Biaritz, France, 4-6 August

CR-Form-v7

CHANGE REQUEST

⌘ **TS 24.229** **CR** **141** ⌘ **rev** ~~1~~ **2** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Adding MESSAGE to 24.229
Source:	⌘	Ericsson, dynamicsoft, Nortel, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	~~02~~06/~~08~~09/2002
Category:	⌘	**F**
Release:	⌘	REL-5

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:	⌘	Align with SA2's 23.228 which documents the capabilities that an IM CN susbsytems can be used to conduct session-unrelated and session unrelated MESSAGE interactions between: 1) users, 2) S-CSCF & users, 3) AS & users.
Summary of change:	⌘	Add MESSAGE in 24.229 R5 to support that SA2 capability.
Consequences if not approved:	⌘	Functional misalignment with SA2.

Clauses affected:	⌘	2, 5.1.1.2, 5.1.x, 5.2.x, 5.3.x, ~~5.4.1.2.1,~~ 5.4.x, 5.7.x, A.2.1.2, A.2.1.3, A.2.1.4.x

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

Other comments: ⌘ TS 24.229 CR 146 rev 2 and CR 153 rev 3 are linked

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".

[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".

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

[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".

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

[21] RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 2806: "URLs for Telephone Calls".

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

[24] RFC 2916: "E.164 number and DNS".

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

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

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

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

[29] RFC 3311 (April 2002): "The SIP UPDATE method".

[30] RFC 3312 (May 2002): "Integration of resource management and SIP".

[31] RFC 3313 (February 2002): "SIP extensions for media authorization".

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

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

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

[35] RFC 3327 (May 2002): "SIP Extension for Registering Non-Adjacent Contacts".

[36] draft-sparks-sip-refer-split-00 (April 2002): "The REFER method".

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

[37] draft-sparks-sip-mimetypes (April 2002): "Internet Media Type message/sipfrag".

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

[38] draft-willis-scvrtdisco-03 (May 2002): "SIP Extension Header for Service Route Discovery in Private Networks".

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

[39] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

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

[40] draft-ietf-dhc-dhcpv6-23 (February 2002): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

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

[41] draft-ietf-sip-dhcpv6-00 (April 2002): "DHCPv6 options for SIP servers".

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

[42] draft-ietf-sipping-sigcomp-sip-dictionary-00.txt (May 2002): "The SIP/SDP static dictionary for Signaling Compression".

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

[43] draft-beckmann-sip-reg-event-01 (May 2002): "Registration event package".

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

[44] draft-garcia-sip-visited-network-id-00 (March 2002): "Private SIP extension for Visited Network Identifier".

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

[45] draft-henrikson-sip-charging-information-01 (May 2002): "Private SIP Extension for Mobile Charging Information".

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

[46] draft-henrikson-sip-original-dialog-id-01 (May 2002): "Private SIP Extension for Original Dialog Identifier".

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

[47] draft-mills-sip-access-network-info-01.txt (April 2002): “SIP Access Network Information header”

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

[48] draft-ietf-sip-message-06.txt (July 2002): “Session Initiation Protocol Extension for Instant Messaging”

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

[49] draft-ietf-sip-callerprefs-06.txt (July 2002): “Session Initiation Protocol (SIP) Caller Preferences and Callee Capabilities”

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

5 Application usage of SIP

5.1 Procedures at the UE

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

As the UE supports the SIP MESSAGE method, at registration time the UE shall add the ";methods" tag to the Contact header, with an indication of support of the MESSAGE method, according to the procedures described in the SIP MESSAGE method draft-ietf-sip-message-06 [48], and in the Caller Preferences draft-ietf-sip-callerprefs-06.txt [49].

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], received in an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity;

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration; and

e) a Request-URI that contains the SIP URI of the domain name of the home network.

NOTE: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

The use of the Path header shall not be supported by the UE.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

- send another REGISTER request populating the Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

5.1.x MESSAGE support

The UE shall support the SIP MESSAGE method described in draft-ietf-sip-message-06 [48]. A UE shall be capable of sending and receiving MESSAGE method to conduct session-unrelated or session-related interactions. To do so, a UE may either initiate or terminate MESSAGE requests per draft-ietf-sip-message-06.txt [48]. The UE should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [48].

The size of the payload in a SIP MESSAGE may vary significantly. When the size of the whole SIP MESSAGE request exceeds 1300 bytes before applying any compression, the UE shall use TCP transport protocol for sending the MESSAGE request.

