3GPP TSG CN Plenary Meeting #22 **NP-030482**
10th - 12th December 2003. Hawaii, USA.

Source: **TSG CN WG 1**

Title: **CRs to Rel-6 on Work Item IMS2 towards 24.229 and 23.218**

Agenda item: **9.1**

Document for: **APPROVAL**

Introduction:

This document contains **8** CRs, **Rel-6** Work Item **"IMS2"**, that have been agreed by **TSG CN WG1 in CN1#32 meeting**, and are forwarded to TSG CN Plenary meeting #22 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	Rel
N1-031468	Corrections on charging specification number	23.218	059		F	5.6.0	Rel-6
N1-031627	Registration amendments in profile	24.229	487	1	F	6.0.0	Rel-6
N1-031351	Privacy considerations for the UE	24.229	489		F	6.0.0	Rel-6
N1-031375	Correction of I-CSCF handling of multiple private user identities with same public user identity	24.229	494		F	6.0.0	Rel-6
N1-031378	Addition of reference to Gq interface	24.229	497		F	6.0.0	Rel-6
N1-031392	Unavailable definitions	24.229	507		F	6.0.0	Rel-6
N1-031681	Profile support of RFC 3326: The Reason Header Field for the Session Initiation Protocol	24.229	518	1	B	6.0.0	Rel-6
N1-031439	Profile support of RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing	24.229	519		B	6.0.0	Rel-6

3GPP TSG-CN1 Meeting #32
Bangkok, Thailand, 27- 31 October, 2003

Tdoc N1-031468

CR-Form-v7

CHANGE REQUEST

⌘ **23.218** **CR** **059** ⌘**rev** **-** ⌘ Current version: **5.6.0** ⌘

*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 **X**

Title:	⌘	Corrections on charging specification number
Source:	⌘	NEC Corporation
Work item code:	⌘	IMS2
Date:	⌘	18/10/2003
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

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

Reason for change:	⌘	The charging specifications for rel6 are restructured, taken into account the emerging services for rel6 onwards. 23.218 needs to be aligned accordingly.
Summary of change:	⌘	Stage2 IMS related charging specification number is changed from TS32.200 to TS32.240. Stage3 IMS charging specification number is changed from TS32.225 to TS32.260.
Consequences if not approved:	⌘	Inconsistency is remained between 23.218 and charging specifications.

Clauses affected:	⌘	2, 12

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

Other comments:	⌘	

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

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

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

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

Start of first change

2 References

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

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

[1] Void.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[20] 3GPP TS 32.~~200~~240: "Telecommunication management; Charging management; Charging architecture and principles ~~Charging management; Charging principles~~".

[21] 3GPP TS 32.~~225~~260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging ~~Charging management; Charging data description for the IP Multimedia subsystem~~".

End of first change

Start of second change

12. IP multimedia session handling with an Charging Server

This clause describes the functional architecture needed to support interactions with the S-CSCF in the IP Multimedia Subsystem and Charging Server. The Charging Server is a specific SIP Application Server that performs the role of online charging mechanism for the Event Charging Function (ECF) and Session Charging Function (SCF).

The detailed procedures for Charging Server are specified in 3GPP TS 32.~~200~~ 240 [20] and 3GPP TS 32.~~225~~ 260 [21].

End of second change

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031627**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **487** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Registration amendments in profile
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	30/09/2003
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Table A.4 (Major capabilities for the UA) currently defines the client behaviour for registration (item A.4/1) as mandatory under the RFC status column. Since this value was set, there have been some major changes prior to the publication of RFC 3261, and it would now be a better representation of RFC 3261 to represent this as optional (o). Additionally in this table, support of the registrar capability at the AS is currently indicated as mandatory, and the text in 5.7.1.1 clearly indicates this as optional for an AS. (The equivalent support at the S-CSCF for sending the REGISTER is mandatory according to 4.1 and 5.4.1.2.2). Table A.5 (Supported methods for the UA) currently has entries for the REGISTER method in the RFC status column which are incorrect given that a registrar is a UA, and can therefore receive REGISTER requests and send REGISTER responses. The profile status column is currently empty and these need to be specified in 3GPP. More specifically these entries should be related back to the major capabilities defined in Table A.4. It is believed that the proxy entries (no capabilities defined in table A.162, and the status of mandatory to send and receive in table A.163) are correct, and no change is required in this area.
Summary of change:	⌘	In table A.4 item A.4/1 the RFC status entry is changed from mandatory to optional. The contents of c4 are amended to demonstrate the optional support at the AS. In table A.5, item A.5/18 and item A.5/19, the send and receive status are made dependent on new conditionals which relate back to table A.4. These new conditionals are defined at the bottom of the table.
Consequences if	⌘	Incomplete / incorrect specification

not approved:	

Clauses affected:	⌘	A.2.1.2, A.2.1.3			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

A.2 Profile definition for the Session Initiation Protocol as used in the present document

A.2.1 User agent role

A.2.1.1 Introduction

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations:

Prerequisite: A.2/1 - - user agent role.

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~~m~~	c3
2	registrar?	[26] subclause 10.3	o	c4
2A	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	[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	
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	
26F	application of the privacy option "user"	[33] 5.3	c10	

	such that user level privacy functions are provided by the network?			
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

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 ~~OR A.3/7~~ 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.3/4 THEN m ELSE (IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - S-CSCF or 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 o A3./4 THEN m ELSE n/a – UE or S-CSCF
c18:	IF A.4/2A THEN m ELSE n/a - - initiating sessions
c19:	IF A.4/2A 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.
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.

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	m	m	[26] 13	m	m
2	BYE request	[26] 15.1	o		[26] 15.1	o	
3	BYE response	[26] 15.1	o		[26] 15.1	o	
4	CANCEL request	[26] 9	o		[26] 9	o	
5	CANCEL response	[26] 9	o		[26] 9	o	
8	INVITE request	[26] 13	m	m	[26] 13	m	m
9	INVITE response	[26] 13	m	m	[26] 13	m	m
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
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	~~o~~c8	c8	[26] 10	~~n/a~~c9	c9
19	REGISTER response	[26] 10	~~n/a~~c9	c9	[26] 10	~~m~~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.

Editor's note: Optional status of BYE in RFC status is given because RFC states SHOULD (client and server).

~~Editor's note: Optional status of REGISTER in RFC status is given because RFC states RECOMMENDED (client); for the UAS, not statement is made, but it is assumed that this therefore means n/a.~~

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031351**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **489** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Privacy considerations for the UE
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2-~~CCR~~
Date:	⌘	30/09/2003
Category:	⌘	F ~~A~~
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:	⌘	RFC 3323 clause 4.1 specifies additional considerations that relate to identity of the user being revealed by other headers, over and above the guidelines given in RFC 3261. As this information is critical to ensuring privacy, it is considered that a note giving this specific reference would be useful at both the originating and terminating side.
Summary of change:	⌘	Addition of notes referencing RFC 3323 considerations. Additionally, in subclause 5.1.2A.1, last paragraph, the term "protected port" is used. It is believed that here what is meant is the defined term "protected server port" and therefore that term is substituted
Consequences if not approved:	⌘	Insufficient guidance to implementors.

Clauses affected:	⌘	5.1.2A.1, 5.1.2A.2

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

Other comments:	⌘	This information was removed from a previous proposed CR, based on an objection that this consistutes one of the options of privacy, and therefore was an issue needing to be resolved as to which options were supported in release 5. However this is not one of the options of privacy; it appears in a different clause to the options, and these considerations apply to all usage of the privacy draft.

How to create CRs using this form:

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

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

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

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

5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

5.1.2A.1 Mobile-originating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE shall discard any SIP message that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Preferred-Identity header:

- a public user identity which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

NOTE 3: A number of headers can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

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

NOTE 4~~3~~: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected server port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

5.1.2A.2 Mobile-terminating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

The UE shall discard any SIP message that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 1: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

NOTE 2: A number of headers can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031375**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **494** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Correction of I-CSCF handling of multiple private user identities with same public user identity
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	01/10/2003
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change: ⌘
- At the last meeting we agreed a note in subclause 5.3.1.2 (CR473) that contained non standard terminology to 24.229, and for which the meaning was not clear, as raised by subsequent queries on the CN1 mailing list.
- As regards the term "IMS public user identity", the defined term is just plain "public user identity" and the use of "IMS" in front of it implies a degree of multiple types of public user identity that just does not exist. Therefore the "IMS" should be stripped off, because it is not an appropriate part of the term.
- CR473 introduced text in subclause 5.4.3.3 relating to the use of the qvalue parameter (RFC 3261 style of referring to). Changes are made to align to the RFC 3261 style.
- CR473 also introduced into 24.229 the concept of supporting more than one registration of public user identity at the S-CSCF. It is believed that this is appropriately represented by an entry in the major capabilities tables, in addition to that which represents the ability to do a parallel search on qvalue, i.e. forking. It is assumed that this is an optional capability at release 6.
- This CR proposed revised text which resolves these problems.

Summary of change: ⌘ The note is revised. A new major capability is added for the registrar.

Consequences if not approved: ⌘ Unclear specification

Clauses affected: ⌘ 5.3.1.2, 5.4.3.3, A.2.1.2

		Y	N		
Other specs	⌘		X	Other core specifications	⌘

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

How to create CRs using this form:

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

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

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

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

5.3 Procedures at the I-CSCF

5.3.1 Registration procedure

5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

5.3.1.2 Normal procedures

When I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

NOTE: Different UEs, each with its own private user identity, ~~One IMS user~~ may register the same ~~IMS~~ public user identity ~~from different terminals~~. ~~These registrations from the same user~~ Registrations for the same shared public user identity are directed to the same S-CSCF as described in 3GPP TS 29.228 [14].

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;

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

3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;

2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;

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

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

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

5.4.3.3 Requests terminated at the served user

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

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

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

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

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

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

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

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

5) insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

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

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

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

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

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

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

9) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2. Furthermore, the S-CSCF shall:

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

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall either fork the request or perform sequential search based on the relative preference indicated by the ~~q value~~qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no ~~q~~ qvalue parameter was provided, the S-CSCF shall look into the user profile of the user to find the indication about the default handling of the request;

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

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

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

11) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

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

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

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

2) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that

the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14]; and

3) execute the procedure described in step 4, 5, 6, 7, 8, 9, 11 and 12 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

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

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

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

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

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

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS.

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

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

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

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

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

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

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

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

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

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

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

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

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	m	c3
2	registrar?	[26] subclause 10.3	o	c4
2B	registration of multiple contacts for a single address of record	[26] 10.2.1.2, 16.6	o	o
2A	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	[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	
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message	[33] 5.2	c10	

	occurs?			
26F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	c10	
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

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 OR A.3/7 THEN m 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.3/4 THEN m ELSE (IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - S-CSCF or 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 o A3./4 THEN m ELSE n/a – UE or S-CSCF
c18:	IF A.4/2A THEN m ELSE n/a - - initiating sessions
c19:	IF A.4/2A 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.
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.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031378**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **497** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Addition of reference to Gq interface
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	02/10/2003
Category:	⌘	F ~~D~~
Release:	⌘	Rel-6

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

Use one of the following releases:

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:	⌘	At CN1#31 we approved a CR (CR465R1, N1-031267, NP-030418) that added the Gq interface to various clauses. At one of these points it is also appropriate to insert a reference to the specification defining the Gq interface, for which a number has now been allocated.
Summary of change:	⌘	Addition of reference to references clause. Addition of pointer to that reference in subclause 7.2A.5.2.
Consequences if not approved:	⌘	Unclear reference for Gq.
Clauses affected:	⌘	2, 7.2A.5.2

	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.

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 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

[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".

[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] draft-ietf-sip-scvrtdisco-04 (May 2003): "Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration".

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

[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".

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

7.2A.5 P-Charging-Vector header

7.2A.5.1 Introduction

The P-Charging-Vector header is is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

7.2A.5.2 Syntax

The P-Charging-Vector header field has the syntax described in RFC 3455 [52]. Table 7.3 describes extensions required for 3GPP to that syntax.

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
access-network-charging-info = (gprs-charging-info / generic-param)
gprs-charging-info = ggsn *(SEMI pdp-info) [SEMI extension-param]
ggsn = "ggsn" EQUAL gen-value
pdp-info = pdp-sig SEMI gcid SEMI auth-token *(SEMI flow-id)
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "gcid" EQUAL gen-value
auth-token = "auth-token" EQUAL gen-value
flow-id = "flow-id" EQUAL gen-value
extension-param = token [EQUAL (token | quoted-string)]
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header

The access-network-charging-info parameter includes alternative definitions for different types access networks.

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter) and one or more PDP contexts (pdp-info parameter). Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), a media authorization token (auth-token parameter) and one or more flow identifiers (flow-id parameter) that identify associated m-lines within the SDP from the SIP signalling. These parameters are transferred from the GGSN to the P-CSCF via the PDF over the Go interface (see 3GPP TS 29.207 [12]) and Gq interface~~s, see 3GPP TS 29.207 [12]~~ (see 3GPP TS 29.209 [13A].

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

7.2A.5.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031392**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **507** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Unavailable definitions
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2-~~CCR~~
Date:	⌘	09/10/03
Category:	⌘	F ~~A~~
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 TS 24.229 there are no definitions for USIM and ISIM, and no generic reference in the definitions clause to a specification that might include them (no text of the form "all definitions included in…"). As the concepts of USIM and ISIM are fundamental to the security of information held in the UE, and which is then used within SIP, it is important that these terms are defined in this specification. Such definition can be performed by reference, and it is proposed that this is the mechanism used. Additionally the term MRFP is used extensively throughout the document and this term would benefit from an appropriate referenced definition.
Summary of change:	⌘	In subclause 3.1, the terms USIM, ISIM and MRFP are defined by reference to 3GPP TR 21.905. As a result of adding these definitions, it has been discovered that the expansion of the related abbreviations USIM and ISIM is incorrect, at least according to the references chosen containing definitions. Subclause 3.2 has therefore been amended. Similarly, the expansion of the abbreviation MRFC in the scope is also found to be incorrect, and this is corrected.
Consequences if not approved:	⌘	Without formal definition of the term USIM and ISIM, the reader to free to take any meaning they like for these terms, which may or may not include the security requirements associated with the 3GPP definition used elsewhere.

Clauses affected:	⌘	1, 3.1, 3.2

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

How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

1 Scope

The present document defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP).

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);
- the interface between the CSCF and any other CSCF;
- the interface between the CSCF and an Application Server (AS);
- the interface between the CSCF and the Media Gateway Control Function (MGCF);
- the interface between the S-CSCF and the ~~Media~~ Multimedia Resource Function Controller (MRFC)
- the interface between the CSCF and the Breakout Gateway Control Function (BGCF);
- the interface between the BGCF and the MGCF;
- the interface between the BGCF and any other BGCF; and
- the interface between the CSCF and an external Multimedia IP network.

Where possible the present document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of SIP and SDP. Where this is not possible, extensions to SIP and SDP are defined within the present document. The document has therefore been structured in order to allow both forms of specification.

