	513 (Message Too Large)	[26] 21.5.7			[26] 21.5.7		
49	580 (Precondition Failure)	[30] 8			[30] 8		
50	600 (Busy Everywhere)	[26] 21.6.1			[26] 21.6.1		
51	603 (Decline)	[26] 21.6.2	m	m	[26] 21.6.2	i	i
52	604 (Does Not Exist Anywhere)	[26] 21.6.3			[26] 21.6.3		
53	606 (Not Acceptable)	[26] 21.6.4			[26] 21.6.4		

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c1:	IF A.162/15 THEN m ELSE n/a - - stateful proxy.						
c2:	IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						
c3:	IF A.163/9 THEN m ELSE n/a - - INVITE response.						
c4:	IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.						
c5:	IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.						
c6:	IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response.						
c7:	IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						
c8:	IF A.162/52 THEN m ELSE n/a - - the SIP session timer.						
c9:	IF A.162/53 AND A.163/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.						
c20:	IF A.4/51 THEN m ELSE n/a						

PROPOSED CHANGE

A.2.2.4.10A 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.163/15A - - PUBLISH request

Table A.260A: 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	c28	c28	[56B] 9.2	c28	c29
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c29	c29
4	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
5	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6	Call-Info	[26] 24.9	m	m	[26] 24.9	c4	c4
7	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
8	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
9	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
12	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
14	Event	[70] ~~3.6~~4, 6	m	m	[70] ~~3.6~~4, 6	m	m
15	Expires	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	m	m	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	i	i
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	In-Reply-To	[26] 20.21	m	m	[26] 20.21	i	i
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
19	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
20	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
21	P-Access-Network-Info	[52] 4.4	c23	c23	[52] 4.4	c24	c24
22	P-Asserted-Identity	[34] 9.1	c10	c10	[34] 9.1	c11	c11
23	P-Called-Party-ID	[52] 4.2	c14	c14	[52] 4.2	c15	c16
24	P-Charging-Function-Addresses	[52] 4.5	c21	c21	[52] 4.5	c22	c22
25	P-Charging-Vector	[52] 4.6	c19	c19	[52] 4.6	c20	c20
26	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c9	c9

27	P-Visited-Network-ID	[52] 4.3	c17	n/a	[52] 4.3	c18	n/a
28	Priorità	[26] 20.26	m	m	[26] 20.26	i	i
29	Privacy	[33] 4.2	c12	c12	[33] 4.2	c13	c13
30	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c7	c7
31	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
32	Reason	[34A] 2	c8	c8	[34A] 2	c1	c1
33	Referred-By	[59] 3	c30	c30	[59] 3	c31	c31
34	Reject-Contact	[56B] 9.2	c27	c27	[56B] 9.2	c27	c28
34A	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
35	Request-Disposition	[56B] 9.1	c27	c27	[56B] 9.1	c27	c27
36	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
37	Route	[26] 20.34	m	m	[26] 20.34	m	m
38	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c25	c25
39	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c26	c26
40	SIP-If-Match	[70] ~~7~~11.3.2	m	m	[70] ~~7~~11.3.2	i	i
41	Subject	[26] 20.36	m	m	[26] 20.36	i	i
42	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
43	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
44	To	[26] 20.39	m	m	[26] 20.39	m	m
45	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
46	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
c2:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c3:	IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c4:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c5:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.
c6:	IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.
c7:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
c8:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c9:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c10:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c11:	IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c12:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c13:	IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c14:	IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.
c15:	IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.
c16:	IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF.
c17:	IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.
c18:	IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.
c19:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c20:	IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c21:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c22:	IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c23:	IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c24:	IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c25:	IF A.162/47 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 1).
c26:	IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c27:	IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c28:	IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.
c29:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension (note 2).
c30:	IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.
c31:	IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.
NOTE 1:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented.
NOTE 2:	c29 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.

