TTC標準
Standard

The difference between TTC JT-Q3402 and ITU-T Q.3402

NGN UNI Signalling Profile (Protocol Set 1)

(The English Edition)

Version 3.0

Published on May 21, 2015

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

Telecommunication Technology Committee

Contents

Introduction

This document provides the English Edition.

In case of dispute, the original to be referred is the Japanese edition of the text.

This document provides the difference between TTC standard JT-Q3402 (Version 2.0, May 31, 2011) and ITU-T Recommendation Q.3402(February 29,2008).

・Change History

Version	Date	Outline
1.0	May 27, 2009	Published.
2.0	May 31, 2011	The descriptions for bandwidth control are modified.
3.0	May 21, 2015	The reference for CUG/PNP is added.

・Industrial Property Rights

Information regarding submittal of TTC's "The Policy for the Handling of Industrial Property Rights" is available on TTC's website.

・Responsible working group

Signalling Working Group

TTC JT-Q3402 supplements ITU-T Q.3402 with the following items as annexes and appendices

(a) Clarifications on the specifications, network options, and terminal options of the JT-Q3402 main body in order to improve the interoperability of SIP terminals connected to domestic NGN carriers through the UNI.
This annex shows the clarifications in tables with the corresponding clause number of the main body; follow the content of this annex in addition to the main body. (Annex a)
(b) Calling line identification presentation (Annex b)
(c) Terminal registration (Annex c)
(d) Negotiating SIP capabilities (Annex d)
(e) SDP setting and media handling (Annex e)
(f) Considerations on congestion prevention and control (Annex f)
(g) Bandwidth control (Annex g)
(h) Limitations of SIP message settings (Annex h)
(i) Audio terminal's behaviour (Annex i)
(j) List of network options and terminal options for this standard (Appendix i)
(k) Guidelines for response code usage (Appendix ii)
(l) Mapping SDP description to QoS classes (Appendix iii)
(m) Security considerations (Appendix iv)
(n) Discovery procedureof the SCF (Appendix v)
(o) Signalling rule tables of SIP messages and headers (Appendix vi)
(p) Examples of message flows (Appendix vii)

The difference of references between TTC JT-Q3402 and ITU-T Q.3402 is shown in:

Table 1-a/ JT-Q3402: Modifications of references (ITU and ISO/IEC references)

Table 1-b/ JT-Q3402: Modifications of references (IETF references / Service-level signalling specifcations)

Table 1-c/ JT-Q3402: Modifications of references (IETF references / Transport-level specifications)

See "TTC Standard Summary" in TTC Website (http://www.ttc.or.jp/e/) for the summary of difference between TTC standards and referred international standards (ex. ITU-T recommendations).

Table 1-a/ JT-Q3402: Modifications of references (ITU and ISO/IEC references)