5.2 Procedures at the P-CSCF

5.2.x MESSAGE support

If the P-CSCF proxies a SIP MESSAGE request which size exceeds 1300 bytes (before applying any compression), the P-CSCF shall use TCP transport protocol for sending the MESSAGE request.

5.3 Procedures at the I-CSCF

5.3.x MESSAGE support

If the I-CSCF proxies a SIP MESSAGE request which size exceeds 1300 bytes, the I-CSCF shall use TCP transport protocol for sending the MESSAGE request.

5.4 Procedures at the S-CSCF

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Initial registration

Upon receipt of a REGISTER request for a user that is not registered and for which also no authentication is currently ongoing (i.e. timer reg-await-auth is not running), the S-CSCF shall:

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

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

3) check the value of the Expires header. The S-CSCF shall only proceed with the following procedures if the Expires header is set to a value greater than zero;

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

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

NOTE 1: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URL to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

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

6) remove the P-Access-Network-Info header and may act upon the contents accordingly;

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

   - the home network identification in the realm field;
   - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
   - the security mechanism, which is AKAv1-MD5, in the algorithm field;
   - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2.3);
   - optionally the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2.3);

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

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

While timer reg-await-auth is running, upon receipt of a REGISTER request, the S-CSCF shall:

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

2) stop timer reg-await-auth;

3) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps it the integrity check parameter is included;

4) check whether an Authorization header is included, containing:

- the private user identity of the user in the username field;
- the algorithm which is AKAv1-MD5 in the algorithm field; and
- the RES parameter needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the RES parameter was included;

5) check whether the received RES parameter and the XRES parameter match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if RES and XRES are matching;

6) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

- the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,
- the user profile of the user including initial Filter Criteria;

7) bind to each non-barred registered public user identity all registered contact information; ~~and store the related method tag values from the Contact header for future use;~~

NOTE 2: There might be more then one contact information available for one public user identity.

NOTE 3: The barred public user identities are not bound to the contact information.

8) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

9) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may adjust the duration of the registration due to local policy;

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

11) remove the P-Access-Network-Info header and may act upon the contents accordingly;

12) create a 200 (OK) response for the REGISTER request, including:

- an expiration time in the Expires header, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE; and,
- the list of received Path headers;
- a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network. Using information supplied by the HSS, the P-Associated-URI header will indicate the default public user identity to be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header;

Editor's note: The mechanism for indicating this default public user identity is yet to be agreed.

- a P-Service-Route header containing:
  - the SIP URL identifying the S-CSCF; and,
  - an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) shall be treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part or be a port number;
  - if network topology hiding is required a SIP URL identifying an I-CSCF(THIG) as the topmost entry;

13) send the so created 200 (OK) response to the UE;

14) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

15) handle the user as registered for the duration indicated in the Expires header.

5.4.x MESSAGE support

A S-CSCF may be capable of sending and/or receiving the MESSAGE method to conduct session-unrelated or session related interactions. To do so, a S-CSCF may initiate or terminate the MESSAGE method per draft-ietf-sip-message-06.txt [48]. The S-CSCF should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [48].

The size of the payload in a SIP MESSAGE may vary significantly. When the size of the whole SIP MESSAGE request exceeds 1300 bytes, the S-CSCF shall use TCP transport protocol for sending the MESSAGE request.

5.7 Procedures at the Application Server (AS)

5.7.x MESSAGE support

An application server (AS) may be capable of sending and/or receiving the MESSAGE method to conduct session-unrelated or session related interactions. To do so, the AS may initiate or terminate MESSAGE requests per draft-ietf-sip-message-06.txt [48]. The AS should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [48].

The size of the payload in a SIP MESSAGE may vary significantly. When the size of the whole SIP MESSAGE request exceeds 1300 bytes, the AS shall use TCP transport protocol for sending the MESSAGE request.

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

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

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
3	client behaviour for session requests?	[26] subclause 13.2	m	o
4	server behaviour for session requests?	[26] subclause 13.3	m	o
5	session release?	[26] subclause 15.1	m	c1
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
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]	o	m
15	the REFER method?	[36]	o	o
16	Integration of resource management and SIP?	[30]	o	m
17	the SIP UPDATE method	[29]	c5	m
18	SIP extensions for caller identity and privacy?	[34]	o	m
19	SIP extensions for media authorization?	[31]	o	m
20	SIP specific event notification	[28]	o	o
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	c2
23	acting as the recipient of event information	[28]	c2	c2
24	Path Extension Header for Establishing Service Route with SIP REGISTER	[35]	o	c6
25	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
27	A messaging mechanism for the Session Initiation Protocol (SIP)	[48]	o	m

