3GPP TSG-CN Meeting #24 **NP-040198**
2nd – 4th June 2004. Seoul, Korea.

Source: **TSG CN WG 1**

Title: **CRs to Rel-6 on Work Item PRESNC towards 24.229**

Agenda item: **9.2**

Document for: **APPROVAL**

Introduction:

This document contains **2** CRs, **Rel-6** Work Item **"PRESNC"**, that have been agreed by **TSG CN WG1 in CN1#34 meeting**, and are forwarded to TSG CN Plenary meeting #24 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version-Current	Doc-2nd-Level
24.229	629	2	Rel-6	Addition of PRESNC material	B	6.2.0	N1-040996
24.229	652		Rel-6	Creation of separate event package table for UA role	C	6.2.0	N1-041066

3GPP TSG-CN1 Meeting #34 **Tdoc N1-040996**

Zagreb, Croatia 10 – 14 May 2004

was Tdoc N1-040621, Tdoc N1-040766

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **629** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Addition of PRESNC material
Source:	⌘	Lucent Technologies
Work item code:	⌘	PRESNC
Date:	⌘	22/03/2004
Category:	⌘	**B**
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 3GPP CN1, the PRESNC work item has been progressed as 3GPP TR 24.841. This includes material that is needed for PRESNC, but is generic in its operation, and therefore needs to be placed in 3GPP TS 24.229. This CR performs that transfer of material.
Summary of change:	⌘	New procedures are added for application server authentication requirements. New procedures are added for throttling at the application server. Requirements from the draft-ietf-sipping-publish draft, e.g. PUBLISH method and 412 status-code are added to the SIP profile.
Consequences if not approved:	⌘	PRESNC will not be in release 6.

Clauses affected:	⌘	2, 5.7.1.4 (new), 5.7.1.5 (new), 5.7.1.6 (new), A.2.1.2, A.2.1.3, A.2.1.4.1, A.2.1.4.10A, A.2.2.2, A.2.2.3, A.2.2.4.1, A.2.2.4.10A

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

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

2 References

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

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

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

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

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

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

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

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

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

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

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

[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)".

[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] draft-ietf-sipping-reg-event-00 (October 2002): "A Session Initiation Protocol (SIP) Event Package for Registrations".

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

[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".

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

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

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

[73] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[74] draft-ietf-simple-presence-10 (January 2003): "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".

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

[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".

PROPOSED CHANGE

5.7.1 Common Application Server (AS) procedures

5.7.1.1 Notification about registration status

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

Upon receipt of a third-party REGISTER request, the AS may subscribe to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in draft-ietf-sipping-reg-event-00 [43].

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

a) a Request URI set to the resource to which the AS wants to be subscribed to, i.e. to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

b) a From header field set to the AS's SIP URI;

c) a To header field, set to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

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

e) a P-Asserted-Identity header field set to the SIP URI of the AS; and

NOTE 1: The S-CSCF expects the SIP URI used in the P-Asserted-Identity header to correspond to the SIP URI, which identified this AS in the initial filter criteria of the user to whose registration state the AS subscribes to.

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

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

NOTE 2: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header set to "terminated", the AS considers the subscription to the reg event package terminated, i.e. as if the AS had sent a SUBSCRIBE request with an Expires header containing a value of zero.

5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request (excluding ACK requests and CANCEL requests and responses) for a standalone transaction, the AS shall store the values received in the P-Charging-Vector header, e.g. icid

parameter, and retain the P-Charging-Vector header in the message. The AS shall store the values received in the P-Charging-Function-Addresses header and retain the P-Charging-Function-Addresses header in the message.

When an AS sends any request or response related to a dialog or standalone transaction, the AS may insert previously saved values into the P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.7.1.3 Access-Network-Info

The AS may receive in any request or response (excluding ACK requests and CANCEL requests and responses) information about the served user access network. This information is contained in the P-Access-Network-Info header. The AS can use the header to provide an appropriate service to the user.

5.7.1.4 User identify verification at the AS

The procedures at the AS to accomplish user identity verification are described with the help of figure 5-1.

