3GPP TSG CN Meeting #27 **NP-050127**
9th - 11th March 2005. Tokyo, Japan.
was **Tdoc N1-050326 & 66**

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229**	**CR 849**	⌘ **rev**	2 ~~1~~	⌘	Current version:	**6.5.1** ⌘

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

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

Title:	⌘	Corrections to addition of session set-up not requiring preconditions and reliable transport of provisional responses		
Source:	⌘	Lucent Technologies		
Work item code:	⌘	IMS2	***Date:*** ⌘	06/02/2005
Category:	⌘	**F** *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.	***Release:*** ⌘	Rel-6 *Use one of the following releases:* *Ph2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)* *Rel-7 (Release 7)*

Reason for change:	⌘	In CN1#35 a CR was introduced "Addition of session set-up not requiring preconditions and reliable transport of provisional responses" (N1-041632 → NP-040383). During the approval of that CR a number of textual improvements were identified which still need to be made: 1) Discussed in the meeting, two existing subclauses at header level 5 were subdivided, creating a number of subclauses at header level 6. Reasonably simple modifications can keep all this text at header level 5. Indeed, as currently structured, the heading of 5.1.4.1.2.3 is inconsistent with its heading one level up in 5.1.4.1.2, as the higher level heading indicates that all text in this subclause is with preconditions required by the terminating UE, whereas the lower one explicitly precludes it. 2) by using term "preconditions extension" or "preconditions mechanism" with no further explanation we have a discontinuity with the name of the extension in annex A, and no connection of that to mean the entirety of RFC 3312 – precondition is the name of the option-tag rather than the extension. However, rather than change all the usages, an explanatory phrase is inserted at the start of all the appropriate subclauses, and the usage made consistent throughout. 3) References to RFC 3312 are not made at the point where we introduce the extension, but rather inconsistently within the text on some but not all instances.

Further, draft-ietf-sip-rfc3312-update-03.txt has just been approved as a proposed standard by IESG as a document that updates RFC 3312. RFC 3312 is referenced from 3GPP TS 24.229, and some of the changes proposed in draft-ietf-sip-rfc3312-update-03.txt have impact (minor in nature) on the manner in which RFC 3312 is used in the context of these references.

In order to ensure that session establishment does not take place until certain preconditions are met, the RFC-3312 introduces two state variables that describe the state of the media stream: current status and desired status. Session establishment stops until the current status reaches or surpasses the threshold indicated in the desired status. Once this threshold is reached or surpassed, session establishment resumes.

RFC 3312 assumes that the media streams do not move around. That is, media is sent between the same end-points throughout the duration of the session. However, media stream are not always static. For example, in case of call transfer, an existing media stream from point A to B is moved to new transport address C. Moving an existing media stream to a new termination point, from the preconditions point of view, is like establishing a new media stream. Therefore, it is appropriate to set all the current status values of the media streams to "No" and start a new precondition negotiation.

While the RFC 3312 allows to update current status information using offers, it does not allow to downgrade current status values in answers, as shown in the third row of Table 3 of RFC-3312. Since such downgrades are sometimes needed, the Table 3 of RFC 3312 needs to be updated to allow answers to downgrade current status values. The document draft-ietf-sip-rfc3312-update-03.txt provides the required updates that will allow moving an existing stream to a new location [i.e. transport address].

Additionally, even if 3GPP preclude this occurring in 3GPP IMS, given release 6 interworking with other SIP network we cannot prevent such requests entering the IMS and having to dealt with

Summary of change: ⌘ Structure of subclause 5.1.3.1 and 5.1.4.1 is revised to remove descent to header level 6.
Usage of term "precondition mechanism" is properly introduced, and then used consistently throughout.
Appropriate references to RFC 3312 are inserted.
The headlines were changed to be of consistent wording.
Add a reference [30A] to draft-ietf-sip-rfc3312-update-03.txt.
Replace all references to RFC 3312 [30] by text stating RFC 3312 [30] as revised by draft-ietf-sip-rfc3312-update [30A].
The references used for the UPDATE method are incorrectly using [30] at the moment, when they should be to [29] so these are changed.

Consequences if not approved: ⌘ Inconsistent terminology and confusing structure within document. Use of obsolete and incomplete reference RFC.