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[ITU-T G.711]	Recommendation ITU-T G.711 (1988), *Pulse code modulation (PCM) of voice frequencies.*	[G.711]	"Pulse Code Modulation (PCM) of Voice Frequencies", TTC standard JT-G711, version 4, The Telecommunication Technology Committee, Apr 2001
[ITU-T G.722]	Recommendation ITU-T G.722 (1988), *7KHz audio-coding within 64kbit/s.*	[G.722]	"7 kHz Audio Coding within 64 kbit/s", TTC standard JT-G722, version 2.2, The Telecommunication Technology Committee, Jun 2004
[ITU-T G.722.1]	Recommendation ITU-T G.722.1 (2005), *Low-complexity coding at 24 and 32kbit/s for hands-free operation in systems with low frame loss.*	[G.722.1]	"7kHz Audio-coding at 24 and 32 kbit/s for Hands Free Operation in Systems with Low Frame Loss", TTC standard JT-G722.1, version 4, The Telecommunication Technology Committee, Nov 2005
[ITU-T G.722.2]	Recommendation ITU-T G.722.2 (2003), *Wideband coding of speech at around 16kbit/s using Adaptive Multi-Rate Wideband (AMR-WB).*	[G.722.2]	"WIDEBAND CODING OF SPEECH AT AROUND 16 KBIT/S USING ADAPTIVE MULTI-RATE WIDEBAND (AMR-WB))", TTC standard JT-G722.2, version 3.3, The Telecommunication Technology Committee, May 2007
[ITU-T G.726]	Recommendation ITU-T G.726 (1990), *40, 32, 24, 16kbit/s Adaptive Differential Pulse Code Modulation (ADPCM).*	[G.726]	"40,32,24,16 kbit/s Adaptive Differential Pulse code Modulation (ADPCM)", TTC standard JT-G726, version 2.1, The Telecommunication Technology Committee, Jun 2005
[ITU-T G.729]	Recommendation ITU-T G.729 (2007), *Coding of speech at 8kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP).*	[G.729]	"Coding of Speech at 8kbit/s using Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-ACELP)", TTC standard JT-G729, version 6.1, The Telecommunication Technology Committee, Nov 2006
[ITU-T G.729.1]	Recommendation ITU-T G.729.1 (2006), *G.729-based embedded variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729.*	[G.729.1]	"G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729", TTC standard JT-G729.1, version 1, The Telecommunication Technology Committee, Mar 2007
[ITU-T H.263]	Recommendation ITU-T H.263 (2005), *Video coding for low bit rate communication.*	[H.263]	"Video Coding For Low Bitrate Communication, TTC standard JT-H263, version 3.2, The Telecommunication Technology Committee, Jun 2005
[ITU-T H.264]	Recommendation ITU-T H.264 (2005), *Advanced video coding for generic audiovisual services.*	[H.264]	"ADVANCED VIDEO CODING FOR GENERIC AUDIOVISUAL SERVICES," TTC standard JT-H264, version 2.0, The Telecommunication Technology Committee, Aug 2006
[ITU-T T.38]	Recommendation ITU-T T.38 (2007), *Procedures for real-time Group 3 facsimile communication over IP networks.*	[T.38]	"Procedures for real-time Group 3 facsimile communication over IP networks", TTC standard JT-T38, version 4, The Telecommunication Technology Committee, Jan 2006
[ITU-T Y.2012]	Recommendation ITU-T Y.2012 (2006), *Functional requirements and architecture of the NGN release 1.*	[TR-1014]	"General overview of NGN architecture", TTC technical report TR-1014, version 1, The Telecommunication Technology Committee, Jun 2006

Table 1-b/ JT-Q3402: Modifications of references (IETF references / Service-level signalling specifcations)

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 2046]	IETF RFC 2046 (1996), *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*	[RFC2046]	"Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", TTC standard JF-IETF-RFC2046, version 1, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 2327]	IETF RFC 2327 (1998), *SDP: Session Description Protocol.*	[RFC2327]	"Session Description Protocol", TTC standard JF-IETF-RFC2327, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 2617]	IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication.*	[RFC2617]	"HTTP Authentication: Basic and Digest Access Authentication", TTC standard JF-IETF-RFC2617, The Telecommunication Technology Committee, May 2009
[IETF RFC 2976]	IETF RFC 2976 (2000), *The SIP INFO Method.*	[RFC2976]	"The SIP INFO Method", TTC standard JF-IETF-RFC2976, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3261]	IETF RFC 3261 (2002), *SIP: Session Initiation Protocol.*	[RFC3261]	"Session Initiation Protocol", TTC standard JF-IETF-RFC3261, version 1, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3262]	IETF RFC 3262 (2002), *Reliability of Provisional Responses in the Session Initiation Protocol (SIP).*	[RFC3262]	"Reliability of Provisional Responses in SIP", TTC standard JF-IETF-RFC3262, version 1, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3263]	IETF RFC 3263 (2002), *Session Initiation Protocol (SIP): Locating SIP Servers.*	[RFC3263]	"Session Initiation Protocol (SIP): Locating SIP Servers", TTC standard JF-IETF-RFC3263, version 1, The Telecommunication Technology Committee, May 2009