Prerequisite A.163/15A - - PUBLISH request

Table A.260B: Supported message bodies within the PUBLISH request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/15B - - PUBLISH response

Table A.260C: Supported headers within the PUBLISH response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 24.9	m	m	[26] 24.9	c3	c3
3	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
4	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
5	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
8	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
10	From	[26] 20.20	m	m	[26] 20.20	m	m
11	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
12	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
13	P-Access-Network-Info	[52] 4.4	c13	c13	[52] 4.4	c14	c14
14	P-Asserted-Identity	[34] 9.1	c5	c5	[34] 9.1	c6	c6
15	P-Charging-Function-Addresses	[52] 4.5	c11	c11	[52] 4.5	c12	c12
16	P-Charging-Vector	[52] 4.6	c9	n/a	[52] 4.6	c10	n/a
17	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c4	n/a
18	Privacy	[33] 4.2	c7	c7	[33] 4.2	c8	c8
19	Require	[26] 20.32	m	m	[26] 20.32	c15	c15
20	Server	[26] 20.35	m	m	[26] 20.35	i	i
21	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
22	To	[26] 20.39	m	m	[26] 20.39	m	m
23	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
24	Via	[26] 20.42	m	m	[26] 20.42	m	m
25	Warning	[26] 20.43	m	m	[26] 20.43	i	i

c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c4: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c5: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c7: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c9: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c11: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c13: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c14: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c15: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/7 - - 200 (OK)

Table A.260D: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
3	Expires	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	m	m	[26] 20.19, [70] ~~7.1.1~~4, 5, 6	i	i
4	SIP-Etag	[70] ~~7~~11.3.1	m	m	[70] ~~7~~11.3.1	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.260E: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c1:	IF A.162/19E THEN m ELSE i - - deleting Contact headers.						

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 401 (Unauthorized)

Table A.260F: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.260G: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/18 -- 405 (Method Not Allowed)

Table A.260H: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.260I: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/25 -- 415 (Unsupported Media Type)

Table A.260J: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	m	m	[26] 20.1	i	i
2	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
4	Allow	[26] 20.5	m	m	[26] 20.5	i	i
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.260K: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Supported	[26] 20.37	m	m	[26] 20.37	i	i
4	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
c3:	IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER.						

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.260L: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/29 - - 423 (Interval Too Brief)

Table A.260M: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	o		[26] 20.18	o	
3	Min-Expires	[26] 20.23, [70] ~~6~~5, 6	m	m	[26] 20.23, [70] ~~6~~5, 6	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.260N: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/39 - - 489

Table A.260O: Supported headers within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i

Prerequisite A.163/17 - - PUBLISH response

Table A.260P: Supported message bodies within the PUBLISH response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

3GPP TSG-CN1 Meeting #36 **Tdoc N1-042086**
Seoul, Korea, 15-19 November 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **741** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Throttling
Source:	⌘	Nokia
Work item code:	⌘	IMS2
Date:	⌘	18/11/2004
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:	⌘	Event notification throttling is not supported in IETF, and postponed in OMA.
Summary of change:	⌘	Reference to throttling removed
Consequences if not approved:	⌘	Reference to obsoleted RFCs (RFC2806, RFC 2916) in TS.
Clauses affected:	⌘	2, 5.7.1.6

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

Other comments: ⌘

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

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

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

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

=======FIRST 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 2806 (April 2000): "URLs for Telephone Calls".

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

[24] RFC 2916 (September 2000): "E.164 number and DNS".

[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] draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)"

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

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

[58] draft-ietf-sip-session-timer-13 (January 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] draft-ietf-sip-referredby-05 (March 2004): "The SIP Referred-By Mechanism".

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

[60] draft-ietf-sip-replaces-05 (February 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

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

[61] draft-ietf-sip-join-03 (February 2004): "The Session Inititation Protocol (SIP) "Join" Header".

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

[62] 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.

[70] draft-ietf-sip-publish-02 (January 2004): "Session Initiation Protocol (SIP) Extension for Presence Publication".

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

[71] Void.

~~[71] draft-niemi-sipping-event-throttle-00 (October 2003): "Session Initiation Protocol (SIP) Event Notification Throttles".~~

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

[72] draft-ietf-simple-winfo-package-05 (January 2003): "A Session Initiation Protocol (SIP) Event Template-Package for Watcher Information".