Clauses affected: ⌘ 2, 5.1.3.1, 5.1.4.1, 5.5.3.1.1, 6.1, A.2.1.2, A.2.1.3, A.2.2.2, A.2.2.3, A.3.2.1, A.3.3.1

Other specs affected: ⌘

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

Other comments: ⌘ ~~If the CR 729, "Incorporation of draft-ietf-sip-rfc3312-update-03.txt" is accepted, the RFC 3312 references in this CR will need some correction, as will that CR, due to interaction.~~ Revision 2 to incorporate CR729R1 "Incorporation of draft-ietf-

	sip-rfc3312-update-03.txt"

How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[44] Void.

[45] Void.

[46] Void.

[47] Void.

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

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

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

[51] Void.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[71] Void.

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

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

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

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

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

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

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

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

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

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

PROPOSED CHANGE

5.1.3.1 Initial INVITE request

5.1.3.1.1 General

Subclause 5.1.3.1 describes the procedures when the initial INVITE is sent by the originating UE. The default behaviour using the "integration of resource management and SIP" extension (~~SIP~~ herafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64], and with the request for such a mechanism known as a precondition) is described in subclause 5.1.3.1.2.~~1~~. Session without preconditions may be initiated:

- when the remote node does not support the precondition mechanism, as discovered in subclause 5.1.3.1.3~~2.2~~; or
- when the specifc service does not require the precondition mechanism, as described in subclause 5.1.3.1.4~~3~~.

Editor's Note: The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

The UE may indicate that proxies should not fork the INVITE request by including a "no-fork" directive within the Request-Disposition header in the initial INVITE request as described in RFC 3841 [56B].

NOTE 1: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

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

If the UE receives a 488 (Not Acceptable Here) response to an initial INVITE request, the UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 2: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements

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

5.1.3.1.2~~.1~~ "Integration of resource management and SIP" required by originating UE~~Preconditions required by originating UE~~

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

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;

- indicate the requirement ~~of~~ for the preconditions mechanism and specify it using the Require header mechanism.

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

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

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

b) try to complete the session by relaxing the requirement on the usage of the ~~"integration of resource management in SIP" extension as described in RFC 3312 [30]~~ precondition mechanism and proceed with the procedures described in subclause 5.1.3.1.3 and subclause 6.1.

5.1.3.1.3~~2.2~~ "Integration of resource management and SIP" required by originating UE and ~~Preconditions~~ not supported by ~~remote end~~terminating UE

This procedure is initiated upon the reception of a 420 (Bad Extension) response to an initial INVITE request, the response containing the "precondition" option-tag in the Unsupported header field value.

The UE may create a new INVITE request addressed to the same destination as initial INVITE. When creating the new INVITE request, the UE shall:

1) populate the From, To, Call-ID headers and the Request-URI as per the initial INVITE request;

2) include the "precondition" option-tag in the Supported header;

3) set each of the media streams in inactive mode in SDP as described in subclause 6.1 in this specification in order to prevent the terminating end to send media whereas the resource reservation is not done at the originating side; and

4) forward the INVITE request as per regular procedures.

Upon receiving a provisional response or final response containing the remote SDP, the UE shall:

1) acknowledge, if required, the SIP response as per regular SIP procedures defined in RFC 3261 [26] and RFC 3262 [27]; and

2) initiate the regular resource reservation mechanism, as described in subclause 9.2.5.

When the above INVITE transaction is successfully completed, and the local resource reservation procedure is complete, the UE shall create and forward a re-INVITE request including:

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

2) SDP in which the media streams previously set in inactive mode are set to active (sendrecv, sendonly or recvonly) mode, according to the procedures described in subclause 6.1 in this specification.

5.1.3.1.4~~3~~ "Integration of resource management and SIP" not required by originating UE

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

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

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

PROPOSED CHANGE

5.1.4 Call initiation - mobile terminating case

5.1.4.1 Initial INVITE request

5.1.4.1.1 General

The handling of incoming initial INVITE requests at the terminating UE is mainly dependant on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (herafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64], and with the request for such a mechanism known as a precondition)~~resource reservation~~; and

- the UEs configuration for the case when the specific service does not require ~~resource reservation~~the precondition mechanism.