c1:	IF A.4/3 OR A.4/4 THEN m ELSE o.
c2:	IF A.4/20 THEN o.1 ELSE n/a.
c3:	IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UA 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.
c6:	IF (A.150/3 AND A.150/4) THEN m ELSE n/a. - - S-CSCF acting as registrar.
o.1:	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	
6	INFO request	[25] 2	c2	n/a	[25] 2	c2	n/a
7	INFO response	[25] 2	c2	n/a	[25] 2	c2	n/a
8	INVITE request	[26] 13	m	m	[26] 13	m	m
9	INVITE response	[26] 13	m	m	[26] 13	m	m
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
24	MESSAGE request	[48] 4	c7	c7	[48] 7	c7	c7
25	MESSAGE response	[48] 4	c7	c7	[48] 7	c7	c7
c1:	IF A.4/15 THEN m ELSE n/a.						
c2:	IF A.4/13 THEN m ELSE n/a.						
c3:	IF A.4/23 THEN m ELSE n/a.						
c4:	IF A.4/22 THEN m ELSE n/a.						
c5:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses.						
c6:	IF A.4/17 THEN m ELSE n/a - - the SIP update method.						
c7:	IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.						

A.2.1.4 PDU parameters

A.2.1.4.X MESSAGE method

Prerequisite A.5/24 – MESSAGE request

Table A.xxx: Supported headers within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[48] 10	m		[48] 10	m	
2	Accept-Encoding	[48] 10	m		[48] 10	m	
3	Accept-Language	[48] 10	m		[48] 10	m	
4	Alert-Info	[48] 10	-		[48] 10	-	
5	Allow	[48] 10	o		[48] 10	m	
6	Allow-Events	[48] 10	n/a		[48] 10	n/a	
7	Anonymity	[48] 10	n/a		[48] 10	n/a	
xxx	Authentication-Info	[48] 10	o		[48] 10	o	
8	Authorization	[48] 10	o		[48] 10	o	
9	Call-ID	[48] 10	m		[48] 10	m	
10	Call-Info	[48] 10	o		[48] 10	o	
11	Contact	[48] 10	o		[48] 10	o	
12	Content-Disposition	[48] 10	o		[48] 10	o	
13	Content-Encoding	[48] 10	o		[48] 10	o	
14	Content-Language	[48] 10	o		[48] 10	o	
15	Content-Length	[48] 10	t		[48] 10	t	
16	Content-Type	[48] 10	*		[48] 10	*	
17	Cseq	[48] 10	m		[48] 10	m	
18	Date	[48] 10	o		[48] 10	o	
19	Expires	[48] 10			[48] 10		
Xxx	Error-Info	[48] 10	o		[48] 10	o	
xxx	Expires	[48] 10	o		[48] 10	o	
20	From	[48] 10	m		[48] 10	m	
21	In-Reply-To	[48] 10	o		[48] 10	o	
22	Max-Forwards	[48] 10	m		[48] 10	m	
23	MIME-Version	[48] 10	-		[48] 10	-	
24	Organization	[48] 10	o		[48] 10	o	
25	P-Media-Authorization	[48] 10	n/a		[48] 10	n/a	
26	Priority	[48] 10	o		[48] 10	o	
27	Proxy-Authorization	[48] 10	o		[48] 10	o	
28	Proxy-Require	[48] 10	o		[48] 10	o	
29	Record-Route	[48] 10	-		[48] 10	-	
30	Remote-Party-ID	[48] 10	n/a		[48] 10	n/a	
31	Reply-To	[48] 10	o		[48] 10	o	
32	Require	[48] 10	c		[48] 10	c	
xxx	Retry-After	[48] 10	o		[48] 10	o	
33	Route	[48] 10	o		[48] 10	o	
xxx	Server	[48] 10	o		[48] 10	o	
34	Subject	[48] 10	o		[48] 10	o	
35	Supported	[48] 10	n/a		[48] 10	n/a	
36	Timestamp	[48] 10	o		[48] 10	o	
37	To	[48] 10	m		[48] 10	m	
xxx	Unsupported	[48] 10	o		[48] 10	o	
38	User-Agent	[48] 10	o		[48] 10	o	
39	Via	[48] 10	m		[48] 10	m	
xxx	Warning	[48] 10	m		[48] 10	m	
xxx	WWW-Authenticate	[48] 10	o		[48] 10	o	