NOTE: The present document covers only the usage of SIP and SDP to communicate with the enitities of the IM CN subsystem. It is possible, and not precluded, to use the capabilities of GPRS to allow a terminal containing a SIP UA to communicate with SIP servers or SIP UAs outside the IM CN subsystem, and therefore utilise the services provided by those SIP servers. The usage of SIP and SDP for communicating with SIP servers or SIP UAs outside the IM CN subsystem is outside the scope of the present document.

PROPOSED CHANGE

3 Definitions and abbreviations

3.1 Definitions

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

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

Fully-Qualified Domain Name (FQDN)

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

Back-to-Back User Agent (B2BUA)
Client

Dialog
Final response
Header
Header field
Loose routeing
Method
Option-tag (see RFC 3261 [26] subclause 19.2)
Provisional response
Proxy, proxy server
Redirect server
Registrar
Request
Response
Server
Session
(SIP) transaction
Stateful proxy
Stateless proxy
Status-code (see RFC 3261 [26] subclause 7.2)
Tag (see RFC 3261 [26] subclause 19.3)
Target Refresh Request
User agent client (UAC)
User agent server (UAS)
User agent (UA)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

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

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

Filter criteria
Initial filter criteria
Initial request
Standalone transacation
Subsequent request

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

Interrogating-CSCF (I-CSCF)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

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

IM Suscriber Identity Module (ISIM)
Protected ~~Server~~ server ~~Port~~port
Protected ~~Client~~ client ~~Port~~port

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

User Equipment (UE)

Universal Subscriber Identity Module (USIM)

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

Security association

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

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

International public telecommunication number

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
APN	Access Point Name
AUTN	Authentication TokeN
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional
CCF	Charging Collection Function
CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTD	Document Type Definition
ECF	Event Charging Function
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HSS	Home Subscriber Server
i	irrelevant
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia core network Subsystem
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifier
IP	Internet Protocol
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP multimedia Subsystem Service Control
ISIM	~~IMS~~ IM Suscriber Identity Module
m	mandatory
MAC	Message Authentication Code
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Media Gateway
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller

MRFP	Multimedia Resource Function Processor
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
n/a	not applicable
NAI	Netework Access Identifier
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SGSN	Serving GPRS Support Node
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Universal Resource Identifier
URL	Universal Resource Locator
USIM	~~UMTS~~ Universal Subscriber Identity Module
x	prohibited
XMAC	expected MAC
XML	eXtensible Markup Language

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031681**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **518** ⌘ **rev** **1** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Profile support of RFC 3326: The Reason Header Field for the Session Initiation Protocol
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	13/10/2003
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: ⌘ RFC 3326 extends SIP by means of a new header valid in requests. This document has become available subsequent to the release 5 freeze date, and the operation does not form an essential part of release 5. However, the functionality is considered by previous decision of CN1 to be useful for inclusion in the IM CN subsystem (IETF dependencies discussions), and therefore it is proposed to be included in release 6 functionality, with a support identical to that given for IETF.

Summary of change: ⌘

IETF requirements

Where the "The Reason Header Field for the Session Initiation Protocol" extension is supported, the header is allowed in all requests. It is optional for clients to include the header in requests, and optional for a server to understand such received headers in requests.

While the specification makes provision for the header to appear in responses, it clearly states that it can only appear in such responses where the status code has been defined to allow it. No such status code has so far been defined, and therefore currently the header is not allowed in responses.

3GPP requirements

Current decisions within 3GPP WG CN1 state that this specification is regarded as useful for use in 3GPP, but no explicit specification is made for its use. As such, as specified for IETF and included within the profile, it is generally available for any UA to use (User agent, Application server).

	A question lies over the use for the MGCF. The MGCF is a user agent. Discussions within CN3 have lead to the conclusion that the mapping specification will not document a mapping from cause values to the Reason header. There is this no specified issue why the Reason header should be sent or received by the MGCF. However CN3 did not wish to explicitly preclude an MGCF handling the Reason header in any proprietary fashion. The MGCF is therefore specified as for the UE handling, but with the addition of a note stating that this is not covered in the interworking specifications. Additionally, it should be noted that occasionally other entities that normally act as proxies can source and sink requests. These are typically the REGISTER request, and the SUBSCRIBE and NOTIFY requests. While we do not normally expect to see the Reason header occurring in these circumstances, there does not seem to be a great deal of point in explicitly precluding it from these methods, especially as we have not explicitly precluded other end-to-end headers (e.g. Organization) under similar circumstances. Thus if an implementor can really think of a use for it, then we propose that 24.229 will not prevent it happening. We consider the argument for this is different from that relating to the support in the MGCF, as the MGCF functionality should only respond to headers, and generate headers, as a result of interworking functionality. Further, in the examples given, one shows the use by a proxy in the case of a forked request. The proxy sends a CANCEL to the unsuccessful UAS, the CANCEL containing a Reason header. In this case it is probably best considered that the forking proxy is acting as a UA to send the CANCEL request. As such it will be found that this is perfectly legitimate behaviour for a user agent, and no further entries are required in the SIP profile. Note that if identification of this additional behaviour is considered to be important, then a better representation would be to place an additional new capability in the major capabilities table.
Consequences if not approved: ⌘	The reader of 3GPP TS 24.229 will not know the level of support required to be implemented for this header, despite it being a published part of the range of SIP specifications.

Clauses affected: ⌘	2, A.2				
Other specs affected: ⌘	**Y**	**N**		⌘	
		X	Other core specifications		
		X	Test specifications		
		X	O&M Specifications		
Other comments: ⌘	In table A.165, the Privacy header is incorrectly positioned in the table, and this interferes with placing and correctly numbering the Reason header. As part of this CR, this header is therefore placed in the correct location, with no technical change. In table A.181, the item numbering is aligned with the equivalent UA table for consistency.				

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".

[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 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

[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] draft-ietf-sip-scvrtdisco-04 (May 2003): "Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration".

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

[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".

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

PROPOSED CHANGE

A.2 Profile definition for the Session Initiation Protocol as used in the present document

A.2.1 User agent role

A.2.1.1 Introduction

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations:

Prerequisite: A.2/1 - - user agent role.

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	m	c3
2	registrar?	[26] subclause 10.3	o	c4
2A	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	[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	
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	
26F	application of the privacy option "user"	[33] 5.3	c10	

	such that user level privacy functions are provided by the network?			
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)

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 OR A.3/7 THEN m 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.3/4 THEN m ELSE (IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - S-CSCF or 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 o A3./4 THEN m ELSE n/a – UE or S-CSCF
c18:	IF A.4/2A THEN m ELSE n/a - - initiating sessions
c19:	IF A.4/2A 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.
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.
NOTE 1:	At the MGCF, the interworking specifications do not support a handling of the header associated with this extension.

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	m	m	[26] 13	m	m
2	BYE request	[26] 15.1	o		[26] 15.1	o	
3	BYE response	[26] 15.1	o		[26] 15.1	o	
4	CANCEL request	[26] 9	o		[26] 9	o	
5	CANCEL response	[26] 9	o		[26] 9	o	
8	INVITE request	[26] 13	m	m	[26] 13	m	m
9	INVITE response	[26] 13	m	m	[26] 13	m	m
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
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	o		[26] 10	n/a	
19	REGISTER response	[26] 10	n/a		[26] 10	m	
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.						

Editor's note: Optional status of BYE in RFC status is given because RFC states SHOULD (client and server).

Editor's note: Optional status of REGISTER in RFC status is given because RFC states RECOMMENDED (client); for the UAS, not statement is made, but it is assumed that this therefore means n/a.

A.2.1.4 PDU parameters

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		
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		
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		

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

A.2.1.4.2 ACK method

Prerequisite A.5/1 – ACK request

Table A.7: Supported headers within the ACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
7	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
8	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	o	o	[26] 20.15	m	m
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
13	From	[26] 20.20	m	m	[26] 20.20	m	m
14	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
15	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
15A	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
16	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
17	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
17A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
18	Require	[26] 20.32	o	o	[26] 20.32	m	m
19	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
20	Timestamp	[26] 20.38	c7	c7	[26] 20.38	m	m
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o	o	[26] 20.41	m	m
23	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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c7:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c8:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						

Editor's note: Is the following table a suitable way of showing the contents of message bodies.

Prerequisite A.5/1 – ACK request

Table A.8: Supported message bodies within the ACK request

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

A.2.1.4.3 BYE method

Prerequisite A.5/2 - - BYE request

Table A.9: Supported headers within the BYE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
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	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
16	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
16A	P-Access-Network-Info	[52] 4.4	c9	c10	[52] 4.4	c9	c11
16B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
16C	P-Charging-Function-Addresses	[52] 4.5	c13	c14	[52] 4.5	c13	c14
16D	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c12	n/a
16E	P-Preferred-Identity	[34] 9.2	c6	x	[34] 9.2	n/a	n/a
16F	Privacy	[33] 4.2	c7	n/a	[33] 4.2	c7	c7
17	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
18	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
18A	Reason	[34A] 2	c17	c17	[34A] 2	c17	c17
19	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
20	Require	[26] 20.32	o	o	[26] 20.32	m	m
21	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
21A	Security-Client	[48] 2.3.1	c15	c15	[48] 2.3.1	n/a	n/a
21B	Security-Verify	[48] 2.3.1	c16	c16	[48] 2.3.1	n/a	n/a
22	Supported	[26] 20.37	o	o	[26] 20.37	m	m
23	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
24	To	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
26	Via	[26] 20.42	m	m	[20] 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.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c10: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c11: 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.
c12: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c13: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c14: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15: IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note).
c16: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c17: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.

NOTE:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/2 - - BYE request

Table A.10: Supported message bodies within the BYE request

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

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.11: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/3 - - BYE response

Table A.12: Supported headers within the BYE 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	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c6
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c10	[52] 4.5	c9	c10
10D	P-Charging-Vector	[52] 4.6	c8	n/a	[52] 4.6	c8	n/a
10E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10F	Privacy	[33] 4.2	c4	n/a	[33] 4.2	c4	c4
10G	Require	[26] 20.32	m	m	[26] 20.32	m	m
10H	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	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.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	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.5/3 - - BYE response

Prerequisite: A.6/6 - - 2xx

Table A.13: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
4	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.5/3 - - BYE 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.14: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
0B	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
1	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.5/3 - - BYE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.15: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/3 - - BYE 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.16: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/3 - - BYE response

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

Table A.17: Supported headers within the BYE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/19 - - 407 (Proxy Authentication Required)

Table A.18: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	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.5/3 - - BYE response

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

Table A.19: Supported headers within the BYE 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
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/3 - - BYE response

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

Table A.20: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/3 - - BYE response

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

Table A.20A: Supported headers within the BYE 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
3	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.5/3 - - BYE response

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

Table A.21: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/3 - - BYE response

Table A.22: Supported message bodies within the BYE response

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

A.2.1.4.4 CANCEL method

Prerequisite A.5/4 - - CANCEL request

Table A.23: Supported headers within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
9	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
10	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
14	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
15	Reason	[34A] 2	c7	c7	[34A] 2	c7	c7
16	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
18	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
19	Supported	[26] 20.37	o	o	[26] 20.37	m	m
20	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o		[26] 20.41	o	
23	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.
c6: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.

Prerequisite A.5/4 - - CANCEL request

Table A.24: Supported message bodies within the CANCEL request

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

Prerequisite A.5/5 - - CANCEL response

Table A.25: Supported headers within the CANCEL response - all 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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	Privacy	[33] 4.2	c3	n/a	[33] 4.2	c3	n/a
6	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
7	To	[26] 20.39	m	m	[26] 20.39	m	m
7A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
8	Via	[26] 20.42	m	m	[26] 20.42	m	m
9	Warning	[26] 20.43	o (note)	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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
NOTE:	For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/5 - - CANCEL response

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

Table A.26: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.27: Supported headers within the CANCEL response

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

Prerequisite A.5/5 - - CANCEL response

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

Table A.28: Supported headers within the CANCEL response

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

Prerequisite A.5/5 - - CANCEL response

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

Table A.30: Supported headers within the CANCEL response

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

Prerequisite A.5/5 - - CANCEL response

Table A.31: Supported message bodies within the CANCEL response

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

A.2.1.4.5 COMET method

Void

A.2.1.4.6 INFO method

Void

A.2.1.4.7 INVITE method

Prerequisite A.5/8 - - INVITE request

Table A.46: Supported headers within the INVITE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
4	Alert-Info	[26] 20.4	o	o	[26] 20.4	c1	c1
5	Allow	[26] 20.5, [26] 5.1	o (note 1)	o	[26] 20.5, [26] 5.1	m	m
6	Allow-Events	[28] 7.2.2	c2	c2	[28] 7.2.2	c2	c2
8	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
9	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
10	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
11	Contact	[26] 20.10	m	m	[26] 20.10	m	m
12	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
13	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
14	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
17	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
19	Expires	[26] 20.19	o	o	[26] 20.19	o	o
20	From	[26] 20.20	m	m	[26] 20.20	m	m
21	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
23	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
24	Organization	[26] 20.25	o	o	[26] 20.25	o	o
24A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
24B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c7	c7
24C	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
24D	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
24E	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
25	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
25A	P-Preferred-Identity	[34] 9.2	c7	c5	[34] 9.2	n/a	n/a
25B	P-Visited-Network-ID	[52] 4.3	x (note 3)	x	[52] 4.3	c14	n/a
26	Priority	[26] 20.26	o	o	[26] 20.26	o	o
26A	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
27	Proxy-Authorization	[26] 20.28	c6	c6	[26] 20.28	n/a	n/a
28	Proxy-Require	[26] 20.29	o (note 2)	o (note 2)	[26] 20.29	n/a	n/a
28A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
29	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
31	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
32	Require	[26] 20.32	o	m	[26] 20.32	m	m
33	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
33A	Security-Client	[48] 2.3.1	c22	c22	[48] 2.3.1	n/a	n/a
33B	Security-Verify	[48] 2.3.1	c23	c23	[48] 2.3.1	n/a	n/a
34	Subject	[26] 20.36	o	o	[26] 20.36	o	o
35	Supported	[26] 20.37	c8	m	[26] 20.37	m	m
36	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
37	To	[26] 20.39	m	m	[26] 20.39	m	m
38	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
39	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/12 THEN m ELSE n/a - - downloading of alerting information.						
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.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.						
c6:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.						
c7:	IF A.4/25 THEN o ELSE n/a - - 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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c10:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c11:	IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.						
c12:	IF A.3/1 THEN m ELSE n/a - - UE.						
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.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 4).						
c23:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						
o.1:	At least one of these shall be supported.						
NOTE 1:	The strength of this requirement in RFC 3261 [26] is RECOMMENDED, rather than OPTIONAL.						
NOTE 2:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.						
NOTE 3:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.						
NOTE 4:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].						