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 3264]	IETF RFC 3264 (2002), *An Offer/Answer Model with the Session Description Protocol (SDP).*	[RFC3264]	"An Offer/Answer model with SDP", TTC standard JF-IETF-RFC3264, version 1, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3265]	IETF RFC 3265 (2002), *Session Initiation Protocol (SIP)-Specific Event Notification.*	[RFC3265]	"Session Initiation Protocol (SIP)-Specific Event Notification", TTC standard JF-IETF-RFC3265, version 1, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3310]	IETF RFC 3310 (2002), Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA).	[RFC3310]	"Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", TTC standard JF-IETF-RFC3310, The Telecommunication Technology Committee, May 2009
[IETF RFC 3311]	IETF RFC 3311 (2002), *The Session Initiation Protocol (SIP) UPDATE Method.*	[RFC3311]	"The Session Initiation Protocol UPDATE Method", TTC standard JF-IETF-RFC3311, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3312]	IETF RFC 3312 (2002), *Integration of Resource Management and Session Initiation Protocol (SIP).*	[RFC3312]	"Integration of Resource Management and Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3312, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3313]	IETF RFC 3313 (2003), *Private Session Initiation Protocol (SIP) Extensions for Media Authorization.*	[RFC3313]	"Private Session Initiation Protocol (SIP) Extensions for Media Authorization", TTC standard JF-IETF-RFC3313, The Telecommunication Technology Committee, May 2009
[IETF RFC 3320]	IETF RFC 3320 (2003), *Signaling Compression (SigComp).*	[RFC3320]	"Signaling Compression (SigComp)", TTC standard JF-IETF-RFC3320, The Telecommunication Technology Committee, May 2009
[IETF RFC 3323]	IETF RFC 3323 (2002), *A Privacy Mechanism for the Session Initiation Protocol (SIP).*	[RFC3323]	"A Privacy Mechanism for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3323, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3324]	IETF RFC 3324 (2002), *Short Term Requirements for Network Asserted Identity.*	[RFC3324]	"Short Term Requirements for Network Asserted Identity", TTC standard JF-IETF-RFC 3324, version 1, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3325]	IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.*	[RFC3325]	"Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", TTC standard JF-IETF-RFC3325, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3326]	IETF RFC 3326 (2002), *The Reason Header Field for the Session Initiation Protocol (SIP).*	[RFC3326]	"The Reason Header Field for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3326, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3327]	IETF RFC 3327 (2002), *Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts.*	[RFC3327]	"Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", TTC standard JF-IETF-RFC3327, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3329]	IETF RFC 3329 (2003), *Security Mechanism Agreement for the Session Initiation Protocol (SIP).*	[RFC3329]	"Security Mechanism Agreement for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3329, The Telecommunication Technology Committee, May 2009
[IETF RFC 3388]	IETF RFC 3388 (2002), *Grouping of Media Lines in the Session Description Protocol (SDP).*	[RFC3388]	"Grouping of Media Lines in the Session Description Protocol (SDP)", TTC standard JF-IETF-RFC3388, The Telecommunication Technology Committee, May 2009
[IETF RFC 3420]	IETF RFC 3420 (2002), *Internet Media Type message/sipfrag.*	[RFC3420]	"Internet Media Type message/sipfrag", TTC standard JF-IETF-RFC3420, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3428]	IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging.*	[RFC3428]	"Session Initiation Protocol (SIP) Extension for Instant Messaging, TTC standard JF-IETF-RFC3428, The Telecommunication Technology Committee, Sep 2006
[IETF RFC 3455]	IETF RFC 3455 (2003), *Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP).*	[RFC3455]	"Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", TTC standard JF-IETF-RFC3455, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3485]	IETF RFC 3485 (2003), *The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp).*	[RFC3485]	"The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signaling Compression (SigComp)", TTC standard JF-IETF-RFC3485, The Telecommunication Technology Committee, May 2009
[IETF RFC 3486]	IETF RFC 3486 (2003), *Compressing the Session Initiation Protocol (SIP).*	[RFC3486]	"Compressing the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3486, The Telecommunication Technology Committee, May 2009
[IETF RFC 3515]	IETF RFC 3515 (2003), *The Session Initiation Protocol (SIP) Refer Method.*	[RFC3515]	"The Session Initiation Protocol (SIP) Refer Method", TTC standard JF-IETF-RFC3515, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3524]	IETF RFC 3524 (2003), *Mapping of Media Streams to Resource Reservation Flows.*	[RFC3524]	"Mapping of Media Streams to Resource Reservation Flows", TTC standard JF-IETF-RFC3524, The Telecommunication Technology Committee, May 2009