Editor's Note: The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires integration of resource management ~~is required~~ either due to the requested service or due to local configuration.

If resource management is required at the terminating UE and:

a) the received INVITE request includes the "precondition" option-tag in the Require header, the terminating UE shall perform the actions as described in subclause 5.1.4.1.2.~~1~~;

b) the received INVITE request does not include the "precondition" option-tag in the Require header and the terminating UE, based on local configuration, requires the usage of ~~preconditions~~ the precondition mechanism in this case, the terminating UE shall perform the actions as described in subclause 5.1.4.1.3~~2.2~~; or

c) the received INVITE request does not include the "precondition" option-tag in the Require header and the terminating UE, based on local configuration, does not require the usage of ~~preconditions~~ the precondition mechanism in this case, the terminating UE shall perform the actions as described in subclause 5.1.4.1.4~~2.3~~.

If resource management is not required by the terminating UE and:

a) the received INVITE request includes the "precondition" option-tag in the Require header, the terminating UE shall perform the actions as described in subclause 5.1.4.1.2~~.1~~, i.e. the terminating UE shall use the precondition mechanism in order to fulfil the requirement of the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Require header, the terminating UE shall perform the actions as described in subclause 5.1.4.1.4~~3~~.

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

Editor's Note: The above note needs further investigation.

~~5.1.4.1.2 "Integration of resource management" required by terminating UE~~

5.1.4.1.2~~.1~~ "Integration of resource management and SIP" required by terminating UE and ~~Preconditions~~ used by originating UE

Upon generating the first response to the initial INVITE request that indicated the "precondition" option-tag in the Require header, the UE shall indicate the requirement for reliable provisional responses and specify it using the Require header mechanism.The UE shall send the 200 (OK) response to the initial INVITE request only after the local resource reservation has been completed and the call is accepted by the termination user.

5.1.4.1.3~~2.2~~ "Integration of resource management and SIP" required by terminating UE and ~~Preconditions~~ not used by originating UE ~~but preconditions required by terminating UE~~

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

5.1.4.1.4~~2.3~~ "Integration of resource management and SIP" ~~Preconditions~~ not ~~used~~ required by ~~originating~~ terminating UE and ~~preconditions~~ not ~~required~~ used by ~~terminating~~ originating UE

Upon receiving an initial INVITE request without containing the "precondition" option-tag in the Require header, if the terminating UE is configured to not use the precondition~~s extension~~ mechanism~~as described in RFC 3312 [30]~~, the UE shall:

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

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

~~5.1.4.1.5~~3 ~~"Integration of resource management" not required by terminating UE~~

~~Upon receiving an initial INVITE request without containing the "precondition" option-tag Require headers, and "integration of resource management" is not required by the terminating UE, the terminating UE shall:~~

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

~~2) send 200 (OK) response, when the call is accepted by the terminating user.~~

PROPOSED CHANGE

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

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

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

PROPOSED CHANGE

6.1 Procedures at the UE

Usage of SDP by the UE:

1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.
2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP payload with the most preferred codec listed first.
3. If the SIP request includes a "precondition" option-tag in the Require header (indicating the requirement for "Integration of resource management and SIP" and hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by draft-ietf-sip-rfc3312-update [64]), the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

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

   a=des:qos optional local sendrecv

   In the case described in subclause 5.1.3.1.3~~2.2~~ in the first SDP offer the UE sends, the UE shall set each media stream in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

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

4. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, and the precondition mechanism is used as described in subclause 5.1.4.1.2~~.1~~, the first 183 (Session Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.

   In the case described in subclause 5.1.4.1.5~~3~~ no specific SDP procedures for integration of resource reservation have to be performed.

   In the case described in subclause 5.1.4.1.4~~2.3~~ in the first SDP answer the UE sends, the UE shall set each media streams in inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].

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

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

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

7. For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

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

   For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [13].