Prerequisite A.5/8 - - INVITE request

Table A.47: Supported message bodies within the INVITE request

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

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.48: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/9 - - INVITE response

Table A.49: Supported headers within the INVITE 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
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
11B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
11C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c11	c11
11D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
11E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
11F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
11G	Require	[26] 20.32	m	m	[26] 20.32	m	m
11H	Server	[26] 20.35	o	o	[26] 20.35	o	o
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	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.5/9 - - INVITE response

Prerequisite: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 - - 1xx

Table A.50: Supported headers within the INVITE 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
4	Contact	[26] 20.10	o	m	[26] 20.10	m	m
6	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
9	Rseq	[27] 7.1	c2	m	[27] 7.1	c3	m
11	Supported	[26] 20.37	o	o	[26] 20.37	m	m
c2:	IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP.						
c3:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP.						
c11:	IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.						
c12:	IF A.3/1 THEN m ELSE n/a - - UE.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/6 - - 2xx

Table A.51: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
2	Allow	[26] 20.5	o (note 1)	o	[26] 20.5	m	m
4	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
6	Contact	[26] 20.10	m	m	[26] 20.10	m	m
8	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
9	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
13	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.						
c11:	IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.						
c12:	IF A.3/1 THEN m ELSE n/a - - UE.						
NOTE 1:	The strength of this requirement in RFC 3261 [26] is RECOMMENDED, rather than OPTIONAL.						

Prerequisite A.5/9 - - INVITE 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.52: Supported headers within the INVITE 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
4	Contact	[26] 20.10	o (note 1)	o	[26] 20.10	m	m
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.53: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	c3	c3
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
13	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
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.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9 - - INVITE response

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

Table A.54: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9 - - INVITE response

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

Table A.55: Supported headers within the INVITE response

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

Prerequisite A.5/9 - - INVITE response

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

Table A.56: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
11	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.5/9 - - INVITE response

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

Table A.57: Supported headers within the INVITE 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
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
6	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
11	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9 - - INVITE response

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

Table A.58: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9 - - INVITE response

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

Table A.58A: Supported headers within the INVITE 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
3	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.5/9 - - INVITE response

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

Table A.59: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/42 - - 500 (Server Internal Error)

Table A.60: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
8	Retry-After	[26] 20.33	m	m	[26] 20.33	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/45 - - 503 (Service Unavailable)

Table A.61: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9 - - INVITE response

Table A.62: Supported message bodies within the INVITE response

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

A.2.1.4.7A MESSAGE method

Prerequisite A.5/9A - - MESSAGE request

Table A.62A: Supported headers within the MESSAGE request

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] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
6	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
7	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
8	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 29.15	m	m
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
13	Expires	[26] 20.19	o	o	[26] 20.19	o	o
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
17	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
18	Organization	[26] 20.25	o	o	[26] 20.25	o	o
18A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c16
18B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c11	c11
18C	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
18D	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
18E	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
18F	P-Preferred-Identity	[34] 9.2	c11	c7	[34] 9.2	n/a	n/a
18G	P-Visited-Network-ID	[52] 4.3	x (note 1)	x	[52] 4.3	c14	n/a
19	Priority	[26] 20.26	o	o	[26] 20.26	o	o
19A	Privacy	[33] 4.2	c12	c12	[33] 4.2	c12	c12
20	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
21	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
21A	Reason	[34A] 2	c6	c6	[34A] 2	c6	c6
22	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
23	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
24	Require	[26] 20.32	c8	o	[26] 20.32	m	m
25	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
25A	Security-Client	[48] 2.3.1	c22	c22	[48] 2.3.1	n/a	n/a
25B	Security-Verify	[48] 2.3.1	c23	c23	[48] 2.3.1	n/a	n/a
26	Subject	[26] 20.35	o	o	[26] 20.36	o	o
27	Supported	[26] 20.37	c9	m	[26] 20.37	m	m
28	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m
29	To	[26] 20.39	m	m	[26] 20.39	m	m
30	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
31	Via	[26] 20.42	m	m	[26] 20.42	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
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.162/8A THEN m ELSE i - - authentication between UA and proxy.						
c6:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						
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.4/14 THEN o.1 ELSE o - - Reliable transport.						
c9:	IF IF A.4/14 THEN o.1 ELSE o - - support of reliable transport.						
c10:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
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.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 2).						
c23:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						
NOTE 1:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.						
NOTE 2:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].						

Prerequisite A.5/9A - - MESSAGE request

Table A.62B: Supported message bodies within the MESSAGE request

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

Prerequisite A.5/9B - - MESSAGE response

Table A.62C: Supported headers within the MESSAGE 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] 20.9	o	o	[26] 20.9	o	o
3	Content-Disposition	[26] 20.11	o (note 2)	o (note 2)	[26] 20.11	m (note 2)	m (note 2)
4	Content-Encoding	[26] 20.12	o (note 2)	o (note 2)	[26] 20.12	m (note 2)	m (note 2)
5	Content-Language	[26] 20.13	o (note 2)	o (note 2)	[26] 20.13	m (note 2)	m (note 2)
6	Content-Length	[26] 20.14	m (note 2)	m (note 2)	[26] 20.14	m (note 2)	m (note 2)
7	Content-Type	[26] 20.15	m (note 2)	m (note 2)	[26] 20.15	m (note 2)	m (note 2)
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
12A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
12B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
12C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
12D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
12E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
12F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
12G	Require	[26] 20.32	o	o	[26] 20.32	m	m
13	Server	[26] 20.35	o	o	[26] 20.35	o	o
14	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
15	To	[26] 20.39	m	m	[26] 20.39	m	m
16	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
17	Via	[26] 20.42	m	m	[26] 20.42	m	m
18	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 1: For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.
NOTE 2: RFC 3428 [50] clause 7 states that all 2xx class responses to a MESSAGE request must not include any body, therefore for 2xx responses to the MESSAGE request the values on Sending side for "RFC status" and "Profile status" are "x", the values for Receiving side for "RFC status" and "Profile Status" are "n/a". RFC 3261 [26] subclause 7.4 states that all responses may contain bodies, therefore for all responses to the MESSAGE request other than 2xx responses, the values on Sending side for "RFC status" and "Profile status" are "o", the values for Receiving side for "RFC status" and "Profile Status" are "m".

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/6 - - 2xx

Table A.62D: Supported headers within the MESSAGE 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
4	Supported	[26] 20.37	o	o	[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.5/9B - - MESSAGE 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.62E: Supported headers within the MESSAGE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.62F: Supported headers within the MESSAGE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	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.5/9B - - MESSAGE 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.62G: Supported headers within the MESSAGE 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
4	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62H: Supported headers within the MESSAGE 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
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62I: Supported headers within the MESSAGE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	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.5/9B - - MESSAGE response

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

Table A.62J: Supported headers within the MESSAGE 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
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62K: Supported headers within the MESSAGE 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
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62L: Supported headers within the MESSAGE 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.5/9B - - MESSAGE response

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

Table A.62M: Supported headers within the MESSAGE 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
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

Table A.62N: Supported message bodies within the MESSAGE response

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

A.2.1.4.8 NOTIFY method

Prerequisite A.5/10 - - NOTIFY request

Table A.63: Supported headers within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Contact	[26] 20.10	m	m	[26] 20.10	m	m
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] 7.2.1	m	m	[28] 7.2.1	m	m
15	From	[26] 20.20	m	m	[26] 20.20	m	m
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
17	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
17A	P-Access-Network-Info	[52] 4.4	c10	c11	[52] 4.4	c10	c12
17B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
17C	P-Charging-Function-Addresses	[52] 4.5	c14	c15	[52] 4.5	c14	c15
17D	P-Charging-Vector	[52] 4.6	c13	n/a	[52] 4.6	c13	n/a
17E	P-Preferred-Identity	[34] 9.2	c6	x	[34] 9.2	n/a	n/a
17F	Privacy	[33] 4.2	c7	n/a	[33] 4.2	c7	c7
18	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
19	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
19A	Reason	[34A] 2	c18	c18	[34A] 2	c18	c18
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	c9	c9
21	Require	[26] 20.32	o	o	[26] 20.32	m	m
22A	Security-Client	[48] 2.3.1	c16	c16	[48] 2.3.1	n/a	n/a
22B	Security-Verify	[48] 2.3.1	c17	c17	[48] 2.3.1	n/a	n/a
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23	Subscription-State	[28] 8.2.3	m	m	[28] 8.2.3	m	m
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
28	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.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9:	IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension.
c10:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c11:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c12:	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.
c13:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c14:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c16:	IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note).
c17:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c18:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/10 - - NOTIFY request

Table A.64: Supported message bodies within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	sipfrag	[37] 2	c1	c1	[37]	c1	c1
c1:	IF A.4/15 THEN m ELSE o - - the REFER method extension						

Prerequisite A.5/11 - - NOTIFY response

Table A.65: Supported headers within the NOTIFY response - all 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	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c10	[52] 4.5	c9	c10
10D	P-Charging-Vector	[52] 4.6	c8	n/a	[52] 4.6	c8	n/a
10E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10F	Privacy	[33] 4.2	c4	n/a	[33] 4.2	c4	c4
10G	Require	[26] 20.32	m	m	[26] 20.32	m	m
10H	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	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.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	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.5/11 - - NOTIFY response

Prerequisite: A.6/6 and A.6/7 - - 2xx

Table A.66: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
1A	Contact	[26] 20.10	m	m	[26] 20.10	m	m
2	Record-Route	[26] 20.30	c3	c3	[26] 20.30	c3	c3
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.						
c3:	IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension.						

Prerequisite A.5/11 - - NOTIFY 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.67: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Contact	[26] 20.10	m (note)	m	[26] 20.10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than MANDATORY for a 485 response.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.68: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/11 - - NOTIFY 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.69: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.70: Supported headers within the NOTIFY 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.71: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	c3	c3
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c3:	IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/11 - - NOTIFY response

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

Table A.72: Supported headers within the NOTIFY 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
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.73: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.73A: Supported headers within the NOTIFY 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.5/11 - - NOTIFY response

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

Table A.74: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.75: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	m	m
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/11 - - NOTIFY response

Table A.76: Supported message bodies within the NOTIFY response

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

A.2.1.4.9 OPTIONS method

Prerequisite A.5/12 - - OPTIONS request

Table A.77: Supported headers within the OPTIONS request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	m	m	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	c2	c2	[26] 20.7	c2	c2
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
8	Contact	[26] 20.10	o	o	[26] 20.10	o	o
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
18	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
19	Organization	[26] 20.25	o	o	[26] 20.25	o	o
19A	P-Access-Network-Info	[52] 4.4	c11	c12	[52] 4.4	c11	c13
19B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
19C	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c9	c9
19D	P-Charging-Function-Addresses	[52] 4.5	c16	c17	[52] 4.5	c16	c17
19E	P-Charging-Vector	[52] 4.6	c14	c15	[52] 4.6	c14	c15
19F	P-Preferred-Identity	[34] 9.2	c6	c4	[34] 9.2	n/a	n/a
19G	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c10	n/a
19H	Privacy	[33] 4.2	c8	c8	[33] 4.2	c8	c8
20	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
21	Proxy-Require	[26] 20.29	o	o (note 1)	[26] 20.29	n/a	n/a
21A	Reason	[34A] 2	c20	c20	[34A] 2	c20	c20
22	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
24A	Security-Client	[48] 2.3.1	c18	c18	[48] 2.3.1	n/a	n/a
24B	Security-Verify	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
25	Supported	[26] 20.37	c6	c6	[26] 20.37	m	m
26	Timestamp	[26] 20.38	c7	c7	[26] 20.38	m	m
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c3:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c4:	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.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c8:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c10:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c11:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c12:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c13:	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.
c14:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c15:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c17:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3).
c19:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c20:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE 1:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.
NOTE 2:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 3:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/12 - - OPTIONS request

Table A.78: Supported message bodies within the OPTIONS request

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

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.79: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/13 - - OPTIONS response

Table A.80: Supported headers within the OPTIONS 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
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
11B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
11C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
11D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
11E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
11F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
11G	Require	[26] 20.32	m	m	[26] 20.32	m	m
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	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.5/13 - - OPTIONS response

Prerequisite: A.6/6 - - 2xx

Table A.81: Supported headers within the OPTIONS 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	m	m
2	Allow	[26] 20.5	o (note 1)	o	[26] 20.5	m	m
3	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
5	Contact	[26] 20.10	o		[26] 20.10	o	
8	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.						
NOTE 1:	The strength of this requirement in RFC 3261 [26] is RECOMMENDED, rather than OPTIONAL.						

Prerequisite A.5/13 - - OPTIONS 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.82: Supported headers within the OPTIONS 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
3	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.83: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	
c1:	IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/13 - - OPTIONS 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.84: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/13 - - OPTIONS response

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

Table A.85: Supported headers within the OPTIONS response

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

Prerequisite A.5/13 - - OPTIONS response

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

Table A.86: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/13 - - OPTIONS response

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

Table A.87: Supported headers within the OPTIONS 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
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/13 - - OPTIONS response

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

Table A.88: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/13 - - OPTIONS response

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

Table A.88A: Supported headers within the OPTIONS 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.5/13 - - OPTIONS response

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

Table A.89: Supported headers within the OPTIONS 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
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/13 - - OPTIONS response

Table A.90: Supported message bodies within the OPTIONS response

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

A.2.1.3.10 PRACK method

Prerequisite A.5/14 - - PRACK request

Table A.91: Supported headers within the PRACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
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	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
16	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
16A	P-Access-Network-Info	[52] 4.4	c9	c10	[52] 4.4	c9	c11
16B	P-Charging-Function-Addresses	[52] 4.5	c13	c14	[52] 4.5	c13	c14
16C	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c12	n/a
16D	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
17	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
18	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
19	RAck	[27] 7.2	m	m	[27] 7.2	m	m
19A	Reason	[34A] 2	c7	c7	[34A] 2	c7	c7
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
21	Require	[26] 20.32	o	o	[26] 20.32	m	m
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23	Supported	[26] 20.37	o	o	[26] 20.37	m	m
24	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
25	To	[26] 20.39	m	m	[26] 20.39	m	m
26	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
27	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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c10: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c11: 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.
c12: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c13: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c14: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.