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

[74] draft-ietf-simple-presence-10 (January 2003): "A Presence Event Package for the Session Initiation Protocol (SIP)".

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

[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.

---------- next change ----------

5.7.1.6 Event notification throttling

If the AS has a local configuration information limiting the rate at which notification generation is allowed, then the AS shall take that information into account. Such local configuration information could be e.g. the shortest time period between issuing consecutive NOTIFY requests.~~If the user has indicated a preference for throttling of SIP event notifications using the parameters defined in draft-niemi-sipping-event-throttle-00 [71], then the AS shall generate notifications in accordance with the user's preference and possibly other policies (e.g. AS internal policy) applied to the case.~~

~~Editor's Note: draft-niemi-sipping-event-throttle-00 [71] is one solution for the requirement. If other solutions are identified, the text shall be updated to reflect the chosen solution.~~

---------- end of changes ----------

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042087

was Tdoc N1-041883

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **744** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Corrections to text on receiving SDP offer in 200 (OK) response
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	06/11/2004
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:	⌘	CR682R1 to 24.229 (N1-041592 → NP-040381) agreed at CN1#35 proposed text associated with receiving an SDP offer in a SIP 200 (OK) response. There are some errors in this text, in that includes what is apparently a normative requirement on the SIP procedures, when this is clause 6 and therefore the SDP procedures. However there is a normative requirement which is to forward the SDP offer, and the text is rephrased to reflect this.
Summary of change:	⌘	See reason for change. Additionally "ACK message" is changed to "ACK request".
Consequences if not approved:	⌘	Unclear text with SDP procedures wrongly phrased as SIP procedures.

Clauses affected:	⌘	6.2, 6.3

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.

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.

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.

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 ~~200 OK~~ SDP offer and on the receipt of the ACK ~~message~~request containing the SDP answer, it shall 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 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.

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].

When the S-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 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.

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 200 OK~~ SDP offer and on the receipt of the ACK ~~message~~request containing the SDP answer, it shall immediately terminate the session as described described in subclause 5.4.5.1.2.

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042088

was **Tdoc N1-041886**

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **745** ⌘ **rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Privacy corrections
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	07/11/2004
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: ⌘ 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. This CR also made changes to the references used for the privacy procedures at the S-CSCF, such that the reference is now only to RFC 3325.

RFC 3325 only defines the "id" privacy tag within the Privacy header. RFC 3323 defines the Privacy header itself, and other tags, e.g. the "none" and "critical" tags, see below:

none: The user requests that a privacy service apply no privacy functions to this message, regardless of any pre-provisioned profile for the user or default behavior of the service. User agents can specify this option when they are forced to route a message through a privacy service which will, if no Privacy header is present, apply some privacy functions which the user does not desire for this message. Intermediaries MUST NOT remove or alter a Privacy header whose priv-value is 'none'. User agents MUST NOT populate any other priv-values (including 'critical') in a Privacy header that contains a value of 'none'.

critical: The user asserts that the privacy services requested for this message are critical, and that therefore, if these privacy services cannot be provided by the network, this request should be rejected. Criticality cannot be managed appropriately for responses.

Therefore while it is perfectly valid for a reference to be made to RFC 3325, as now currently stands in the S-CSCF procedures text, the key reference is still

		that to RFC 3323, which was the one that was removed in the last CR. Note also that procedures in relation to the trust domain are also specified in RFC 3325, as this is a concent defined in that document. Therefore the subsequent note is corrected.
Summary of change:	⌘	In the S-CSCF procedures, references to RFC 3323 are reinstated.
Consequences if not approved:	⌘	Essential procedures for the operation of privacy will not be referenced.

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

How to create CRs using this form:

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

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

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

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

5.4.3.2 Requests initiated by the served user

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

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

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

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

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

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

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

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

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. 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 2: 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 3: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 4: 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~~3~~ [34~~3~~].

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.