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

8. The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [23].

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

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

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

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

PROPOSED CHANGE

A.2.1.2 Major capabilities

Table A.4: Major capabilities

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

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

c2:	IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.
c3:	IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UE or S-CSCF functional entity.
c4:	IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.
c5:	IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.
c6:	IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7:	IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control.
c8:	IF A.3/1 THEN m ELSE n/a - - UE behaviour.
c9:	IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.
c11:	IF A.3/1 OR A.3/6 THEN o ELSE n/a - - UE or MGCF.
c12:	IF A.3/7D THEN m ELSE n/a - - AS performing 3rd-party call control.
c13:	IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE behaviour or S-CSCF.
c14:	IF A.3/1 THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE or P-CSCF.
c15:	IF A.4/20 and A.3/4 THEN m ELSE o – SIP specific event notification extensions and S-CSCF.
c16:	IF A.4/20 and (A.3/1 OR A.3/2) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF.
c17:	IF A.3/1 or A.3/4 THEN m ELSE n/a - - UE or S-CSCF.
c18:	IF A.4/2B THEN m ELSE n/a - - initiating sessions.
c19:	IF A.4/2B THEN o ELSE n/a - - initiating sessions.
c20:	IF A.3/1 THEN m ELSE n/a - - UE behaviour.
c21:	IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).
c22:	IF A.4/30 AND (A.3/1 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UA.
c23:	IF A.4/30 AND A.3/1 THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE.
c24:	IF A.4/30 AND A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF.
c25:	IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CSCF or AS acting as terminating UA or AS acting as third-party call controller.
c26:	IF A.4/30 AND (A.3/6 OR A.3/7A OR A.3/7B or A.3/7D) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller.
c27:	IF A.3/7D THEN o ELSE x - - AS performing 3rd party call control.
c28:	IF A.3/1 THEN m ELSE o.5 - - UE.
c29:	IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.
c30:	IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS.
c33:	IF A.3/11 OR A.3/12 OR A.4/44 THEN m ELSE o - - conference focus or conference participant or the Session Inititation Protocol (SIP) "Replaces" header.
c34:	IF A.4/44 OR A.4/45 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header or the Session Inititation Protocol (SIP) "Join" header.
c35:	IF A.3/4 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8) THEN o ELSE n/a - - UE, MGCF, AS MRFC or S-CSCF functional entity.
o.1:	At least one of these capabilities is supported.
o.2:	At least one of these capabilities is supported.
o.3:	At least one of these capabilities is supported.
o.4:	At least one of these capabilities is supported.
o.5:	At least one of these capabilities is supported.
NOTE 1:	At the MGCF, the interworking specifications do not support a handling of the header associated with this extension.

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

Table A.4A: Supported event packages

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

c1: IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.
c2: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c3: IF A.3/1 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, P-CSCF, AS.
c4: IF A.3/4 THEN m ELSE n/a - - S-CSCF.
c5: IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.
c6: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - watcher, acting as the notifier of event information.
c7: IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.
c8: IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.
c9: IF A.3A/1 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.
c10: IF A.3A/2 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c11: IF A.3A/2 OR A.3A/4 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - watcher or presence user agent, acting as the subscriber to event information.
c12: IF A.3A/1 OR A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server, acting as the notifier of event information.
c13: IF A.4/15 THEN m ELSE n/a - - the REFER method.
c21: IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.
c22: IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.