Prerequisite A.5/14 - - PRACK request

Table A.92: Supported message bodies within the PRACK request

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

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.93: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/15 - - PRACK response

Table A.94: Supported headers within the PRACK 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	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c3	c4	[52] 4.4	c3	c5
10B	P-Charging-Function-Addresses	[52] 4.5	c7	c8	[52] 4.5	c7	c8
10C	P-Charging-Vector	[52] 4.6	c6	n/a	[52] 4.6	c6	n/a
10D	Privacy	[33] 4.2	c2	n/a	[33] 4.2	c2	n/a
10E	Require	[26] 20.32	o	o	[26] 20.32	m	m
10F	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c3:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c4:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c5:	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.						
c6:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c7:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c8:	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.5/15 - - PRACK response

Prerequisite: A.6/6 - - 2xx

Table A.95: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
0B	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	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.5/15 - - PRACK 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.96: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.97: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/15 - - PRACK 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.98: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

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

Table A.99: Supported headers within the PRACK 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

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

Table A.100: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	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.5/15 - - PRACK response

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

Table A.101: Supported headers within the PRACK 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
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

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

Table A.102: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

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

Table A.102A: Supported headers within the PRACK 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.5/15 - - PRACK response

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

Table A.103: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

Table A.104: Supported message bodies within the PRACK response

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

A.2.1.4.11 REFER method

Prerequisite A.5/16 - - REFER request

Table A.105: Supported headers within the REFER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept	[26] 20.1	o	o	[26] 20.1	m	m
0B	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
1A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	m	m	[26] 20.10	m	m
5A	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
5B	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
5C	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	c4	c4	[26] 20.17	m	m
10	Expires	[26] 20.19	o	o	[26] 20.19	o	o
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
13	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
14	Organization	[26] 20.25	o	o	[26] 20.25	o	o
14A	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
14B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c8	c8
14C	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c10	c10
14D	P-Charging-Function-Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
14E	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
14F	P-Preferred-Identity	[34] 9.2	c8	c7	[34] 9.2	n/a	n/a
14G	P-Visited-Network-ID	[52] 4.3	x (note 1)	x	[52] 4.3	c11	n/a
14H	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
15	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
16	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
16A	Reason	[34A] 2	c21	c21	[34A] 2	c21	c21
17	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
18	Refer-To	[36] 3	m	m	[36] 3	m	m
19	Require	[26] 20.32	o	o	[26] 20.32	m	m
20	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
20A	Security-Client	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
20B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	n/a	n/a
20C	Subject	[26] 20.36	o	o	[26] 20.36	o	o
21	Supported	[26] 20.37, [26] 7.1	o	o	[26] 20.37, [26] 7.1	m	m
22	Timestamp	[26] 20.38	c6	c6	[26] 20.38	m	m
23	To	[26] 20.39	m	m	[26] 20.39	m	m
24	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
25	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.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c11:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c13:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c14:	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.
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c19:	IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 2).
c20:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c21:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE 1:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 2:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/16 - - REFER request

Table A.106: Supported message bodies within the REFER request

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

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.107: Supported headers within the REFER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/17 - - REFER response

Table A.108: Supported headers within the REFER 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
1A	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
2	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
3	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
4	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
5	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
6	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
7	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
8	From	[26] 20.20	m	m	[26] 20.20	m	m
9	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10	Organization	[26] 20.25	o	o	[26] 20.25	o	o
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
10D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
10E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
10G	Require	[26] 20.32	m	m	[26] 20.32	m	m
10H	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	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.5/17 - - REFER response

Prerequisite: A.6/7 - - 202 (Accepted)

Table A.109: Supported headers within the REFER 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	Contact	[26] 20.10	m	m	[26] 20.10	m	m
5	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
8	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.5/17 - - REFER 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.110: Supported headers within the REFER 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
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.111: Supported headers within the REFER 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
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	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.5/17 - - REFER 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.112: Supported headers within the REFER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/17 - - REFER response

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

Table A.113: Supported headers within the REFER response

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

Prerequisite A.5/17 - - REFER response

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

Table A.114: Supported headers within the REFER 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
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/17 - - REFER response

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

Table A.115: Supported headers within the REFER 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
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/17 - - REFER response

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

Table A.116: Supported headers within the REFER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/17 - - REFER response

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

Table A.116A: Supported headers within the REFER 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.5/17 - - REFER response

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

Table A.117: Supported headers within the REFER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/17 - - REFER response

Table A.118: Supported message bodies within the REFER response

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

A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

Table A.119: Supported headers within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7, [49]	c2	o	[26] 20.7, [49]	m	c22
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
8	Contact	[26] 20.10	o	o	[26] 20.10	m	m
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	Expires	[26] 20.19	o	o	[26] 20.19	m	m
17	From	[26] 20.20	m	m	[26] 20.20	m	m
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
20A	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
20B	P-Charging-Function-Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
20C	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
20D	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c10	c11
20E	Path	[35] 4	c4	c5	[35] 4	m	c6
20F	Privacy	[33] 4.2	c9	n/a	[33] 4.2	c9	n/a
21	Proxy-Authorization	[26] 20.28	c8	c8	[26] 20.28	n/a	n/a
22	Proxy-Require	[26] 20.29	o	o (note 1)	[26] 20.29	n/a	n/a
22A	Reason	[34A] 2	c23	c23	[34A] 2	c23	c23
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	o	n/a	[26] 20.34	n/a	n/a
24A	Security-Client	[48] 2.3.1	c19	c20	[48] 2.3.1	n/a	n/a
24B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	c21	n/a
25	Supported	[26] 20.37	o	o	[26] 20.37	m	m
26	Timestamp	[26] 20.38	m	m	[26] 20.38	c7	c7
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c2:	IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.
c3:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c4:	IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c5:	IF A.4/24 THEN x ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c6:	IF A.3/4 THEN m ELSE n/a. - - S-CSCF.
c7:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c8:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c11:	IF A.4/33 THEN m ELSE n/a - - the P-Visited-Network-ID extension.
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c13:	IF A.4/34 AND (A.3/1 OR A.3/4) THEN o ELSE n/a - - the P-Access-Network-Info header extension and UE or S-CSCF (note 4).
c14:	IF A.4/34 AND (A.3/4 OR A.3/7A) THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF or AS acting as terminating UA.
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).
c19:	IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3).
c20:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c21:	IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.
c22:	IF A.3/4 THEN m ELSE n/a - - S-CSCF.
c23:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE 1:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.
NOTE 2:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 3:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented.
NOTE 4:	Refere to subclause 5.1.1.2 for information on when the UE sets the P-Access-Network-Info header.

Prerequisite A.5/18 - - REGISTER request

Table A.120: Supported message bodies within the REGISTER request

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

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.121: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m
6	To	[26] 20.39	n/a	n/a	[26] 20.39	m	m
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m

Prerequisite A.5/19 - - REGISTER response

Table A.122: Supported headers within the REGISTER response - all 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
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c3	n/a	[52] 4.4	c3	n/a
11B	P-Charging-Function-Addresses	[52] 4.5	c6	c7	[52] 4.5	c6	c7
11C	P-Charging-Vector	[52] 4.6	c4	c5	[52] 4.6	c4	c5
11D	Privacy	[33] 4.2	c2	n/a	[33] 4.2	c2	n/a
11E	Require	[26] 20.32	m	m	[26] 20.32	m	m
11F	Server	[26] 20.35	o	o	[26] 20.35	o	o
12	Timestamp	[26] 20.38	c2	c2	[26] 20.38	m	m
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c3:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c4:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c5:	IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).						
c6:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c7:	IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).						
NOTE:	For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/6 - - 2xx

Table A.123: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
2	Allow	[26] 20.5	o	o	[26] 20.5	m	m
3	Authentication-Info	[26] 20.6	c6	c6	[26] 20.6	c7	c7
5	Contact	[26] 20.10	o	o	[26] 20.10	m	m
5A	P-Associated-URI	[52] 4.1	c8	c9	[52] 4.1	c10	c11
6	Path	[35] 4	c3	c3	[35] 4	c4	c4
8	Service-Route	[38] 6	c5	c5	[38] 6	c5	c5
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF (A.3/4 AND A.4/2) THEN m ELSE n/a. - - S-CSCF acting as registrar.						
c2:	IF A.3/4 OR A.3/1THEN m ELSE n/a. - - S-CSCF or UE.						
c3:	IF A.4/24 THEN m ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.						
c4:	IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.						
c5:	IF A.4/28 THEN m ELSE n/a - - session initiation protocol extension header field for service route discovery during registration.						
c6:	IF A.4/8 THEN o ELSE n/a - - authentication between UA and registrar.						
c7:	IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.						
c8:	IF A.4/2 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and registrar.						
c9:	IF A.3/1 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and S-CSCF.						
c10:	IF A.4/31 THEN o ELSE n/a - - P-Assocated-URI header extension.						
c11:	IF A.4/31 AND A.3/1 THEN m ELSE n/a - - P-Assocated-URI header extension and UE.						

Prerequisite A.5/19 - - REGISTER 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.124: Supported headers within the REGISTER 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
3	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
4	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.125: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Proxy-Authenticate	[26] 20.27	c1	x	[26] 20.27	c1	x
6	Security-Server	[48] 2	x	x	[48] 2	n/a	c2
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.5/8 THEN m ELSE n/a - - support of authentication between UA and UA.						
c2:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/19 - - REGISTER 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.126: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/19 - - REGISTER response

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

Table A.127: Supported headers within the REGISTER response

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

Prerequisite A.5/19 - - REGISTER response

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

Table A.128: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Proxy-Authenticate	[26] 20.27	c1	x	[26] 20.27	c1	x
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
9	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.5/8 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.129: Supported headers within the REGISTER 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
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.130: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/19 - - REGISTER response

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

Table A.130A: Supported headers within the REGISTER 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	c2	c2	[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.						
c2:	IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.131: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o		[26] 20.18	o	
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/19 - - REGISTER response

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

Table A.132: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/19 - - REGISTER response

Table A.133: Supported message bodies within the REGISTER response

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

A.2.1.4.13 SUBSCRIBE method

Prerequisite A.5/20 - - SUBSCRIBE request

Table A.134: Supported headers within the SUBSCRIBE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Contact	[26] 20.10	m	m	[26] 20.10	m	m
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] 7.2.1	m	m	[28] 7.2.1	m	m
15	Expires	[26] 20.19	o (note 1)	o (note 1)	[26] 20.19	m	m
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
18	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
18A	Organization	[26] 20.25	o	o	[26] 20.25	o	o
18B	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
18C	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
18D	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c10	c10
18E	P-Charging-Function-Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
18F	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
18G	P-Preferred-Identity	[34] 9.2	c6	c7	[34] 9.2	n/a	n/a
18H	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c11	n/a
18I	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
19	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
20	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
20A	Reason	[34A] 2	c21	c21	[34A] 2	c21	c21
21	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
22	Require	[26] 20.32	o	o	[26] 20.32	m	m
23	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23A	Security-Client	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
23B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	n/a	n/a
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
28	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.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
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.4/6 THEN o ELSE n/a - - timestamping of requests.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c11:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c13:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c14:	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.
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c19:	IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3).
c20:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c21:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE 1:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.
NOTE 2:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 3:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/20 - - SUBSCRIBE request

Table A.135: Supported message bodies within the SUBSCRIBE request

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

Prerequisite A.5/21 - - SUBSCRIBE response

Table A.136: Supported headers within the SUBSCRIBE response - all 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	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	Organization	[26] 20.25	o	o	[26] 20.25	o	o
10B	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10C	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10D	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
10E	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
10F	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10G	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
10H	Require	[26] 20.32	m	m	[26] 20.32	m	m
10I	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	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.5/21 - - SUBSCRIBE response

Prerequisite: A.6/6 and A.6/7 - - 2xx

Table A.137: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
1A	Contact	[26] 20.10	m	m	[26] 20.10	m	m
2	Expires	[26] 20.19	m	m	[26] 20.19	m	m
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	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.5/21 - - SUBSCRIBE 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.138: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Contact	[26] 20.10	m (note)	m	[26] 20.10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than MANDATORY for a 485 response.						

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.139: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/21 - - SUBSCRIBE response

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

Table A.140: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Retry-After	[26] 20.33	o		[26] 20.33	o	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.141: Supported headers within the SUBSCRIBE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.142: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	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.5/21 - - SUBSCRIBE response

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

Table A.143: Supported headers within the SUBSCRIBE 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
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.144: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.144A: Supported headers within the SUBSCRIBE 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.5/21 - - SUBSCRIBE response

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

Table A.145: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.146: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.147: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	m	m
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/45 - - 503 (Service Unavailable)

Table A.148: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

Table A.149: Supported message bodies within the SUBSCRIBE response

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

A.2.1.4.14 UPDATE method

Prerequisite A.5/22 - - UPDATE request

Table A.150: Supported headers within the UPDATE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
4	Allow	[26] 20.5	o	o	[26] 20.5	m	m
5	Allow-Events	[28] 7.2.2	c2	c2	[28] 7.2.2	c3	c3
6	Authorization	[26] 20.7	c4	c4	[26] 20.7	c4	c4
7	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
9	Contact	[26] 20.10	m	m	[26] 20.10	m	m
10	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
11	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
12	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
13	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
14	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
15	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
16	Date	[26] 20.17	c5	c5	[26] 20.17	m	m
17	From	[26] 20.20	m	m	[26] 20.20	m	m
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
20A	P-Access-Network-Info	[52] 4.4	c11	c12	[52] 4.4	c11	c13
20B	P-Charging-Function-Addresses	[52] 4.5	c16	c17	[52] 4.5	c16	c17
20C	P-Charging-Vector	[52] 4.6	c14	c15	[52] 4.6	c14	c15
20D	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
21	Proxy-Authorization	[26] 20.28	c10	c10	[26] 20.28	n/a	n/a
22	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
22A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
23	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
24	Require	[26] 20.32	o	o	[26] 20.32	m	m
25	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
25A	Security-Client	[48] 2.3.1	c18	c18	[48] 2.3.1	n/a	n/a
25B	Security-Verify	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
26	Supported	[26] 20.37	o	o	[26] 20.37	m	m
27	Timestamp	[26] 20.38	c9	c9	[26] 20.38	m	m
28	To	[26] 20.39	m	m	[26] 20.39	m	m
29	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
30	Via	[26] 20.42	m	m	[26] 20.42	m	m

c2: IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c4: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c5: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c6: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c10: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c11: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c12: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c13: 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.
c14: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c15: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c16: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c17: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18: IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note).
c19: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.

NOTE:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/22 - - UPDATE request

Table A.151: Supported message bodies within the UPDATE request

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

Prerequisite A.5/23 - - UPDATE response

Table A.152: Supported headers within the UPDATE 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
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	Organization	[26] 20.25	o	o	[26] 20.25	o	o
10B	P-Access-Network-Info	[52] 4.4	c4	c5	[52] 4.4	c4	c6
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c10	[52] 4.5	c9	c10
10D	P-Charging-Vector	[52] 4.6	c7	c8	[52] 4.6	c7	c8
10E	Privacy	[33] 4.2	c3	n/a	[33] 4.2	c3	n/a
10F	Require	[26] 20.31	m	m	[26] 20.31	m	m
10G	Server	[26] 20.35	o	o	[26] 20.35	o	o
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	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.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c4:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c5:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c6:	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.						
c7:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c8:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	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.5/23 - - UPDATE response

Prerequisite: A.6/6 - - 2xx

Table A.153: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept	[26] 20.1	o	o	[26] 20.1	m	m
0B	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
0C	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
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	Contact	[26] 20.10	m	m	[26] 20.10	m	m
6	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.5/23 - - UPDATE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 - - 3xx

Table A.154: Supported headers within the UPDATE 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	o	[26] 20.10	o	o
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.154A: Supported headers within the UPDATE 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	o		[26] 20.27	o	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	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.5/23 - - UPDATE 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.155: Supported headers within the UPDATE 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
5	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/23 - - UPDATE response

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

Table A.156: Supported headers within the UPDATE 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
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/23 - - UPDATE response

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

Table A.157: Supported headers within the UPDATE 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
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
8	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.5/23 - - UPDATE response

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

Table A.158: Supported headers within the UPDATE 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
6	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/23 - - UPDATE response

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

Table A.159: Supported headers within the UPDATE 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
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
7	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/23 - - UPDATE response

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

Table A.159A: Supported headers within the UPDATE 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.5/23 - - UPDATE response

Prerequisite: A.6/35 - - 485 (Ambiguous)

Table A.160: Supported headers within the UPDATE 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
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE: The strength of this requirement is RECOMMENDED rather than OPTIONAL.							