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 3556]	IETF RFC 3556 (2003), *Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth.*	[RFC3556]	"Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth", TTC standard JF-IETF-RFC3556, The Telecommunication Technology Committee, May 2009
[IETF RFC 3581]	IETF RFC 3581 (2003), *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing.*	[RFC3581]	"An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing", TTC standard JF-IETF-RFC3581, The Telecommunication Technology Committee, May 2009
[IETF RFC 3608]	IETF RFC 3608 (2003), *Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration.*	[RFC3608]	"Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration", TTC standard JF-IETF-RFC3608, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3680]	IETF RFC 3680 (2004), *A Session Initiation Protocol (SIP) Event Package for Registrations.*	[RFC3680]	"A Session Initiation Protocol (SIP) Event Package for Registrations", TTC standard JF-IETF-RFC3680, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3725]	IETF RFC 3725 (2004), *Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP).*	[RFC3725]	"Best Current Practices for Third Party Call Control (3pcc) in the Session Initiation Protocol (SIP) ", TTC standard JF-IETF-RFC3725, The Telecommunication Technology Committee, May 2009
[IETF RFC 3824]	IETF RFC 3824 (2004), *Using E.164 numbers with the Session Initiation Protocol (SIP).*	[RFC3824]	"Using E.164 numbers with the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3824, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3840]	IETF RFC 3840 (2004), *Indicating User Agent Capabilities in the Session Initiation Protocol (SIP).*	[RFC3840]	"Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3840, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3841]	IETF RFC 3841 (2004), *Caller Preferences for the Session Initiation Protocol (SIP).*	[RFC3841]	"Caller Preferences for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3841, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3842]	IETF RFC 3842 (2004), *A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP).*	[RFC3842]	"A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3842, The Telecommunication Technology Committee, May 2009
[IETF RFC 3853]	IETF RFC 3853 (2004), *S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP).*	[RFC3853]	"S/MIME Advanced Encryption Standard (AES) Requirement for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3853, The Telecommunication Technology Committee, May 2009
[IETF RFC 3856]	IETF RFC 3856 (2004), *A Presence Event Package for the Session Initiation Protocol (SIP).*	[RFC3856]	"A Presence Event Package for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3856, The Telecommunication Technology Committee, May 2009
[IETF RFC 3857]	IETF RFC 3857 (2004), *A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP).*	[RFC3857]	"A Watcher Information Event Template-Package for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3857, The Telecommunication Technology Committee, May 2009
[IETF RFC 3858]	IETF RFC 3858 (2004), *An Extensible Markup Language (XML) Based Format for Watcher Information.*	[RFC3858]	"An Extensible Markup Language (XML) Based Format for Watcher Information", TTC standard JF-IETF-RFC3858, The Telecommunication Technology Committee, Mar 2008
[IETF RFC 3859]	IETF RFC 3859 (2004), *Common Profile for Presence (CPP).*	[RFC3859]	"Common Profile for Presence (CPP)", TTC standard JF-IETF-RFC3859, The Telecommunication Technology Committee, May 2009
[IETF RFC 3860]	IETF RFC 3860 (2004), *Common Profile for Instant Messaging (CPIM).*	[RFC3860]	"Common Profile for Instant Messaging (CPIM)", TTC standard JF-IETF-RFC3860, The Telecommunication Technology Committee, May 2009
[IETF RFC 3861]	IETF RFC 3861 (2004), *Address Resolution for Instant Messaging and Presence.*	[RFC3861]	"Address Resolution for Instant Messaging and Presence", TTC standard JF-IETF-RFC3861, The Telecommunication Technology Committee, May 2009
[IETF RFC 3862]	IETF RFC 3862 (2004), *Common Presence and Instant Messaging (CPIM): Message Format.*	[RFC3862]	"Common Presence and Instant Messaging (CPIM): Message Format", TTC standard JF-IETF-RFC3862, The Telecommunication Technology Committee, May 2009
[IETF RFC 3863]	IETF RFC 3863 (2004), *Presence Information Data Format (PIDF).*	[RFC3863]	"Presence Information Data Format (PIDF)", TTC standard JF-IETF-RFC3863, The Telecommunication Technology Committee, May 2009
[IETF RFC 3891]	IETF RFC 3891 (2004), *The Session Initiation Protocol (SIP) Replaces Header.*	[RFC3891]	"The Session Initiation Protocol (SIP) "Replaces" Header", TTC standard JF-IETF-RFC3891, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3892]	IETF RFC 3892 (2004), *The Session Initiation Protocol (SIP) Referred-By Mechanism.*	[RFC3892]	"The Session Initiation Protocol (SIP) Referred-By Mechanism", TTC standard JF-IETF-RFC3892, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 3903]	IETF RFC 3903 (2004), *Session Initiation Protocol (SIP) Extension for Event State Publication.*	[RFC3903]	"Session Initiation Protocol (SIP) Extension for Event State Publication", TTC standard JF-IETF-RFC3903, The Telecommunication Technology Committee, Mar 2007