When the AS receives a SIP initial or standalone request that does not contain credentials, the AS shall:

Editor's Note: it is not clear what are the mechanisms available to transport the credentials. These mechanisms can include, among others, P-Asserted-Identity, Authorization header, digital signatures, S/MIME body, etc.

a) if a Privacy header is present in the initial or standalone request and the Privacy header value is set to "id" or "user", then the user and the request are considered as anonymous, and no further actions are required. The AS shall consider the request as authenticated;

b) if there is no Privacy header present in the initial or standalone request, or if the Privacy header contains a value other than "id" or "user", then the AS shall check for the presence of a P-Asserted-Identity header in the initial or standalone request. Two cases exists:

   i) the initial or standalone request contains a P-Asserted-Identity header. This is typically the case when the user is located inside a trusted domain as defined by subclause 4.4. In this case, the AS is aware of the identity of the user and no extra actions are needed. The AS shall consider the request as authenticated.

   ii) the initial or standalone request does not contain a P-Asserted-Identity header. This is typically the case when the user is located outside a trusted domain as defined by subclause 4.4. In this case, the AS does not have a verified identity of the user. The AS shall check the From header of the initial or standalone request. If the From header value in the SUBSCRIBE request is set to "Anonymous", then the user and the request are considered as anonymous and no further actions are required. If the From header value does not indicate anonymity, then the AS shall challenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [26].

When the AS receives a SIP initial or standalone request that contains credentials but it does not contain a P-Asserted-Identity header the AS shall check the correctness of the credentials as follows:

a) If the credentials are correct, then the AS shall consider the identity of the user verified, and the AS shall consider the request as authenticated;

b) If the credentials are not correct, the AS may either rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [26] (up to a predetermined maximum number of times predefined in the AS configuration data), or consider the user as anonymous. If the user is considered anonymous, the PS shall consider the request as authenticated.

Editor's Note: It needs to be investigated whether the *maximum number of times predefined in the AS configuration data* creates a potential denial of service attack, as it requires the AS to keep states between different different authentications trials.