Prerequisite A.5/23 - - UPDATE response

Table A.161: Supported message bodies within the UPDATE response

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

A.2.2 Proxy role

A.2.2.1 Introduction

This subclause contains the ICS proforma tables related to the proxy role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 - - proxy role

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 response?	[26] 20	o	o
	Extensions			
20	the SIP INFO method?	[25]	o	o
21	reliability of provisional responses in	[27]	o	i

	SIP?			
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	
31B	application of privacy based on the received Privacy header	[33]	c10	
31C	passing on of the Privacy header transparently	[33]	c10	
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	
31E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	n/a	n/a
31F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	n/a	n/a
31G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c11	c12
32	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	c30
33	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	m
34	Compressing the Session Initiation Protocol	[55]	o	c7
35	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m
36	the P-Associated-URI header extension?	[52] 4.1	c14	c15
37	the P-Called-Party-ID header extension?	[52] 4.2	c14	c16
38	the P-Visited-Network-ID header extension?	[52] 4.3	c14	c17
39	reading, or deleting the P-Visited-Network-ID header before proxying the request or response?	[52] 4.3	c18	n/a
41	the P-Access-Network-Info header extension?	[52] 4.4	c14	c19
42	act as first entity within the trust domain	[52] 4.4	c20	c21

	for access network information?			
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

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:	
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:	
c13:	
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
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.
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.

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	o	m	[26] 16	o	m
3	BYE response	[26] 16	o	m	[26] 16	o	m
4	CANCEL request	[26] 16.10	o	m	[26] 16.10	o	m
5	CANCEL response	[26] 16.10	o	m	[26] 16.10	o	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
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.						

A.2.2.4 PDU parameters

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		
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	c5	c5	[26] 21.4.17	c6	c6

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

A.2.2.4.2 ACK method

Prerequisite A.163/1 - - ACK request

Table A.165: Supported headers within the ACK request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
3	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
7	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
8	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c3
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
13	From	[26] 20.20	m	m	[26] 20.20	m	m
14	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
15	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3
15A	Privacy	[33] 4.2	c6	c6	[33] 4.2	c7	c7
16	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c4	c4
17	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
~~17A~~	~~Privacy~~	~~[33] 4.2~~	~~c6~~	~~c6~~	~~[33] 4.2~~	~~c7~~	~~c7~~
17A	Reason	[34A] 2	c8	c8	[34A] 2	c9	c9
18	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
19	Route	[26] 20.34	m	m	[26] 20.34	m	m
20	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
23	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c3: IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c4: IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7: 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.
c8: IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.

NOTE: c1 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.

Editor's note: Is the following table a suitable way of showing the contents of message bodies.

Prerequisite A.163/1 - - ACK request

Table A.166: Supported message bodies within the ACK request

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

A.2.2.4.3 BYE method

Prerequisite A.163/2 - - BYE request

Table A.167: Supported headers within the BYE request

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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c3
8	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c3
9	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c3
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	c3
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	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
16	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3
16A	P-Access-Network-Info	[52] 4.4	c13	c13	[52] 4.4	c14	c14
16B	P-Asserted-Identity	[34] 9.1	c9	c9	[34] 9.1	c10	c10
16C	P-Charging-Function-Addresses	[52] 4.5	c17	c17	[52] 4.5	c18	c18
16D	P-Charging-Vector	[52] 4.6	c15	n/a	[52] 4.6	c16	n/a
16E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c8	n/a
16F	Privacy	[33] 4.2	c11	c11	[33] 4.2	c12	c12
17	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c4	c4
18	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
18A	Reason	[34A] 2	c20	c20	[34A] 2	c21	c21
19	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
20	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
21	Route	[26] 20.34	m	m	[26] 20.34	m	m
21A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c19	c19
21B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c19	c19
22	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
23	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
24	To	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
26	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c3:	IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c4:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c9:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c10:	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.
c11:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c12:	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.
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.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c16:	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.
c17:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	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.
c19:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c20:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c21:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/2 - - BYE request

Table A.168: Supported message bodies within the BYE request

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

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.169: Supported headers within the BYE response

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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.						

Prerequisite A.163/3 - - BYE response

Table A.170: Supported headers within the BYE 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	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c2
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c2
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c2
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c2
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c2
10A	P-Access-Network-Info	[52] 4.4	c12	c12	[52] 4.4	c13	c13
10B	P-Asserted-Identity	[34] 9.1	c4	c4	[34] 9.1	c5	c5
10C	P-Charging-Function-Addresses	[52] 4.5	c10	c10	[52] 4.5	c11	c11
10D	P-Charging-Vector	[52] 4.6	c8	n/a	[52] 4.6	c9	n/a
10E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c3	n/a
10F	Privacy	[33] 4.2	c6	c6	[33] 4.2	c7	c7
10G	Require	[26] 20.32	m	m	[26] 20.32	c14	c14
10H	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.						
c3:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.						
c4:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c5:	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.						
c6:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c7:	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.						
c8:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c9:	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.						
c10:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	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.						
c12:	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.						
c13:	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.						
c14:	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.163/3 - - BYE response

Prerequisite: A.164/6 - - 2xx

Table A.171: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
2	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						

Prerequisite A.163/3 - BYE 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.172: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
2	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.163/3 - - BYE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.173: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/3 - - BYE 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.174: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/3 - - BYE response

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

Table A.175: Supported headers within the BYE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/3 - - BYE response

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

Table A.176: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/3 - - BYE response

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

Table A.177: Supported headers within the BYE 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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/3 - - BYE response

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

Table A.178: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	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.163/3 - - BYE response

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

Table A.178A: Supported headers within the BYE 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.163/3 - - BYE response

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

Table A.179: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/3 - - BYE response

Table A.180: Supported message bodies within the BYE response

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

A.2.2.4.4 CANCEL method

Prerequisite A.163/4 - - CANCEL request

Table A.181: Supported headers within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
9	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
10	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
143	Privacy	[33] 4.2	c3	c3	[33] 4.2	c4	c4
15	Reason	[34A] 2	c8	c8	[34A] 2	c9	c9
16	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
18	Route	[26] 20.34	m	m	[26] 20.34	m	m
19	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
20	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.						
c2:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.						
c3:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c4:	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.						
c6:	IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.						
c7:	IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.						
c8:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.						
c9:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.						
NOTE:	c1 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.163/4 - - CANCEL request

Table A.182: Supported message bodies within the CANCEL request

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

Prerequisite A.163/5 - - CANCEL response

Table A.183: Supported headers within the CANCEL response - all 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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	Privacy	[33] 4.2	c2	c2	[33] 4.2	c3	c3
6	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
7	To	[26] 20.39	m	m	[26] 20.39	m	m
7A	User-Agent	[26] 20.41	o		[26] 20.41	o	
8	Via	[26] 20.42	m	m	[26] 20.42	m	m
9	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.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c3:	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.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/6 - - 200 (OK)

Table A.184: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.185: Supported headers within the CANCEL response

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

Prerequisite A.163/5 - - CANCEL response

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

Table A.186: Supported headers within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Error-Info	[26] 2418	m	m	[26] 20.18	i	i
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/5 - - CANCEL response

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

Table A.188: Supported headers within the CANCEL response

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

Prerequisite A.163/5 - - CANCEL response

Table A.189: Supported message bodies within the CANCEL response

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

A.2.2.4.5 COMET method

Void

A.2.2.4.6 INFO method

Void

A.2.2.4.7 INVITE method

Prerequisite A.163/8 - - INVITE request

Table A.204: Supported headers within the INVITE request

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	Alert-Info	[26] 20.4	c2	c2	[26] 20.4	c3	c3
5	Allow	[26] 20.5	m	m	[26] 20.5	i	i
6	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
8	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
9	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
10	Call-Info	[26] 20.9	m	m	[26] 20.9	c12	c12
11	Contact	[26] 20.10	m	m	[26] 20.10	i	i
12	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c6
13	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c6
14	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c6
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c6
17	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	m	m	[26] 20.17	c4	c4
19	Expires	[26] 20.19	m	m	[26] 20.19	i	i
20	From	[26] 20.20	m	m	[26] 20.20	m	m
21	In-Reply-To	[26] 20.21	m	m	[26] 20.21	i	i
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
23	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c6
24	Organization	[26] 20.25	m	m	[26] 20.25	c5	c5
24A	P-Access-Network-Info	[52] 4.4	c28	c28	[52] 4.4	c29	c30
24B	P-Asserted-Identity	[34] 9.1	c15	c15	[34] 9.1	c16	c16
24C	P-Called-Party-ID	[52] 4.2	c19	c19	[52] 4.2	c20	c21
24D	P-Charging-Function-Addresses	[52] 4.5	c26	c27	[52] 4.5	c26	c27
24E	P-Charging-Vector	[52] 4.6	c24	c24	[52] 4.6	c25	c25
25	P-Media-Authorization	[31] 6.1	c9	c10	[31] 6.1	n/a	n/a
25A	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c14	c14
25B	P-Visited-Network-ID	[52] 4.3	c22	n/a	[52] 4.3	c23	n/a
26	Priority	[26] 20.26	m	m	[26] 20.26	i	i
26A	Privacy	[33] 4.2	c17	c17	[33] 4.2	c18	c18
27	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c13	c13
28	Proxy-Require	[26] 20.29, [34] 4	m	m	[26] 20.29, [34] 4	m	m
28A	Reason	[34A] 2	c32	c32	[34A] 2	c33	c33
29	Record-Route	[26] 20.30	m	m	[26] 20.30	c11	c11
31	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
32	Require	[26] 20.32	m	m	[26] 20.32	c7	c7
33	Route	[26] 20.34	m	m	[26] 20.34	m	m
33A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c31	c31
33B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c31	c31
34	Subject	[26] 20.36	m	m	[26] 20.36	i	i
35	Supported	[26] 20.37	m	m	[26] 20.37	c8	c8

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
36	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
37	To	[26] 20.39	m	m	[26] 20.39	m	m
38	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
39	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2: IF A.162/10 THEN n/a ELSE m - - suppression or modification of alerting information data.
c3: IF A.162/10 THEN m ELSE i - - suppression or modification of alerting information data.
c4: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c5: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c6: IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c7: 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.
c8: IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.
c9: IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.
c10: IF A.3/2 THEN m ELSE n/a - - P-CSCF.
c11: IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c12: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c13: IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
c14: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c15: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c16: 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.
c17: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c18: 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.
c19: IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.
c20: IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.
c21: 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.
c22: IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.
c23: IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.
c24: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c25: 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.
c26: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c27: 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.
c28: 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.
c29: 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.
c30: IF A.162/43 OR (A.162/41 AND A.3/2) 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 (with or without P-CSCF).
c31: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c32: IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c33: IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.

NOTE: c1 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.163/8 - - INVITE request

Table A.205: Supported message bodies within the INVITE request

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

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.206: Supported headers within the INVITE response

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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	c2	c2
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies.						
c2:	IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.						

Prerequisite A.163/9 - - INVITE response

Table A.207: Supported headers within the INVITE 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
1A	Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4
2	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c3
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c3
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c3
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c3
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3
11	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
11A	P-Access-Network-Info	[52] 4.4	c14	c14	[52] 4.4	c15	c15
11B	P-Asserted-Identity	[34] 9.1	c6	c6	[34] 9.1	c7	c7
11C	P-Charging-Function-Addresses	[52] 4.5	c12	c12	[52] 4.5	c13	c13
11D	P-Charging-Vector	[52] 4.6	c10	c10	[52] 4.6	c11	c11
11E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c5	n/a
11F	Privacy	[33] 4.2	c8	c8	[33] 4.2	c9	c9
11G	Require	[26] 20.32	m	m	[26] 20.32	c16	c16
11H	Server	[26] 20.35	m	m	[26] 20.35	i	i
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c4: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c5: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c6: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7: 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.
c8: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9: 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.
c10: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c11: 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.
c12: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c13: 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.
c14: 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.
c15: 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.
c16: 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.163/9 - - INVITE response

Prerequisite: A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 - - 1xx

Table A.208: Supported headers within the INVITE 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
4	Contact	[26] 20.10	m	m	[26] 20.10	i	i
6	P-Media-Authorization	[31] 6.1	c9	c10	[31] 6.1	n/a	n/a
9	Rseq	[27] 7.1	m	m	[27] 7.1	i	i
11	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c9:	IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.						
c10:	IF A.3/2 THEN m ELSE n/a - - P-CSCF.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/6 - - 2xx

Table A.209: Supported headers within the INVITE 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
1A	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
1B	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
6	Contact	[26] 20.10	m	m	[26] 20.10	i	i
8	P-Media-Authorization	[31] 6.1	c9	c10	[31] 6.1	n/a	n/a
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.						
c9:	IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.						
c10:	IF A.3/2 THEN m ELSE n/a - - P-CSCF.						