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 3911]	IETF RFC 3911 (2004), *The Session Initiation Protocol (SIP) Join Header.*	[RFC3911]	"The Session Initiation Protocol (SIP) "Join" Header", TTC standard JF-IETF-RFC3911, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3959]	IETF RFC 3959 (2004), *The Early Session Disposition Type for the Session Initiation Protocol (SIP).*	[RFC3959]	"The Early Session Disposition Type for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3959, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3960]	IETF RFC 3960 (2004), *Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP).*	[RFC3960]	"Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC3960, The Telecommunication Technology Committee, Aug 2006
[IETF RFC 3966]	IETF RFC 3966 (2004), *The tel URI for Telephone Numbers.*	[RFC3966]	"The tel URI for Telephone Numbers", TTC standard JF-IETF-RFC3966, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3994]	IETF RFC 3994 (2005), *Indication of Message Composition for Instant Messaging.*	[RFC3994]	"Indication of Message Composition for Instant Messaging", TTC standard JF-IETF-RFC3994, The Telecommunication Technology Committee, May 2009
[IETF RFC 4028]	IETF RFC 4028 (2005), *Session Timers in the Session Initiation Protocol (SIP).*	[RFC4028]	"Session Timers in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4028, The Telecommunication Technology Committee, Aug 2005
[IETF RFC 4032]	IETF RFC 4032 (2005), *Update to the Session Initiation Protocol (SIP) Preconditions Framework.*	[RFC4032]	"Update to the Session Initiation Protocol (SIP) Preconditions Framework", TTC standard JF-IETF-RFC4032, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4145]	IETF RFC 4145 (2005), *TCP-Based Media Transport in the Session Description Protocol (SDP).*	[RFC4145]	"TCP-Based Media Transport in the Session Description Protocol (SDP)", TTC standard JF-IETF-RFC4145, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 4168]	IETF RFC 4168 (2005), *The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP).*	[RFC4168]	"The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4168, The Telecommunication Technology Committee, May 2009
[IETF RFC 4235]	IETF RFC 4235 (2005), *An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)*	[RFC4235]	"An INVITE Initiated Dialog Event Package for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4235, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4244]	IETF RFC 4244 (2005), *An Extension to the Session Initiation Protocol (SIP) for Request History Information.*	[RFC4244]	"An Extension to the Session Initiation Protocol (SIP) for Request History Information", TTC standard JF-IETF-RFC4244, The Telecommunication Technology Committee, Aug 2006
[IETF RFC 4320]	IETF RFC 4320 (2006), *Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction.*	[RFC4320]	"Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction", TTC standard JF-IETF-RFC4320, The Telecommunication Technology Committee, May 2009
[IETF RFC 4412]	IETF RFC 4412 (2006), *Communications Resource Priority for the Session Initiation Protocol (SIP).*	[RFC4412]	"Communications Resource Priority for the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC4412, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4458]	IETF RFC 4458 (2006), *Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR).*	[RFC4458]	"Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)", TTC standard JF-IETF-RFC4458, The Telecommunication Technology Committee, Aug 2006
[IETF RFC 4480]	IETF RFC 4480 (2006), *RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF).*	[RFC4480]	"RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)", TTC standard JF-IETF-RFC4480, The Telecommunication Technology Committee, May 2009
[IETF RFC 4483]	IETF RFC 4483 (2006), *A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages.*	[RFC4483]	"A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages", TTC standard JF-IETF-RFC4483, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4566]	IETF RFC 4566 (2006), *SDP: Session Description Protocol.*	[RFC4566]	"SDP: Session Description Protocol", TTC standard JF-IETF-RFC4566, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 4575]	IETF RFC 4575 (2006), *A Session Initiation Protocol (SIP) Event Package for Conference State.*	[RFC4575]	"A Session Initiation Protocol (SIP) Event Package for Conference State", TTC standard JF-IETF-RFC4575, The Telecommunication Technology Committee, May 2009
[IETF RFC 4579]	IETF RFC 4579 (2006), *Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents.*	[RFC4579]	"Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents", TTC standard JF-IETF-RFC4579, The Telecommunication Technology Committee, May 2009
[IETF RFC 4583]	IETF RFC 4583 (2006), *Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams.*	[RFC4583]	"Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams", TTC standard JF-IETF-RFC4583, The Telecommunication Technology Committee, May 2009