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) 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) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

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

8) if necessary perform the caller preferences to callee capabilities matching according to draft-ietf-sip-caller-preferences [62];

9) 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;

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", forward the request to the contact with the highest qvalue parameter. In case no qvalue parameters were provided, the S-CSCF shall decide locally how to forward the request; 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 shall forward the request as directed by the Request Disposition header as described in draft-ietf-sip-callerprefs-10 [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 INVITE;

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~~3~~ [34~~3~~].

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, 9, 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) 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;

3) 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

4) in case the response is sent towards the terminating 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 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.

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 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, 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 #36
Seoul, Korea, 15th to 19th November 2004

***Tdoc* ⌘N1-042089**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **753** ⌘**rev** **1** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	SIP messages carrying the access-network-charging-info for sessions without preconditions
Source:	⌘	Orange
Work item code:	⌘	IMS2
Date:	⌘	20/11/2004
Category:	⌘	**F**
Release:	⌘	REL-6

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

Use one of the following releases:

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

Reason for change:	⌘	In TS 24.229, the messages at the P-CSCF where the access-network-charging-info is included are described depending on the support by the remote UE of the integration of resource management in SIP or not (i.e. the support of preconditions or not). However, at the S-CSCF the messages where the access-network-charging-info is received when the remote UE does not support the integration of resource management in SIP (i.e. the preconditions are not supported) are missing.
Summary of change:	⌘	Section 5.4.4 is modified to add the case of remote UE that does not support intergration of ressource management in SIP (i.e. does not support the preconditions).
Consequences if not approved:	⌘	Inconsistency between the P-CSCF procedure and the S-CSCF procedure for the transmission of the access-network-charging-info.

Clauses affected:	⌘	5.4.4			
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 co

*** FIRST MODIFICATION ***

5.4.4 Call initiation

5.4.4.1 Initial INVITE

When the S-CSCF receives an INVITE request, either from the served user or destined to the served user, the S-CSCF may require the periodic refreshment of the session to avoid hung states in the S-CSCF. If the S-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer-12 [58] clause 8.

NOTE: 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.

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives any 1xx response, 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 shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives any 1xx or 2xx response, the S-CSCF shall 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.

When the S-CSCF receives the ~~UPDATE~~ request containing the access-network-charging-info parameter in the P-Charging-Vector, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain access-network-charging-info parameter in the P-Charging-Vector header when the request is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header when the ~~UPDATE~~ request is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

5.4.4.2.2 Mobile-terminating case

When the S-CSCF sends any 1xx response, the S-CSCF shall insert an 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 the any 1xx or 2xx response, the S-CSCF shall 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.

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses containing the access-network-charging-info parameter in the P-Charging-Vector, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header when the response is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header when the response is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #36
Seoul, Korea, 15th to 19th November 2004

***Tdoc* ⌘N1-042090**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **755** ⌘**rev** **1** ⌘ Current version: **6.4.0** ⌘

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

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

Title:	⌘	Network-initiated deregistration for multiple UEs sharing the same user public identity and for the old contact information of a roaming UE registered in a new network
Source:	⌘	Orange
Work item code:	⌘	IMS2
Date:	⌘	20/11/2004
Category:	⌘	**F**
Release:	⌘	REL-6

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

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

Reason for change:	⌘	Public User identities may be shared across multiple UEs. Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and different contact addresses. Thus, a given Public User Identity may be deregistered from this UE, while still be registered from another UE. The de-registration procedure between the S-CSCF and the HSS in section 5.4.1.5 should be improved to cover the case of multiple UEs sharing the same public user identities. When the UE is roaming, registration is done in a new network using a new contact address and the previous registration has not expired, the old contact shall be deregistered but not the new contact. The procedure should be improved to handle this case in section 5.4.1.5.
Summary of change:	⌘	The text in section 5.4.1.5 is modified so that: - De-registration procedure between the S-CSCF and the HSS is done only for the public user identities linked to the same private identity (to cover the case of multiple UEs sharing the same public user identities). - The specific case of deregistration of the old contact information when a UE is roaming, registration is done in a new network (i.e. using a new contact address and the previous registration has not expired) is added. In section 5.4.1.2, a reference is added to the new subclause 5.4.1.5.
Consequences if not approved:	⌘	Incorrect handling in case of multiple UEs registered with the same public user identity. Incorrect handling in the case of deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous

registration has not expired.