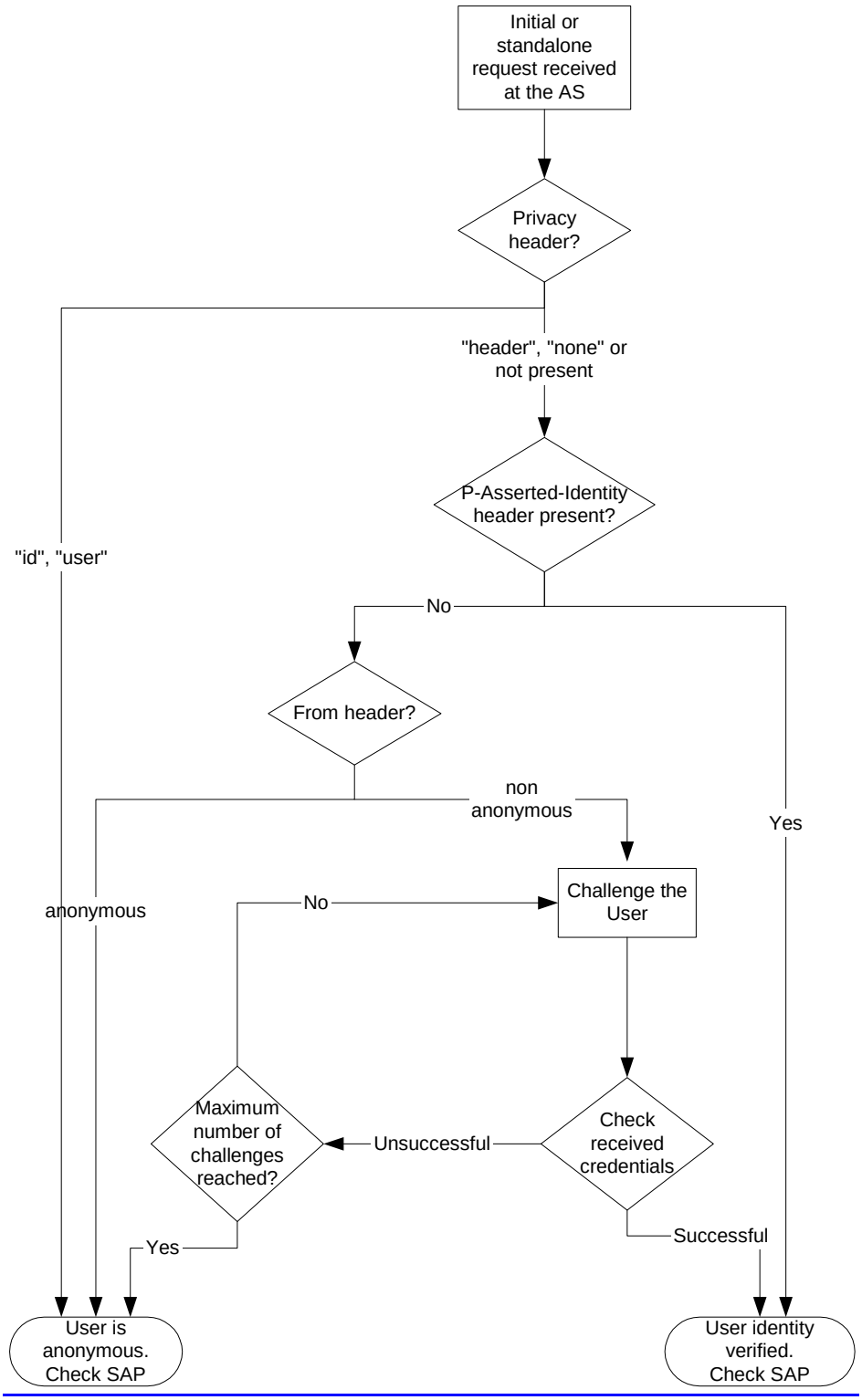

Figure 5-1: User identity verification flow at the AS

5.7.1.5 Request authorization

Once the AS have tried to verify the identity of the user, the AS either has a verified identity of the user or it considers the user as anonymous.

If the user is considered anonymous, the AS shall check whether the authorization policy defined for this request allows anonymous requests. If anonymous requests are allowed, then the AS can proceed with the requested functionality, otherwise, the AS shall not proceed with the requested functionality.

If the user is identified by an identity, the AS shall apply the authorization policy related to the requested functionality to detect whether the particular user is allowed to request the functionality. The authorization policy may require a verified identity of a user.

If the request is authorized then the AS shall continue with the procedures as defined for that request.

If the request is not authorized, the AS shall either:

- reject the request according to the procedures defined for that request e.g., by issuing a 403 (Forbidden) response; or
- send a 2xx final response if the authorization policy requires to deny the requested functionality, whilst appearing to the user as if the request has been granted.

5.7.1.6 Event notification throttling

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.

PROPOSED CHANGE

A.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status
1	User agent	[26]	o.1	o.1
2	Proxy	[26]	o.1	o.1
o.1:	It is mandatory to support exactly one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status
1	UE	5.1	n/a	o.1
2	P-CSCF	5.2	n/a	o.1
3	I-CSCF	5.3	n/a	o.1
3A	I-CSCF (THIG)	5.3	n/a	c1
4	S-CSCF	5.4	n/a	o.1
5	BGCF	5.6	n/a	o.1
6	MGCF	5.5	n/a	o.1
7	AS	5.7	n/a	o.1
7A	AS acting as terminating UA, or redirect server	5.7.2	n/a	c2
7B	AS acting as originating UA	5.7.3	n/a	c2
7C	AS acting as a SIP proxy	5.7.4	n/a	c2
7D	AS performing 3rd party call control	5.7.5	n/a	c2
8	MRFC	5.8	n/a	o.1
c1:	IF A.3/3 THEN o ELSE x - - I-CSCF.			
c2:	IF A.3/7 THEN o.2 ELSE n/a - - AS.			
o.1:	It is mandatory to support exactly one of these items.			
o.2:	It is mandatory to support at least one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

Table A.3A: Roles specific to additional capabilities

Item	Roles	Reference	RFC status	Profile status
1	Presence server	3GPP TS 24.141 [73]	n/a	c1
2	Presence user agent	3GPP TS 24.141 [73]	n/a	c2
3	Resource list server	3GPP TS 24.141 [73]	n/a	c3
4	Watcher	3GPP TS 24.141 [73]	n/a	c4
c1:	IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA.			
c2:	IF A.3/1 THEN o ELSE n/a - - UE.			
c3:	IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server.			
c4:	IF A.3/1 OR A.3/7B THEN o ELSE n/a - - UE or AS acting as originating UA.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

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	o	o
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	o
16	integration of resource management and SIP?	[30]	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
xx	an event state publication extension to the session initiation protocol?	[70]	o	c30

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.3/4 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.
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.

Table A.4A of 3GPP TS 24.229 is modified with the following additional rows (This table is added to 24.229 by a CR to the June 2004 plenary):

Item	Does the implementation support	Subscriber			Notifier		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
aa	presence package?	[8.74] 6	c1	c5	[8.74] 6	c2	c6
bb	eventlist with underlying presence package?	[8.75], [8.74] 6	c1	c7	[8.75], [8.74] 6	c2	c8
cc	presence.winfo template-package?	[8.76] 4	c1	c9	[8.76] 4	c2	c10
dd	xcap-change package?	[8.77] 2	c1	c11	[8.77] 2	c2	c12

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.
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.