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 4662]	IETF RFC 4662 (2006), *A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists.*	[RFC4662]	"A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists", TTC standard JF-IETF-RFC4662, The Telecommunication Technology Committee, May 2009
[IETF RFC 4715]	IETF RFC 4715 (2006), *The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI.*	[RFC4715]	"The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI", TTC standard JF-IETF-RFC4715, The Telecommunication Technology Committee, Mar 2007
[IETF RFC 4730]	IETF RFC 4730 (2006), *A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML).*	[RFC4730]	"A Session Initiation Protocol (SIP) Event Package for Key Press Stimulus (KPML)", TTC standard JF-IETF-RFC4730, The Telecommunication Technology Committee, May 2009
[IETF RFC 5031]	IETF RFC 5031 (2008), *A Uniform Resource Name (URN) for Emergency and Other Well-Known Services.*	[RFC5031]	"A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", TTC standard JF-IETF-RFC5031, The Telecommunication Technology Committee, May 2009
[IETF RFC 5049]	IETF RFC 5049 (2007), *Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP).*	[RFC5049]	"Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC5049, The Telecommunication Technology Committee, May 2009
[IETF RFC 5079]	IETF RFC 5079 (2007), *Rejecting Anonymous Requests in the Session Initiation Protocol (SIP).*	[RFC5079]	"Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC5079, The Telecommunication Technology Committee, May 2009

Table 1-c/ JT-Q3402: Modifications of references (IETF references / Transport-level specifications)