Clauses affected:	⌘	5.4.1.2, 5.4.1.5			
		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 co

*** FIRST MODIFICATION ***

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

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

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

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

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

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated deregistration procedure only for the previous contact information as described in subclause 5.4.1.5.4.

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

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

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

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

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

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

*** END OF FIRST MODIFICATION ***

*** SECOND MODIFICATION ***

5.4.1.5 Network-initiated deregistration

NOTE 1: A network-initiated deregistration event that occurs at the S-CSCF may be received from the HSS or may be an internal event in the S-CSCF.

Prior to initiating the network-initiated deregistration for the only currently registered public user identity and its associated set of implicitly registered public user identities that have been registered with the same contact (i.e. no other public user identity is registered with this contact) while there are still active multimedia sessions belonging to this contact, the S-CSCF shall release only the multimedia sessions belonging to this contact as described in subclause 5.4.5.1. The multimedia sessions for the same public user identi~~i~~ty, if registered with another contact remain unchanged.

When a network-initiated deregistration event occurs for one or more public user identities that are bound to one or more contacts, the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. Prior to sending the NOTIFY request, the S-CSCF may release all sessions related to the contacts that will be deregistered. For each NOTIFY request, the S-CSCF shall:

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

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

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

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

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

   b) if the public user identity:

      i) has been deregistered then:

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

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

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

      ii) has been kept registered then:

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

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

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

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

NOTE 2: There might be more thaen one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user identitity, if registered by another UE using different private user identities remain unchanged.

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

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

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

In case of the deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired, on completion of the above procedures, the S-CSCF shall remove the registration information related to the old contact from the local data.

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

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

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #36
Seoul, Korea, 15th to 19th November 2004

***Tdoc* ⌘N1-042105**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **747** ⌘**rev** **2** ⌘ Current version: **6.4.0** ⌘

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

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

Title:	⌘	P-Charging-Vector syntax
Source:	⌘	Orange
Work item code:	⌘	IMS2
Date:	⌘	20/11/2004
Category:	⌘	**F**
Release:	⌘	REL-6

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

Use one of the following releases:

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

Reason for change:	⌘	The syntax of extensions to the P-Charging-Vector is described in B.4.1. The extension "access-network-charging-info" for GPRS access network contains more information than requested by SA5 for charging correlation. Indeed, in TS 32.225, it is stated that "If GPRS is used to access the IMS, the GCID is used together with the GGSN address as the access part of the charging correlation vector that is comprised of an access part and an IMS part, which is the IMS Charging Identifier." Moreover, it is stated in TS 29.207 that: "To ensure charging correlation, the GGSN shall send the GCID and GGSN address information to the PDF after the successful establishment of the secondary PDP context, i.e. with the report following the initial authorization decision." The access-charging-info extension in the P-Charging Vector contains parameters values that can be set to zero.
Summary of change:	⌘	The value of the different parameters is clarified depending if the session used PDP Contexts for data or used only PDP Context for signalling.
Consequences if not approved:	⌘	Unclear description of the syntax of the "access-network-charging-info" extension

Clauses affected:	⌘	B.4.1			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

*** FIRST MODIFICATION ***

B.4 3GPP specific encoding for SIP header extensions

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~~s~~ 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.

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

The access network charging information is not included in the P-Charging-Vector for non-session based SIP signalling, 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.