Prerequisite A.163/9 - - INVITE 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.210: Supported headers within the INVITE 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
4	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
10	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.163/9 - - INVITE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.211: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
15	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.163/9 - - INVITE response

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

Table A.212: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
12	Via	[26] 20.42	m	m	[26] 20.42	m	m

Prerequisite A.163/9 - - INVITE response

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

Table A.213: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Allow	[26] 20.5	m		[26] 20.5	m/o	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9 - - INVITE response

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

Table A.214: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i
11	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/9 - - INVITE response

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

Table A.215: Supported headers within the INVITE 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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
6	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
11	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9 - - INVITE response

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

Table A.216: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	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.163/9 - - INVITE response

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

Table A.216A: Supported headers within the INVITE 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.163/9 - - INVITE response

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

Table A.217: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/42 - - 500 (Server Internal Error)

Table A.217A: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/45 - - 503 (Service Unavailable)

Table A.217B: Supported headers within the INVITE 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9 - - INVITE response

Table A.218: Supported message bodies within the INVITE response

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

A.2.2.4.7A MESSAGE method

Prerequisite A.163/9A - - MESSAGE request

Table A.218A: Supported headers within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
3	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4
6	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
7	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
8	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
13	Expires	[26] 20.19	m	m	[26] 20.19	I	i
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	In-Reply-To	[26] 20.21	m	m	[50] 10	i	i
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
17	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
18	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
18A	P-Access-Network-Info	[52] 4.4	c23	c23	[52] 4.4	c24	c24
18B	P-Asserted-Identity	[34] 9.1	c10	c10	[34] 9.1	c11	c11
18C	P-Called-Party-ID	[52] 4.2	c14	c14	[52] 4.2	c15	c16
18D	P-Charging-Function-Addresses	[52] 4.5	c21	c21	[52] 4.5	c22	c22
18E	P-Charging-Vector	[52] 4.6	c19	c19	[52] 4.6	c20	c20
18F	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c9	c9
18G	P-Visited-Network-ID	[52] 4.3	c17	n/a	[52] 4.3	c18	n/a
19	Priority	[26] 20.26	m	m	[26] 20.26	i	i
19A	Privacy	[33] 4.2	c12	c12	[33] 4.2	c13	c13
20	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c8	c8
21	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
21A	Reason	[34A] 2	c26	c26	[34A] 2	c27	c27
22	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
23	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
24	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
25	Route	[26] 20.34	m	m	[26] 20.34	m	m
25A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c25	c25
25B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c25	c25
26	Subject	[26] 20.36	m	m	[26] 20.36	i	i
27	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
28	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
29	To	[26] 20.39	m	m	[26] 20.39	m	m
30	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
31	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
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.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c26:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c27:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/9A - - MESSAGE request

Table A.218B: Supported message bodies within the MESSAGE request

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

Prerequisite A.163/9B - - MESSAGE response

Table A.218C: Supported headers within the MESSAGE 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] 20.9	m	m	[26] 20.9	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
12A	P-Access-Network-Info	[52] 4.4	c13	c13	[52] 4.4	c14	c14
12B	P-Asserted-Identity	[34] 9.1	c5	c5	[34] 9.1	c6	c6
12C	P-Charging-Function-Addresses	[52] 4.5	c11	c11	[52] 4.5	c12	c12
12D	P-Charging-Vector	[52] 4.6	c9	n/a	[52] 4.6	c10	n/a
12E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c4	n/a
12F	Privacy	[33] 4.2	c7	c7	[33] 4.2	c8	c8
12G	Require	[26] 20.32	m	m	[26] 20.32	c15	c15
13	Server	[26] 20.35	m	m	[26] 20.35	i	i
14	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
15	To	[26] 20.39	m	m	[26] 20.39	m	m
16	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
17	Via	[26] 20.42	m	m	[26] 20.42	m	m
18	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.163/9B - - MESSAGE response

Prerequisite: A.164/6 - - 2xx

Table A.218D: Supported headers within the MESSAGE 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
4	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						

Prerequisite A.163/9B - - MESSAGE 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.218E: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	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
5	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.163/9B - - MESSAGE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.218F: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/9B - - MESSAGE 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.218G: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

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

Table A.218H: Supported headers within the MESSAGE 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
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

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

Table A.218I: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/9B - - MESSAGE response

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

Table A.218J: Supported headers within the MESSAGE 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	[50] 10	i	i
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

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

Table A.218K: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	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.163/9B - - MESSAGE response

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

Table A.218L: Supported headers within the MESSAGE 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.163/9B - - MESSAGE response

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

Table A.218M: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

Table A.218N: Supported message bodies within the MESSAGE response

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

A.2.2.4.8 NOTIFY method

Prerequisite A.163/10 - - NOTIFY request

Table A.219: Supported headers within the NOTIFY request

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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Contact	[26] 20.10	m	m	[26] 20.10	i	i
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	[28] 7.2.1	m	m	[28] 7.2.1	m	m
15	From	[26] 20.20	m	m	[26] 20.20	m	m
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
17	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
17A	P-Access-Network-Info	[52] 4.4	c16	c16	[52] 4.4	c17	c17
17B	P-Asserted-Identity	[34] 9.1	c8	c8	[34] 9.1	c9	c9
17C	P-Charging-Function-Addresses	[52] 4.5	c14	c14	[52] 4.5	c15	c15
17D	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c13	n/a
17E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c3	n/a
17F	Privacy	[33] 4.2	c10	c10	[33] 4.2	c11	c11
18	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c4	c4
19	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
19A	Reason	[34A] 2	c19	c19	[34A] 2	c20	c20
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
21	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
22	Route	[26] 20.34	m	m	[26] 20.34	m	m
22A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c18	c18
22B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c18	c18
23	Subscription-State	[28] 8.2.3	m	m	[28] 8.2.3	i	i
24	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
28	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c3:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c4:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.162/14 THEN (IF A.162/22 OR A.162/27 THEN m ELSE o) ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog or (the REFER method or SIP specific event notification).
c8:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c9:	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.
c10:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c11:	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.
c12:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c13:	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.
c14:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	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.
c16:	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.
c17:	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.
c18:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c19:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c20:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/10 - - NOTIFY request

Table A.220: Supported message bodies within the NOTIFY request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	sipfrag	[37] 2	m	m	[37] 2	i	i

Prerequisite A.163/11 - - NOTIFY response

Table A.221: Supported headers within the NOTIFY response - all 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	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
10A	P-Access-Network-Info	[52] 4.4	c11	c11	[52] 4.4	c12	c12
10B	P-Asserted-Identity	[34] 9.1	c3	c3	[34] 9.1	c4	c4
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c9	[52] 4.5	c10	c10
10D	P-Charging-Vector	[52] 4.6	c7	n/a	[52] 4.6	c8	n/a
10E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c2	n/a
10F	Privacy	[33] 4.2	c5	c5	[33] 4.2	c6	c6
10G	Require	[26] 20.32	m	m	[26] 20.32	c13	c13
10H	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	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.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.						
c3:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c4:	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.						
c5:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c6:	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.						
c7:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c8:	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.						
c9:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	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.						
c11:	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.						
c12:	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.						
c13:	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.163/11 - - NOTIFY response

Prerequisite: A.164/6 AND A.164/7 - - 2xx

Table A.222: Supported headers within the NOTIFY response

Item	Header	Sending	Receiving

		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
1A	Contact	[26] 20.10	m	m	[26] 20.10	i	i
2	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	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.						

Prerequisite A.163/11 - - NOTIFY 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.223: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	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.163/11 - - NOTIFY response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.224: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/11 - - NOTIFY 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.225: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/11 - - NOTIFY response

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

Table A.226: Supported headers within the NOTIFY 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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/11 - - NOTIFY response

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

Table A.227: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/11 - - NOTIFY response

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

Table A.228: Supported headers within the NOTIFY 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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/11 - - NOTIFY response

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

Table A.229: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	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.163/11 - - NOTIFY response

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

Table A.229A: Supported headers within the NOTIFY 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.163/11 - - NOTIFY response

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

Table A.230: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/39 - - 489 (Bad Event)

Table A.231: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.						
NOTE:	c1 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.163/11 - - NOTIFY response

Table A.232: Supported message bodies within the NOTIFY response

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

A.2.2.4.9 OPTIONS method

Prerequisite A.163/12 - - OPTIONS request

Table A.233: Supported headers within the OPTIONS request

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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4
8	Contact	[26] 20.10	m	m	[26] 20.10	i	i
9	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
10	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
11	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
18	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
19	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
19A	P-Access-Network-Info	[52] 4.4	c23	c23	[52] 4.4	c24	c24
19B	P-Asserted-Identity	[34] 9.1	c10	c10	[34] 9.1	c11	c11
19C	P-Called-Party-ID	[52] 4.2	c14	c14	[52] 4.2	c15	c16
19D	P-Charging-Function-Addresses	[52] 4.5	c21	c21	[52] 4.5	c22	c22
19E	P-Charging-Vector	[52] 4.6	c19	c19	[52] 4.6	c20	c20
19F	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c9	c9
19G	P-Visited-Network-ID	[52] 4.3	c17	n/a	[52] 4.3	c18	n/a
19H	Privacy	[33] 4.2	c12	c12	[33] 4.2	c13	c13
20	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c8	c8
21	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
21A	Reason	[34A] 2	c26	c26	[34A] 2	c27	c27
22	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
23	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
24A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c25	c25
24B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c25	c25
25	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
26	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
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.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c26:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c27:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/12 - - OPTIONS request

Table A.234: Supported message bodies within the OPTIONS request

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

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.235: Supported headers within the OPTIONS response

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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.						

Prerequisite A.163/13 - - OPTIONS response

Table A.236: Supported headers within the OPTIONS 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
1A	Call-Info	[26] 20.9	m	m	[26] 20.9	c3	c3
2	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
11	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
11A	P-Access-Network-Info	[52] 4.4	c13	c13	[52] 4.4	c14	c14
11B	P-Asserted-Identity	[34] 9.1	c5	c5	[34] 9.1	c6	c6
11C	P-Charging-Function-Addresses	[52] 4.5	c11	c11	[52] 4.5	c12	c12
11D	P-Charging-Vector	[52] 4.6	c9	c9	[52] 4.6	c10	c10
11E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c4	n/a
11F	Privacy	[33] 4.2	c7	c7	[33] 4.2	c8	c8
11G	Require	[26] 20.32	m	m	[26] 20.32	c15	c15
11H	Server	[26] 20.35	m	m	[26] 20.35	i	i
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	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.163/13 - - OPTIONS response

Prerequisite: A.164/6 - - 2xx

Table A.237: Supported headers within the OPTIONS 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	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
5	Contact	[26] 20.10	m	m	[26] 20.10	i	i
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
12	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						

Prerequisite A.163/13 - - OPTIONS 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.238: Supported headers within the OPTIONS 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
3	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	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.163/13 - - OPTIONS response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.239: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/13 - - OPTIONS 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.240: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/13 - - OPTIONS response

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

Table A.241: Supported headers within the OPTIONS response

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

Prerequisite A.163/13 - - OPTIONS response

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

Table A.242: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/13 - - OPTIONS response

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

Table A.243: Supported headers within the OPTIONS 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
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/13 - - OPTIONS response

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

Table A.244: Supported headers within the OPTIONS 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
7	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.163/13 - - OPTIONS response

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

Table A.244A: Supported headers within the OPTIONS 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.163/13 - - OPTIONS response

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

Table A.245: Supported headers within the OPTIONS 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
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/13 - - OPTIONS response

Table A.246: Supported message bodies within the OPTIONS response

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

A.2.2.4.10 PRACK method

Prerequisite A.163/14 - - PRACK request

Table A.247: Supported headers within the PRACK request

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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c3
8	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c3
9	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c3
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	c3
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	From	[26] 20.20	m	m	[26] 20.20	m	m
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
16	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3
16A	P-Access-Network-Info	[52] 4.4	c14	c14	[52] 4.4	c15	c15
16B	P-Charging-Function-Addresses	[52] 4.5	c12	c12	[52] 4.5	c13	c13
16C	P-Charging-Vector	[52] 4.6	c10	n/a	[52] 4.6	c11	n/a
16D	Privacy	[33] 4.2	c8	c8	[33] 4.2	c9	c9
17	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c4	c4
18	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
19	RAck	[27] 7.2	m	m	[27] 7.2	i	i
19A	Reason	[34A] 2	c16	c16	[34A] 2	c17	c17
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
21	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
22	Route	[26] 20.34	m	m	[26] 20.34	m	m
23	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
24	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
25	To	[26] 20.39	m	m	[26] 20.39	m	m
26	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
27	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c3:	IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
c4:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.162/14 THEN 0 ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9:	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.
c10:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c11:	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.
c12:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c13:	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.
c14:	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.
c15:	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.
c16:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c17:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/14 - - PRACK request

Table A.248: Supported message bodies within the PRACK request

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

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.249: Supported headers within the PRACK response

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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.						

Prerequisite A.163/15 - - PRACK response

Table A.250: Supported headers within the PRACK 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	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c2
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c2
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c2
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c2
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c2
10A	P-Access-Network-Info	[52] 4.4	c9	c9	[52] 4.4	c10	c10
10B	P-Charging-Function-Addresses	[52] 4.5	c7	c7	[52] 4.5	c8	c8
10C	P-Charging-Vector	[52] 4.6	c5	n/a	[52] 4.6	c6	n/a
10D	Privacy	[33] 4.2	c3	c3	[33] 4.2	c4	c4
10E	Require	[26] 20.32	m	m	[26] 20.32	c11	c11
10F	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.						
c3:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c4:	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.						
c5:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c6:	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.						
c7:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c8:	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.						
c9:	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.						
c10:	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.						
c11:	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.163/15 - - PRACK response

Prerequisite: A.164/6 - - 2xx

Table A.251: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
0B	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
1	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.

Prerequisite A.163/15 - - PRACK 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.252: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	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.163/15 - - PRACK response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.253: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/15 - - PRACK 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.254: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15 - - PRACK response

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

Table A.255: Supported headers within the PRACK 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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15 - - PRACK response

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

Table A.256: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/15 - - PRACK response

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

Table A.257: Supported headers within the PRACK 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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15 - - PRACK response

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

Table A.258: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15 - - PRACK response

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

Table A.258A: Supported headers within the PRACK 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.163/15 - - PRACK response

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

Table A.259: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15 - - PRACK response

Table A.260: Supported message bodies within the PRACK response

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

A.2.2.4.11 REFER method

Prerequisite A.163/16 - - REFER request

Table A.261: Supported headers within the REFER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept	[26] 20.1	m	m	[26] 20.1	i	i
0B	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
1	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
1A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
3	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	m	m	[26] 20.10	i	i
5A	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
5B	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
5C	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	c2	c2
10	Expires	[26] 20.19	m	m	[26] 20.19	i	i
11	From	[26] 20.20	m	m	[26] 20.20	m	m
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
13	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
14	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
14A	P-Access-Network-Info	[52] 4.4	c22	c22	[52] 4.4	c23	c23
14B	P-Asserted-Identity	[34] 9.1	c9	c9	[34] 9.1	c10	c10
14C	P-Called-Party-ID	[52] 4.2	c13	c13	[52] 4.2	c14	c15
14D	P-Charging-Function-Addresses	[52] 4.5	c20	c20	[52] 4.5	c21	c21
14E	P-Charging-Vector	[52] 4.6	c18	c18	[52] 4.6	c19	c19
14F	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c8	c8
14G	P-Visited-Network-ID	[52] 4.3	c16	n/a	[52] 4.3	c17	n/a
14H	Privacy	[33] 4.2	c11	c11	[33] 4.2	c12	c12
15	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c4	c4
16	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
16A	Reason	[34A] 2	c25	c25	[34A] 2	c26	c26
17	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
18	Refer-To	[36] 3	c3	c3	[36] 3	c4	c4
19	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
20	Route	[26] 20.34	m	m	[26] 20.34	m	m
20A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c24	c24
20B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c24	c24
20C	Subject	[26] 20.36	m	m	[26] 20.36	i	i
21	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
22	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
23	To	[26] 20.39	m	m	[26] 20.39	m	m
24	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
25	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
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.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c9:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c10:	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.
c11:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c12:	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.
c13:	IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.
c14:	IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.
c15:	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.
c16:	IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.
c17:	IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.
c18:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c19:	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.
c20:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21:	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.
c22:	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.
c23:	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.
c24:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c25:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c26:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/16 - - REFER request

Table A.262: Supported message bodies within the REFER request

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

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.263: Supported headers within the REFER response

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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.						