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] 3	c20	c20	[70] 3	c20	c20
15B	PUBLISH response	[70] 3	c20	c20	[70] 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/xx 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			[26] 21.4.1		
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 (Precondition Failed)	[70] 7.2.1	c20	c20	[70] 7.2.1	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		
29	423 (Interval Too Brief)	[26] 21.4.17	c4	c4	[26] 21.4.17	m	m
30	480 (Temporarily Unavailable)	[26] 21.4.18			[26] 21.4.18		
31	481 (Call/Transaction Does Not Exist)	[26] 21.4.19			[26] 21.4.19		
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			[26] 21.4.26		
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		
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		

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
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			[26] 21.6.2		
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.						
c20:	IF A.4/xx THEN m ELSE n/a						

PROPOSED CHANGE – new subclause

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	o (note 1)	o (note 1)	[26] 20.19, [70] 7.1.1	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
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] 7.3.2	o	o	[70] 7.3.2	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.
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	m	m	[26] 20.19, [70] 7.1.1	m	m
4	SIP-Etag	[70] 7.3.1	m	m	[70] 7.3.1	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	m	m	[26] 20.23, [70] 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.2.2.2 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 TLS connections on the upstream side?	[26] 16.7	o	n/a
8	support of TLS connections 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	[26] 20	o	o

	response?			
	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]	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	[52] 4.3	c18	n/a

	request or response?			
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
xx	an event state publication extension to the session initiation protocol?	[70]	o	m

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] 3	c20	c20	[70] 3	c20	c20
15B	PUBLISH response	[70] 3	c20	c20	[70] 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/xx 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			[26] 21.4.1		
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 (Precondition Failed)	[70] 7.2.1	c20	c20	[70] 7.2.1	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]			[26]		

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
		21.4.16			21.4.16		
29	423 (Interval Too Brief)	[26] 21.4.17	c5	c5	[26] 21.4.17	c6	c6
30	480 (Temporarily not available)	[26] 21.4.18			[26] 21.4.18		
31	481 (Call /Transaction Does Not Exist)	[26] 21.4.19			[26] 21.4.19		
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			[26] 21.4.26		
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			[26] 21.6.2		
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.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.
c20: IF A.4/xx THEN m ELSE n/a

PROPOSED CHANGE – new subclause

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	m	m	[70] 3.6	m	m
15	Expires	[26] 20.19, [70] 7.1.1	m	m	[26] 20.19, [70] 7.1.1	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	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
34	Reject-Contact	[56B] 9.2	c27	c27	[56B] 9.2	c27	c28
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] 7.3.2	m	m	[70] 7.3.2	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).

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	m	m	[26] 20.19, [70] 7.1.1	i	i
4	SIP-Etag	[70] 7.3.1	m	m	[70] 7.3.1	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	m	m	[26] 20.23, [70] 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 #34 **Tdoc N1-041066**

Zagreb, Croatia 10 – 14 May 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **652** ⌘ **rev** **-** ⌘ Current version: **6.2.0** ⌘

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

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

Title:	⌘	Creation of separate event package table for UA role
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2, PRESNC
Date:	⌘	12/05/2004
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:

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:	⌘	IETF is defining a number of structures for message bodies used in NOTIFY requests called event packages. These are defined for use between subscriber and notifier, and their support does not conveniently fit into table A.4 defining major capabilities as the support for both ends is different. The capabities need to be defined for the UA role only, as the packages are not seen by the proxy role. This table is expected to be used substantially for further extensions for conferencing and presence, but this usage is covered in other and future CRs.
Summary of change:	⌘	A new table A.4A is added to the profile summarizing the event packages that may be used by any UA role. This table is used in this document to describe the reg-event package. An error in table A.4 is also corrected related to the support of RFC 3265, where the P-CSCF is added to the list of entities which mandatorily support the extension, because the P-CSCF must support reg event.
Consequences if not approved:	⌘	Support of event packages will not be adequately documented.

Clauses affected:	⌘	A.2.1.2

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

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

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	o	o
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	o
16	integration of resource management and SIP?	[30]	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 assistance of intermediaries are obscured?	[33] 5.1	c10	c27
26E	application of the privacy option "session" such that anonymization for	[33] 5.2	c10	c27

	the session(s) initiated by this message occurs?			
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

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.
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	c5	c5	[36] 3	c5	c5

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.4/15 THEN m ELSE n/a - - the REFER method.