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #36
Seoul, Korea, 15th to 19th November 2004

***Tdoc* ⌘N1-042106**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **752** ⌘**rev** **2** ⌘ Current version: **6.4.0** ⌘

*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:	⌘	Unavailability of the access-network-charging-info when the session is established without SBLP
Source:	⌘	Orange
Work item code:	⌘	IMS2
Date:	⌘	20/11/2004
Category:	⌘	**F**
Release:	⌘	REL-6

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

Use one of the following releases:

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

Reason for change:	⌘	In TS 24.229, section 4.5.3.2, the description of the access network charging information is the following: "The access network charging information is generated at the first opportunity after the resources are allocated at the IP-CAN. The access network charging information is passed from IP-CAN to P-CSCF via PDF, over the Go and Gq interfaces. Access network charging information will be updated with new information during the session as media flows are added or removed. The P-CSCF provides the access network charging information to the S-CSCF." In TS 23.228, it is stated that: "At IP-CAN bearer activation the user shall have access to either IP-CAN services without service-based local policy, or IP-CAN services with service-based local policy. It is operator choice whether to offer both or only one of these alternatives for accessing the IM Subsystem." According stage 2, the Go and Gq interfaces are optional, this means that for a session established without SBLP, the Go and Gq interface are not used and the GCID is not transmitted to the P-CSCF.
Summary of change:	⌘	The procedures at the P-CSCF in section 5.2.7 for the establishment of a session is modified with the condition for getting the access-network-charging-info if SBLP is used.
Consequences if not approved:	⌘	Incorrect statement on the availability of the access-network-charging-info at the P-CSCF.

Clauses affected:	⌘	5.2.7			
Other specs affected:	⌘	Y / N	Other core specifications	⌘	
			Test specifications		
			O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

*** FIRST MODIFICATION ***

5.2.7 Initial INVITE

5.2.7.1 Introduction

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

5.2.7.2 Mobile-originating case

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

NOTE 1: 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.

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

Upon receiving a response as specified in RFC 3313 [31] to the initial INVITE request, the P-CSCF shall:

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

NOTE 2: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

The P-CSCF shall also include the access-network-charging-info parameter (if received via the PDF, over the Go and Gq interfaces) in the P-Charging-Vector header in the first request originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF, e.g., after the local resource reservation is complete. Typically, this first request is an UPDATE request if the remote UA supports the "integration of resource management in SIP" extension or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer-12 [58] clause 8.

NOTE 1: 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 in order to make it work.

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

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

NOTE 2: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

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

The P-CSCF shall also include the access-network-charging-info parameter (if received via the PDF, over the Go and Gq interfaces) in the P-Charging-Vector header in the first request or response originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF e.g., after the local resource reservation is complete. Typically, this first response is a 180 (Ringing) or 200 (OK) response if the remote UA supports the "integration of resource management in SIP" extension, or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.7.4 Access network charging information

The P-CSCF shall include the access-network-charging-info parameter within the P-Charging-Vector header as described in subclause 7.2A.5.

*** END OF MODIFICATION ***

3GPP TSG-CN1 Meeting #36 **Tdoc N1-042117**
Seoul, Korea, 15-19 November 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229** **CR** **733** ⌘ **rev** **3** ⌘ Current version: **6.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Clarifications to SigComp
Source:	⌘	Ericsson
Work item code:	⌘	IMS2
Date:	⌘	15/11/2004
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:	⌘	Sufficient performance for services as PoC may not be achieved without clearly clarifying compression capabilities aspects left open in RFC 3320.
Summary of change:	⌘	A couple of clarifications are made to ensure sufficient SigComp compression perfomance: • A minimum allocation of compression memory is specified to allow stateful compression • compartments shall be created at registration
Consequences if not approved:	⌘	Application development may not get sufficient performance for delay critical services e.g. PoC

Clauses affected:	⌘	2, 3.2, 8.1.1, 8.1,3, 8.2.1, 8.2.3

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.

*** First Change ***

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 2806 (April 2000): "URLs for Telephone Calls".

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

[24] RFC 2916 (September 2000): "E.164 number and DNS".

[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] draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)"

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

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

[58] draft-ietf-sip-session-timer-13 (January 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] draft-ietf-sip-referredby-05 (March 2004): "The SIP Referred-By Mechanism".

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

[60] draft-ietf-sip-replaces-05 (February 2004): "The Session Inititation Protocol (SIP) "Replaces" Header".