Prerequisite A.163/17 - - REFER response

Table A.264: Supported headers within the REFER 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
1A	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
2	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
3	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
4	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
5	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
6	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
7	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
8	From	[26] 20.20	m	m	[26] 20.20	m	m
9	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
10	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
10A	P-Access-Network-Info	[52] 4.4	c12	c12	[52] 4.4	c13	c13
10B	P-Asserted-Identity	[34] 9.1	c4	c4	[34] 9.1	c5	c5
10C	P-Charging-Function-Addresses	[52] 4.5	c10	c10	[52] 4.5	c11	c11
10D	P-Charging-Vector	[52] 4.6	c8	c8	[52] 4.6	c9	c9
10E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c3	n/a
10F	Privacy	[33] 4.2	c6	c6	[33] 4.2	c7	c7
10G	Require	[26] 20.32	m	m	[26] 20.32	c14	c14
10H	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	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.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.						
c4:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c5:	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.						
c6:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c7:	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.						
c8:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c9:	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.						
c10:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	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.						
c12:	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.						
c13:	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.						
c14:	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.163/17 - - REFER response

Prerequisite: A.164/7 - - 202 (Accepted)

Table A.265: Supported headers within the REFER 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	Contact	[26] 20.10	m	m	[26] 20.10	i	i
5	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	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.						

Prerequisite A.163/17 - - REFER 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.266: Supported headers within the REFER 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
7	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.163/17 - - REFER 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.267: Supported headers within the REFER 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
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/17 - - REFER 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.268: Supported headers within the REFER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/17 - - REFER response

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

Table A.269: Supported headers within the REFER response

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

Prerequisite A.163/17 - - REFER response

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

Table A.270: Supported headers within the REFER 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
4	Proxy-Authenticate	[26] 20.27	o		[26] 20.27	o	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/17 - - REFER response

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

Table A.271: Supported headers within the REFER 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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/17 - - REFER response

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

Table A.272: Supported headers within the REFER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	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.163/17 - - REFER response

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

Table A.272A: Supported headers within the REFER 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.163/17 - - REFER response

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

Table A.273: Supported headers within the REFER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/17 - - REFER response

Table A.274: Supported message bodies within the REFER response

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

A.2.2.4.12 REGISTER method

Prerequisite A.163/18 - - REGISTER request

Table A.275: Supported headers within the REGISTER request

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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7, [49]	m	m	[26] 20.7, [49]	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	m	m	[26] 20.9	c2	c2
8	Contact	[26] 20.10	m	m	[26] 20.10	i	i
9	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
10	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
11	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	m	m	[26] 20.17	m	m
16	Expires	[26] 20.19	m	m	[26] 20.19	i	i
17	From	[26] 20.20	m	m	[26] 20.20	m	m
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
20A	P-Access-Network-Info	[52] 4.4	c16	c16	[52] 4.4	c17	c17
20B	P-Charging-Function-Addresses	[52] 4.5	c14	c14	[52] 4.5	c15	c15
20C	P-Charging-Vector	[52] 4.6	c12	c12	[52] 4.6	c13	c13
20D	P-Visited-Network-ID	[52] 4.3	c10	c10	[52] 4.3	c11	c11
20E	Path	[35] 4.2	c6	c6	[35] 4.2	c6	c6
20F	Privacy	[33] 4.2	c8	c8	[33] 4.2	c9	c9
21	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c7	c7
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
22A	Reason	[34A] 2	c19	c19	[34A] 2	c20	c20
23	Require	[26] 20.32	m	m	[26] 20.32	c4	c4
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
24A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c18	c18
24B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c18	c18
25	Supported	[26] 20.37	m	m	[26] 20.37	c5	c5
26	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c3:	IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c4:	IF A.162/11 OR A.162/12 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.
c5:	IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.
c6:	IF A.162/29 THEN m ELSE n/a - - PATH header support.
c7:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
c8:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9:	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.
c10:	IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.
c11:	IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.
c12:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c13:	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.
c14:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	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.
c16:	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.
c17:	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.
c18:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c19:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c20:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/18 - - REGISTER request

Table A.276: Supported message bodies within the REGISTER request

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

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.277: Supported headers within the REGISTER response

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	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	m	m	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m

Prerequisite A.163/19 - - REGISTER response

Table A.278: Supported headers within the REGISTER 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
1A	Call-Info	[26] 20.9	m	m	[26] 20.9	c2	c2
2	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
11	Organization	[26] 20.25	m	m	[26] 20.25	c1	c1
11A	P-Access-Network-Info	[52] 4.4	c9	c9	[52] 4.4	c10	c10
11B	P-Charging-Function-Addresses	[52] 4.5	c7	c7	[52] 4.5	c8	c8
11C	P-Charging-Vector	[52] 4.6	c5	c5	[52] 4.6	c6	c6
11D	Privacy	[33] 4.2	c3	c3	[33] 4.2	c4	c4
11E	Require	[26] 20.32	m	m	[26] 20.32	c11	c11
11F	Server	[26] 20.35	m	m	[26] 20.35	i	i
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	m	m	[26] 20.43	i	i
c1:	IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.						
c2:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.						
c3:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c4:	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.						
c5:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c6:	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.						
c7:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c8:	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.						
c9:	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.						
c10:	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.						
c11:	IF A.162/11 OR A.162/12 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.163/19 - - REGISTER response

Prerequisite: A.164/6 - - 2xx

Table A.279: Supported headers within the REGISTER 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
1A	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
1B	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
5	Contact	[26] 20.10	m	m	[26] 20.10	i	i
5A	P-Associated-URI	[52] 4.1	c8	c8	[52] 4.1	c9	c10
6	Path	[35] 4.2	c3	c3	[35] 4.2	c4	c4
8	Service-Route	[38] 6	c5	c5	[38] 6	c6	c7
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG).						
c3:	IF A.162/29 THEN m ELSE n/a - - Path extension support.						
c4:	IF A.162/29 THEN i ELSE n/a - - Path extension support.						
c5:	IF A.162/32 THEN m ELSE n/a - - Service-Route extension support.						
c6:	IF A.162/32 THEN i ELSE n/a - - Service-Route extension support.						
c7:	IF A.162/32 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - Service-Route extension and P-CSCF.						
c8:	IF A.162/36 THEN m ELSE n/a - - the P-Associated-URI extension.						
c9:	IF A.162/36 THEN i ELSE n/a - - the P-Associated-URI extension.						
c10:	IF A.162/36 AND A.3/2 THEN m ELSE IF A.162/36 AND A.3/3 THEN i ELSE n/a - - the P-Associated-URI extension and P-CSCF or I-CSCF.						

Prerequisite A.163/19 - - REGISTER 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.280: Supported headers within the REGISTER 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
3	Contact	[26] 20.10	m	m	[26] 20.10	c2	c2
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.162/19E THEN m ELSE i - - deleting Contact headers.						

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.281: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
6	Security-Server	[48] 2	x	c1	[48] 2	n/a	n/a
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i
c1:	IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.163/19 - - REGISTER 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.282: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/19 - - REGISTER response

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

Table A.283: Supported headers within the REGISTER response

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

Prerequisite A.163/19 - - REGISTER response

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

Table A.284: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i
9	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/19 - - REGISTER response

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

Table A.285: Supported headers within the REGISTER 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
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/19 - - REGISTER response

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

Table A.286: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
c3:	IF A.162/17 THEN m ELSE.i						

Prerequisite A.163/19 - - REGISTER response

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

Table A.286A: Supported headers within the REGISTER 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.163/19 - - REGISTER response

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

Table A.287: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	o		[26] 20.18	o	
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/19 - - REGISTER response

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

Table A.288: Supported headers within the REGISTER 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/19 - - REGISTER response

Table A.289: Supported message bodies within the REGISTER response

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

A.2.2.4.13 SUBSCRIBE method

Prerequisite A.163/20 - - SUBSCRIBE request

Table A.290: Supported headers within the SUBSCRIBE request

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
3A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Contact	[26] 20.10	m	m	[26] 20.10	i	i
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	[28] 7.2.1	m	m	[28] 7.2.1	m	m
15	Expires	[26] 20.19	m	m	[26] 20.19	i	i
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
18	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
18A	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
18B	P-Access-Network-Info	[52] 4.4	c22	c22	[52] 4.4	c23	c23
18C	P-Asserted-Identity	[34] 9.1	c9	c9	[34] 9.1	c10	c10
18D	P-Called-Party-ID	[52] 4.2	c13	c13	[52] 4.2	c14	c15
18E	P-Charging-Function-Addresses	[52] 4.5	c20	c20	[52] 4.5	c21	c21
18F	P-Charging-Vector	[52] 4.6	c18	c18	[52] 4.6	c19	c19
18G	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c8	c8
18H	P-Visited-Network-ID	[52] 4.3	c16	n/a	[52] 4.3	c17	n/a
18I	Privacy	[33] 4.2	c11	c11	[33] 4.2	c12	c12
19	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c4	c4
20	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
20A	Reason	[34A] 2	c25	c25	[34A] 2	c26	c26
21	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
22	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
23	Route	[26] 20.34	m	m	[26] 20.34	m	m
23A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c24	c24
23B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c24	c24
24	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
28	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
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.162/8A THEN m ELSE i - - authentication between UA and proxy.
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.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c9:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c10:	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.
c11:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c12:	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.
c13:	IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.
c14:	IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.
c15:	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.
c16:	IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.
c17:	IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.
c18:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c19:	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.
c20:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21:	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.
c22:	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.
c23:	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.
c24:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c25:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c26:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/20 - - SUBSCRIBE request

Table A.291: Supported message bodies within the SUBSCRIBE request

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

Prerequisite A.163/21 - - SUBSCRIBE response

Table A.292: Supported headers within the SUBSCRIBE response - all 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	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
10A	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
10B	P-Access-Network-Info	[52] 4.4	c12	c12	[52] 4.4	c13	c13
10C	P-Asserted-Identity	[34] 9.1	c4	c4	[34] 9.1	c5	c5
10D	P-Charging-Function-Addresses	[52] 4.5	c10	c10	[52] 4.5	c11	c11
10E	P-Charging-Vector	[52] 4.6	c8	c8	[52] 4.6	c9	c9
10F	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c3	n/a
10G	Privacy	[33] 4.2	c6	c6	[33] 4.2	c7	c7
10H	Require	[26] 20.32	m	m	[26] 20.32	c14	c14
10I	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	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.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.						
c4:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c5:	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.						
c6:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c7:	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.						
c8:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c9:	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.						
c10:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	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.						
c12:	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.						
c13:	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.						
c14:	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.163/21 - - SUBSCRIBE response

Prerequisite: A.164/6 AND A.164/7 - - 2xx

Table A.293: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
1A	Contact	[26] 20.10	m	m	[26] 20.10	i	i
2	Expires	[26] 20.19	m	m	[26] 20.19	i	i
3	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	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.						

Prerequisite A.163/21 - - SUBSCRIBE 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.294: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	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.163/21 - - SUBSCRIBE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.295: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

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

Table A.296: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

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

Table A.297: Supported headers within the SUBSCRIBE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

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

Table A.298: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

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

Table A.299: Supported headers within the SUBSCRIBE 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
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

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

Table A.300: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	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.163/21 - - SUBSCRIBE response

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

Table A.300A: Supported headers within the SUBSCRIBE 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.163/21 - - SUBSCRIBE response

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

Table A.301: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

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

Table A.302: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/39 - - 489 (Bad Event)

Table A.303: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.						
NOTE:	c1 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.163/21 - - SUBSCRIBE response

Prerequisite: A.164/45 - - 503 (Service Unavailable)

Table A.303A: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

Table A.304: Supported message bodies within the SUBSCRIBE response

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

A.2.2.4.14 UPDATE method

Prerequisite A.163/22 - - UPDATE request

Table A.305: Supported headers within the UPDATE request

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	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
6	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
7	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Call-Info	[26] 20.9	m	m	[26] 20.9	c8	c8
9	Contact	[26] 20.10	m	m	[26] 20.10	i	i
10	Content-Disposition	[26] 20.11	m	m	[26] 20.11	c4	c4
11	Content-Encoding	[26] 20.12	m	m	[26] 20.12	c4	c4
12	Content-Language	[26] 20.13	m	m	[26] 20.13	c4	c4
13	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
14	Content-Type	[26] 20.15	m	m	[26] 20.15	c4	c4
15	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
16	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
17	From	[26] 20.20	m	m	[26] 20.20	m	m
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	c4
20	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
20A	P-Access-Network-Info	[52] 4.4	c16	c16	[52] 4.4	c17	c17
20B	P-Charging-Function-Addresses	[52] 4.5	c14	c14	[52] 4.5	c15	c15
20C	P-Charging-Vector	[52] 4.6	c12	c12	[52] 4.6	c13	c13
20D	Privacy	[33] 4.2	c10	c10	[33] 4.2	c11	c11
21	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c9	c9
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
22A	Reason	[34A] 2	c19	c19	[34A] 2	c20	c20
23	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
24	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
25A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c18	c18
25B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c18	c18
25	Route	[26] 20.34	m	m	[26] 20.34	m	m
26	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
27	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
28	To	[26] 20.39	m	m	[26] 20.39	m	m
29	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
30	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.
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.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c9:	IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
c10:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c11:	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.
c12:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c13:	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.
c14:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	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.
c16:	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.
c17:	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.
c18:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c19:	IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c20:	IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
NOTE:	c1 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.163/22 - - UPDATE request

Table A.306: Supported message bodies within the UPDATE request

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

Prerequisite A.163/22 - - UPDATE response

Table A.307: Supported headers within the UPDATE 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
1A	Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4
2	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c3
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c3
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c3
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c3
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3
10A	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
10B	P-Access-Network-Info	[52] 4.4	c11	c11	[52] 4.4	c12	c12
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c9	[52] 4.5	c10	c10
10D	P-Charging-Vector	[52] 4.6	c7	n/a	[52] 4.6	c8	n/a
10E	Privacy	[33] 4.2	c5	c5	[33] 4.2	c6	c6
10F	Require	[26] 20.32	m	m	[26] 20.32	c13	c13
10G	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.						
c4:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.						
c5:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c6:	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.						
c7:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c8:	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.						
c9:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	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.						
c11:	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.						
c12:	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.						
c13:	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.163/23 - - UPDATE response

Prerequisite: A.164/6 - - 2xx

Table A.308: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept	[26] 20.1	m	m	[26] 20.1	i	i

0B	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
0C	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
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	Contact	[26] 20.10	m	m	[26] 20.10	i	i
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 3xx

Table A.309: Supported headers within the UPDATE 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
7	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.163/23 - - UPDATE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.309A: Supported headers within the UPDATE 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
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/23 - - UPDATE 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.310: Supported headers within the UPDATE 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
5	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/23 - - UPDATE response

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

Table A.311: Supported headers within the UPDATE 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
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/23 - - UPDATE response

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

Table A.312: Supported headers within the UPDATE 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
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/23 - - UPDATE response

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

Table A.313: Supported headers within the UPDATE 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
6	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/23 - - UPDATE response

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

Table A.314: Supported headers within the UPDATE 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
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
7	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.163/23 - - UPDATE response

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

Table A.314A: Supported headers within the UPDATE 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.163/23 - - UPDATE response

Prerequisite: A.164/35 - - 485 (Ambiguous)

Table A.315: Supported headers within the UPDATE 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
7	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.163/23 - - UPDATE response

Table A.316: Supported message bodies within the UPDATE response

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

A.3 Profile definition for the Session Description Protocol as used in the present document

A.3.1 Introduction

Void.