PROPOSED CHANGE

A.2.1.3 PDUs

Table A.5: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	c10	c10	[26] 13	c11	c11
2	BYE request	[26] 15.1	c12	c12	[26] 15.1	c12	c12
3	BYE response	[26] 15.1	c12	c12	[26] 15.1	c12	c12
4	CANCEL request	[26] 9	m	m	[26] 9	m	m
5	CANCEL response	[26] 9	m	m	[26] 9	m	m
8	INVITE request	[26] 13	c10	c10	[26] 13	c11	c11
9	INVITE response	[26] 13	c11	c11	[26] 13	c10	c10
9A	MESSAGE request	[50] 4	c7	c7	[50] 7	c7	c7
9B	MESSAGE response	[50] 4	c7	c7	[50] 7	c7	c7
10	NOTIFY request	[28] 8.1.2	c4	c4	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c4	c4
12	OPTIONS request	[26] 11	m	m	[26] 11	m	m
13	OPTIONS response	[26] 11	m	m	[26] 11	m	m
14	PRACK request	[27] 6	c5	c5	[27] 6	c5	c5
15	PRACK response	[27] 6	c5	c5	[27] 6	c5	c5
15A	PUBLISH request	[70] 11.1.3	c20	c20	[70] 11.1.3	c20	c20
15B	PUBLISH response	[70] 11.1.3	c20	c20	[70] 11.1.3	c20	c20
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 10	c8	c8	[26] 10	c9	c9
19	REGISTER response	[26] 10	c9	c9	[26] 10	c8	c8
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c4	c4
21	SUBSCRIBE response	[28] 8.1.1	c4	c4	[28] 8.1.1	c3	c3
22	UPDATE request	[~~30~~29] 6.1	c6	c6	[~~30~~29] 6.2	c6	c6
23	UPDATE response	[~~30~~29] 6.2	c6	c6	[~~30~~29] 6.1	c6	c6
c1:	IF A.4/15 THEN m ELSE n/a - - the REFER method extension.						
c3:	IF A.4/23 THEN m ELSE n/a - - recipient for event information.						
c4:	IF A.4/22 THEN m ELSE n/a - - notifier of event information.						
c5:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses extension.						
c6:	IF A.4/17 THEN m ELSE n/a - - the SIP update method extension.						
c7:	IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.						
c8:	IF A.4/1 THEN m ELSE n/a - - client behaviour for registration.						
c9:	IF A.4/2 THEN m ELSE n/a - - registrar.						
c10:	IF A.4/3 THEN m ELSE n/a - - client behaviour for INVITE requests.						
c11:	IF A.4/4 THEN m ELSE n/a - - server behaviour for INVITE requests.						
c12:	IF A.4/5 THEN m ELSE n/a - - session release.						
c20:	IF A.4/41 THEN m ELSE n/a.						

PROPOSED CHANGE

A.2.2.2 Major capabilities

Table A.162: Major capabilities

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

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

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

c1:	IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.
c2:	IF A.3/2 OR A.3/3A OR A.3/4 THEN m ELSE o - - P-CSCF, I-CSCF(THIG) or S-CSCF.
c3:	IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion.
c4:	IF A.162/23 THEN m ELSE o - - integration of resource management and SIP.
c5:	IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6:	IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG).
c7:	IF A.3/2 THEN m ELSE n/a - - P-CSCF.
c8:	IF A.3/2 AND A.162/30 THEN m ELSE n/a - - P-CSCF and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c9:	IF A.3/2 AND A.162/30 THEN m ELSE IF A.3/7C AND A.162/30 THEN o ELSE n/a - - S-CSCF or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (NOTE).
c10:	IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c11:	IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header.
c12:	IF A.162/31 AND A.3/4 THEN m ELSE n/a - - S-CSCF.
c13:	IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C) THEN m ELSE n/a - - P-CSCF OR I-CSCF OR AS acting as a SIP proxy.
c14:	IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).
c15:	IF A.162/35 AND (A.3/2 OR A.3/3) THEN m THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF.
c16:	IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or S-CSCF.
c17:	IF A.162/35 AND (A.3/2 OR A.3/3) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF.
c18:	IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension.
c19:	IF A.162/35 AND (A.3/2 OR A.3.3 OR A.3/4 OR A.3/7 THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy.
c20:	IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c21:	IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF.
c22:	IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF.
c23:	IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c24:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c25:	IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c26:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function Addresses header extension.
c27:	IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF.
c28:	IF A.3/2 OR A.3/4 OR A.3/6 then m ELSE o - - P-CSCF or S-CSCF of MGCF.
c29:	IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m - - P-CSCF or S-CSCF of MGCF.
c30:	IF A.3/2 o ELSE i - - P-CSCF.
c31:	IF A.3/4 THEN m ELSE x - - S-CSCF.
c32:	IF A.3/4 THEN m ELSE o.4 - - S-CSCF.
c33:	IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.
o.1:	It is mandatory to support at least one of these items.
o.2:	It is mandatory to support at least one of these items.
o.3:	It is mandatory to support at least one of these items.
o.4	At least one of these capabilities is supported.
NOTE:	An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.

PROPOSED CHANGE

A.2.2.3 PDUs

Table A.163: Supported methods

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

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

PROPOSED CHANGE

A.3.2.1 Major capabilities

Table A.317: Major capabilities

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

PROPOSED CHANGE

A.3.3.1 Major capabilities

Table A.328: Major capabilities

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