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

[61] draft-ietf-sip-join-03 (February 2004): "The Session Inititation Protocol (SIP) "Join" Header".

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

[62] 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.

[70] draft-ietf-sip-publish-02 (January 2004): "Session Initiation Protocol (SIP) Extension for Presence Publication".

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

[71] draft-niemi-sipping-event-throttle-00 (October 2003): "Session Initiation Protocol (SIP) Event Notification Throttles".

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

[72] draft-ietf-simple-winfo-package-05 (January 2003): "A Session Initiation Protocol (SIP) Event Template-Package for Watcher Information".

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

[74] draft-ietf-simple-presence-10 (January 2003): "A Presence Event Package for the Session Initiation Protocol (SIP)".

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

[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.

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

*** Third Change ***

8 SIP compression

8.1 SIP compression procedures at the UE

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 ~~no longer~~ 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.

8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

8.1.3 Decompression of SIP requests and responses received from the P-CSCF

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific and this may, as an example, include resetting the compartment~~,~~ or changing the algorithm ~~or sending the following message(s) without compression~~.

8.2 SIP compression procedures at the P-CSCF

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 ~~no longer~~ 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.

8.2.2 Compression of SIP requests and responses transmitted to the UE

The P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

8.2.3 Decompression of SIP requests and responses received from the UE

The P-CSCF shall decompress the compressed requests and responses received from the UE according to subclause 8.2.1.

If the P-CSCF detects a decompression failure at the UE, the recovery mechanism is implementation specific and this may, as an example, include resetting the compartment~~,~~ or changing the algorithm ~~or sending the following message(s) without compression~~.

3GPP TSG-CN1 Meeting #36
Seoul, Korea, 15-19 November 2004

Tdoc N1-042120

CR-Form-v7.1

CHANGE REQUEST

⌘ **TS 24.229** **CR** **734** ⌘ **rev** **2** ⌘ Current version: **6.4.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction to subclause 5.1.3 of TS 24.229
Source:	⌘	LM Ericsson
Work item code:	⌘	IMS2
Date:	⌘	29/10/2004
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:	⌘	There is text in subclause 5.1.3.1.2.1 that applies for subclause 5.1.3.1.3.
Summary of change:	⌘	Text that apply both for subclauses 5.1.3.1.2 and 5.1.3.1.3 are moved to subclause 5.1.3.1.1. In addition some editorial chages have been made.
Consequences if not approved:	⌘	The specification will be incomplete for subclause 5.1.3.1.3.

Clauses affected:	⌘	5.1.3.1.1, 5.1.3.2.1, 5.1.3.2.2 and 5.1.3.1.3

		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

5.1.3 Call initiation - mobile originating case

5.1.3.1 Initial INVITE request

5.1.3.1.1 General

Subclause 5.1.3.1 describe the procedures when the initial INVITE is sent by the originating UE. The default behaviour using the SIP precondition~~precodintion~~ mechanism 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 5.1.3.1.2.2; or
- when the specifc service does not require the precondition mechanism, as described in subclause 5.1.3.1.3.

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 draft-ietf-sip-callerprefs-10 [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

Next 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

~~The UE may also indicate that the 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 draft-ietf-sip-callerprefs-10 [56B].~~

~~NOTE 1: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE may 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~~.

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] and proceed with the procedures described in subclause 5.1.3.2 and subclause 6.1

Next 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~~another~~ INVITE request addressed to the same destination as ~~the~~ initial INVITE ~~was sent~~. When~~In~~ creating the~~this~~ new ~~initial~~ 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) acknowledge, if required~~needed~~, 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 ~~when~~ 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.

Last Change

5.1.3.1.3 "Integration of resource management" not required by originating UE

This procedure is initiated when the SIP precondition procedure is not required for a session by the origination UE.

Upon generating the initial INVITE the UE may indicate the support of preconditions by including the "precondition" option-tag in the Supported header.

When the initial INVITE has been created and forwarded~~sent~~ the forthcoming procedures are identical to the procedures ~~those~~ described in subclause 5.1.3.1.1~~5.1.3.1.4.~~