A.3.2 User agent role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations.

Prerequisite: A.2/1 -- user agent role

A.3.2.1 Major capabilities

Table A.317: Major capabilities

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

A.3.2.2 SDP types

Table A.318: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier)	[39] 6	m	m	[39] 6	m	m
3	s= (session name)	[39] 6	m	m	[39] 6	m	m
4	i= (session information)	[39] 6	o		[39] 6		
5	u= (URI of description)	[39] 6	o	n/a	[39] 6		n/a
6	e= (email address)	[39] 6	o	n/a	[39] 6		n/a
7	p= (phone number)	[39] 6	o	n/a	[39] 6		n/a
8	c= (connection information)	[39] 6	o		[39] 6		
9	b= (bandwidth information)	[39] 6	o	o (NOTE 1)	[39] 6		
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	m	m
11	r= (zero or more repeat times)	[39] 6	o	n/a	[39] 6		n/a
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	o	n/a	[39] 6		n/a
13	k= (encryption key)	[39] 6	o		[39] 6		
14	a= (zero or more session attribute lines)	[39] 6	o		[39] 6		
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	o	o	[39] 6	m	m
16	i= (media title)	[39] 6	o		[39] 6		
17	c= (connection information)	[39] 6	c1	c1	[39] 6		
18	b= (bandwidth information)	[39] 6	o	o (NOTE 1)	[39] 6		
19	k= (encryption key)	[39] 6	o		[39] 6		
20	a= (zero or more media attribute lines)	[39] 6	o		[39] 6		
c1: IF A.318/15 THEN m ELSE n/a. NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.							

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

Table A.319: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6			[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
18	current-status attribute (a=curr)	[30] 5	c1	c1	[30] 5	c2	c2
19	desired-status attribute (a=des)	[30] 5	c1	c1	[30] 5	c2	c2
20	confirm-status attribute (a=conf)	[30] 5	c1	c1	[30] 5	c2	c2
21	media stream identification attribute (a=mid)	[53] 3	c3	c3	[53] 3	c4	c4
22	group attribute (a=group)	[53] 4	c5	c5	[53] 3	c6	c6
c1:	IF A.317/22 THEN o ELSE n/a.						
c2:	IF A.317/22 THEN m ELSE n/a.						
c3:	IF A.317/23 THEN o ELSE n/a.						
c4:	IF A.317/23 THEN m ELSE n/a.						
c5:	IF A.317/24 THEN o ELSE n/a.						
c6:	IF A.317/24 THEN m ELSE n/a.						

A.3.2.3 SDP types parameters

Prerequisite A.318/2 - - o= (owner/creator and session identifier)

Table A.320: owner/creator and session identifier type (o=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	username	[39] 6	m	m	[39] 6	m	n/a
2	session id	[39] 6	m	m	[39] 6	m	m
3	version	[39] 6	m	m	[39] 6	m	m
4	network type	[39] 6	m	m	[39] 6	m	n/a
5	address type	[39] 6	m	m	[39] 6	m	n/a
6	address	[39] 6	m	m	[39] 6	m	n/a

Prerequisite A.318/10 - - t= (time the session is active)

Table A.321: time the session is active type (t=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	start time	[39] 6	m	m	[39] 6	m	n/a
2	stop time	[39] 6	m	m	[39] 6	m	n/a

Prerequisite A.318/11 - - r= (zero or more repeat times)

Table A.322: zero or more repeat times (r=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	repeat interval	[39] 6		n/a	[39] 6		n/a
2	active duration	[39] 6		n/a	[39] 6		n/a
3	list of offsets from start-time	[39] 6		n/a	[39] 6		n/a

Prerquisite A.318/12 - - z= (time zone adjustments)

Table A.323: time zone adjustments type (z=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	adjustment time	[39] 6		n/a	[39] 6		n/a
2	offset	[39] 6		n/a	[39] 6		n/a
3	adjustment time	[39] 6		n/a	[39] 6		n/a
4	offset	[39] 6		n/a	[39] 6		n/a

Prerquisite A.318/13 - - k= (encryption key)

Table A.324: encryption key type (k=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	method	[39] 6			[39] 6		
2	encryption key	[39] 6			[39] 6		

Prerequisite A.318/15 - - m= (media name and transport address)

Table A.325: media name and transport address type (m=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	media - ``audio'' - ``video'' - ``application'' - ``data'' - ``control''	[39] 6			[39] 6		
2	port	[39] 6			[39] 6		
3	transport	[39] 6			[39] 6		
4	fmt list	[39] 6			[39] 6		

Editor's note: It is expected that this table will be expanded, as this is the principle table that will distinguish operation of different entities within the IM CN subsystem.

Prerequisite A.318/17 - - c= (connection information)

Table A.326: connection type (c=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	network type	[39] 6			[39] 6		
2	address type	[39] 6			[39] 6		
3	connection address	[39] 6			[39] 6		

Prerequisite A.318/18 - - b= (bandwidth information)

Table A.327: bandwidth information (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	modifier	[39] 6, [56]		o (NOTE 1)	[39] 6, [56]		
2	bandwidth-value	[39] 6		o (NOTE 2)	[39] 6		
NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, the value shall be AS, RR or RS. NOTE 2: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.							

A.3.2.4 SDP types parameters within attribute lines

This subclause dos not intend to show an exhaustive list of all the possible attribute values

Prerequisite A.319/22 - - group attribute (a=group)

Table A.327A: group semantics (a=group)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Lip Synchronization (LS)	[53] 4	o	o	[53] 4	m	m
2	Flow Identification (FID)	[53] 4	o	o	[53] 4	m	m
3	Single Reservation Flow (SRF)	[54] 2	o	m	[54] 2	m	m

A.3.3 Proxy role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 -- proxy role

A.3.3.1 Major capabilities

Table A.328: Major capabilities

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

A.3.3.2 SDP types

Table A.329: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier).	[39] 6	m	m	[39] 6	i	i
3	s= (session name)	[39] 6	m	m	[39] 6	i	i
4	i= (session information)	[39] 6	m	m	[39] 6	i	i
5	u= (URI of description)	[39] 6	m	m	[39] 6	i	i
6	e= (email address)	[39] 6	m	m	[39] 6	i	i
7	p= (phone number)	[39] 6	m	m	[39] 6	i	i
8	c= (connection information)	[39] 6	m	m	[39] 6	i	i
9	b= (bandwidth information)	[39] 6	m	m	[39] 6	i	i
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	i	i
11	r= (zero or more repeat times)	[39] 6	m	m	[39] 6	i	i
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	m	m	[39] 6	i	i
13	k= (encryption key)	[39] 6	m	m	[39] 6	i	i
14	a= (zero or more session attribute lines)	[39] 6	m	m	[39] 6	i	i
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	m	m	[39] 6	m	m
16	i= (media title)	[39] 6	o		[39] 6		
17	c= (connection information)	[39] 6	o		[39] 6		
18	b= (bandwidth information)	[39] 6	o		[39] 6		
19	k= (encryption key)	[39] 6	o		[39] 6		
20	a= (zero or more media attribute lines)	[39] 6	o		[39] 6		

Prerequisite A.329/14 OR A.329/20 - - a= (zero or more session/media attribute lines)

Table A.330: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6			[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
18	current-status attribute (a=curr)	[30] 5	m	m	[30] 5	c2	c2
19	desired-status attribute (a=des)	[30] 5	m	m	[30] 5	c2	c2
20	confirm-status attribute (a=conf)	[30] 5	m	m	[30] 5	c2	c2
21	media stream identification attribute (a=mid)	[53] 3	c3	c3	[53] 3	c4	c4
22	group attribute (a=group)	[53] 4	c5	c6	[53] 3	c5	c6
c2: IF A.328/1 THEN m ELSE i. c3: IF A.328/2 THEN o ELSE n/a. c4: IF A.328/2 THEN m ELSE n/a. c5: IF A.328/3 THEN o ELSE n/a. c6: IF A.328/3 THEN m ELSE n/a.							

A.3.3.3 SDP types parameters

Prerequisite A.329/2 - - o= (owner/creator and session identifier)

Table A.331: owner/creator and session identifier type (o=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	username	[39] 6	m	m	[39] 6	m	m
2	session id	[39] 6	m	m	[39] 6	m	m
3	version	[39] 6	m	m	[39] 6	m	m
4	network type	[39] 6	m	m	[39] 6	m	m
5	address type	[39] 6	m	m	[39] 6	m	m
6	address	[39] 6	m	m	[39] 6	m	m

Prerequisite A.329/10 - - t= (time the session is active)

Table A.332: time the session is active type (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	start time	[39] 6			[39] 6		
2	stop time	[39] 6			[39] 6		

Prerequisite A.329/11 - - r= (zero or more repeat times)

Table A.333: zero or more repeat times (r=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	repeat interval	[39] 6			[39] 6		
2	active duration	[39] 6			[39] 6		
3	list of offsets from start-time	[39] 6			[39] 6		

Prerequisite A.329/12 - - z= (time zone adjustments)

Table A.334: time zone adjustments type (z=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	adjustment time	[39] 6			[39] 6		
2	offset	[39] 6			[39] 6		
3	adjustment time	[39] 6			[39] 6		
4	offset	[39] 6			[39] 6		

Prerequisite A.329/13 - - k= (encryption key)

Table A.335: encryption key type (k=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	method	[39] 6			[39] 6		
2	encryption key	[39] 6			[39] 6		

Prerequisite A.329/15 - - m= (media name and transport address)

Table A.336: media name and transport address type (m=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	media - ``audio'' - ``video'' - ``application'' - ``data'' - ``control''	[39] 6			[39] 6		
2	port	[39] 6			[39] 6		
3	transport	[39] 6			[39] 6		
4	fmt list	[39] 6			[39] 6		

Editor's note: It is expected that this table will be expanded, as this is the principle table that will distinguish operation of different entities within the IM CN subsystem.

Prerequisite A.329/17 - - c= (connection information)

Table A.337: connection type (c=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	network type	[39] 6			[39] 6		
2	address type	[39] 6			[39] 6		
3	connection address	[39] 6			[39] 6		

Prerequisite A.329/18 - - b= (bandwidth information)

Table A.338: bandwidth information (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	modifier	[39] 6, [56]			[39] 6, [56]		
2	bandwidth-value	[39] 6			[39] 6		

A.3.3.4 SDP types parameters within attribute lines

The subclause does not intend to show an exhaustive list of all the possible attribute values.

Prerequisite A.330/22 -- group attribute (a=group)

Table A.339: group semantics (a=group)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Lip Synchronization (LS)	[53] 4	m	m	[53] 4	i	i
2	Flow Identification (FID)	[53] 4	m	m	[53] 4	i	i
3	Single Reservation Flow (SRF)	[54] 2	o	m	[54] 2	m	m

A.4 Profile definition for other message bodies as used in the present document

Void.

3GPP TSG-CN1 Meeting #32 **Tdoc N1-031439**
Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **519** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

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

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

Title:	⌘	Profile support of RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS2
Date:	⌘	14/10/2003
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: ⌘

RFC 3581 has been published. This RFC provides an extension of SIP and should therefore be documented in the SIP profile in annex A of 3GPP TS 24.229.

Previous discussions in 3GPP CN1 on dependencies on IETF specifications have not identified this RFC as having any specific usage within the IM CN subsystem, and given that its scope is:

> " The Session Initiation Protocol (SIP) operates over UDP and TCP, among others. When used with UDP, responses to requests are returned to the source address the request came from, and to the port written into the topmost Via header field value of the request. This behavior is not desirable in many cases, most notably, when the client is behind a Network Address Translator (NAT). This extension defines a new parameter for the Via header field, called "rport", that allows a client to request that the server send the response back to the source IP address and port from which the request originated."

it is proposed that this should be followed in the profile, i.e. optional to support in "RFC status" and prohibited in "Profile status".

Summary of change: ⌘

As this SIP extension only provides an extension parameter to a header, it does not need to appear in the PDU tables, or the PDU parameter tables. It is sufficient therefore just to indicate the required support in the major capabilities tables for both the UA (table A.4) and the proxy (table A.162). A reference to the RFC needs to be included in clause 2.

Consequences if not approved:	⌘	The reader of 3GPP TS 24.229 will not know the level of support required to be implemented for this extension, despite it being a published part of the range of SIP specifications.

Clauses affected:	⌘	2, A.2.1.2, A.2.2.2			
Other specs affected:	⌘	**Y** / **N**	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.

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".

[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 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

[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".

[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] draft-ietf-sip-scvrtdisco-04 (May 2003): "Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration".

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

[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".

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

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	m	c3
2	registrar?	[26] subclause 10.3	o	c4
2A	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	[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	
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	
26F	application of the privacy option "user"	[33] 5.3	c10	

	such that user level privacy functions are provided by the network?			
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	an extension to the session initiation protocol for symmetric response routeing	[56A]	o	x

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 OR A.3/7 THEN m 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.3/4 THEN m ELSE (IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - S-CSCF or 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 o A3./4 THEN m ELSE n/a – UE or S-CSCF
c18:	IF A.4/2A THEN m ELSE n/a - - initiating sessions
c19:	IF A.4/2A 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.
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.

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 response?	[26] 20	o	o
	Extensions			
20	the SIP INFO method?	[25]	o	o
21	reliability of provisional responses in	[27]	o	i

	SIP?			
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	
31B	application of privacy based on the received Privacy header	[33]	c10	
31C	passing on of the Privacy header transparently	[33]	c10	
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	
31E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	n/a	n/a
31F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	n/a	n/a
31G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c11	c12
32	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	c30
33	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	m
34	Compressing the Session Initiation Protocol	[55]	o	c7
35	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m
36	the P-Associated-URI header extension?	[52] 4.1	c14	c15
37	the P-Called-Party-ID header extension?	[52] 4.2	c14	c16
38	the P-Visited-Network-ID header extension?	[52] 4.3	c14	c17
39	reading, or deleting the P-Visited-Network-ID header before proxying the request or response?	[52] 4.3	c18	n/a
41	the P-Access-Network-Info header extension?	[52] 4.4	c14	c19
42	act as first entity within the trust domain	[52] 4.4	c20	c21

	for access network information?			
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	an extension to the session initiation protocol for symmetric response routeing	[56A]	o	x

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:	
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:	
c13:	
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
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.
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.