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 3016]	IETF RFC 3016 (2000), *RTP Payload Format for MPEG-4 Audio/Visual Streams.*	[RFC3016]	"RTP Payload Format for MPEG-4 Audio/Visual Streams", TTC standard JF-IETF-RFC3016, The Telecommunication Technology Committee, May 2009
[IETF RFC 3047]	IETF RFC 3047 (2001), *RTP Payload Format for ITU-T Recommendation G.722.1.*	[RFC3047]	"RTP Payload Format for ITU-T Recommendation G.722.1", TTC standard JF-IETF-RFC3047, The Telecommunication Technology Committee, May 2009
[IETF RFC 3267]	IETF RFC 3267 (2002), *Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs.*	[RFC3267]	"Real-time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs", TTC standard JF-IETF-RFC3267, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3389]	IETF RFC 3389 (2002), *Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN).*	[RFC3389]	"RTP Payload for Comfort Noise", TTC standard JF-IETF-RFC3389, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 3550]	IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications.*	[RFC3550]	"RTP: A Transport Protocol for Real-Time Applications", TTC standard JF-IETF-STD64, The Telecommunication Technology Committee, May 2005
[IETF RFC 3551]	IETF RFC 3551 (2003), *RTP Profile for Audio and Video Conferences with Minimal Control.*	[RFC3551]	"RTP Profile for Audio and Video Conferences with Minimal Control", TTC standard JF-IETF-STD65, The Telecommunication Technology Committee, Jun 2005
[IETF RFC 3558]	IETF RFC 3558 (2003), *RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV).*	[RFC3558]	"RTP Payload Format for Enhanced Variable Rate Codecs (EVRC) and Selectable Mode Vocoders (SMV)", TTC standard JF-IETF-RFC3558, The Telecommunication Technology Committee, May 2009
[IETF RFC 3611]	IETF RFC 3611 (2003), *RTP Control Protocol Extended Reports (RTCP XR).*	[RFC3611]	"RTP Control Protocol Extended Reports (RTCP XR)", TTC standard JF-IETF-RFC3611, The Telecommunication Technology Committee, Mar 2008
[IETF RFC 3711]	IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP).*	[RFC3711]	"The Secure Real-time Transport Protocol (SRTP)", TTC standard JF-IETF-RFC3711, The Telecommunication Technology Committee, May 2009
[IETF RFC 3984]	IETF RFC 3984 (2005), *RTP Payload Format for H.264 Video.*	[RFC3984]	"RTP Payload Format for H.264 Video", TTC standard JF-IETF-RFC3984, The Telecommunication Technology Committee, May 2009
[IETF RFC 4103]	IETF RFC 4103 (2005), *RTP Payload for Text Conversation.*	[RFC4103]	"RTP Payload for Text Conversation", TTC standard JF-IETF-RFC4103, The Telecommunication Technology Committee, Nov 2007
[IETF RFC 4348]	IETF RFC 4348 (2006), *Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec.*	[RFC4348]	"Real-Time Transport Protocol (RTP) Payload Format for the Variable-Rate Multimode Wideband (VMR-WB) Audio Codec", TTC standard JF-IETF-RFC4348, The Telecommunication Technology Committee, May 2009
[IETF RFC 4629]	IETF RFC 4629 (2007), *RTP Payload Format for ITU-T Rec. H.263 Video.*	[RFC4629]	"RTP Payload Format for ITU-T Rec. H.263 Video", TTC standard JF-IETF-RFC4629, The Telecommunication Technology Committee, May 2009

Reference in ITU-T Q.3402		Modified Reference in TTC JT-Q3402	
[IETF RFC 4733]	IETF RFC 4733 (2006), *RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals.*	[RFC4733]	"RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals", TTC standard JF-IETF-RFC4733, The Telecommunication Technology Committee, May 2009
[IETF RFC 4749]	IETF RFC 4749 (2006), *RTP Payload Format for the G.729.1 Audio Codec.*	[RFC4749]	"RTP Payload Format for the G.729.1 Audio Codec", TTC standard JF-IETF-RFC4749, The Telecommunication Technology Committee, May 2009

Annex a. Clarification and option lists of JT-Q3402 main body

(This annex is a normative part of this standard.)

a.1. Overview

This annex provides clarification and option lists of the JT-Q3402 main body to improve the interoperability of SIP terminals to the NGN connected through the UNI in the architecture defined in the JT-Q3402 main body.

a.2. References

References used in this annex are as follows.

[RFC4585] "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)", TTC standard JF-IETF-RFC4585, version 1.0, Mar 2008

[RFC5104] "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)", TTC standard JF-IETF-RFC5104, version 1.0, Mar 2008

[RFC5407] "Example calls flows of race conditions in the Session Initiation Protocol (SIP)", TTC standard JF-IETF-RFC5407, version 1.1, Nov 2009

a.3. Clarification and option lists

Annex Table a-1 shows the clarification and option lists for the main body of TTC JT-Q3402. Clauses unmentioned in the table mean that specifications in the base document are applied as they are. Lists of options described in Annex a to Annex i and Appendix i to Appendix vi are not shown in Annex Table a-1. Refer to Appendix i for lists of options including these annexes and appendices.

Annex Table a-1/ JT-Q3402: Clarification and option lists

Clause of JT-Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
2.	References	References needed for this standard are described in each annex and appendix in addition to the base document.	–	
5	Reference model	In the case that the EUF is an audio telephone terminal, follow Annex i.	–	
6.	Assumptions	2. SRTP is not to be used for the transfer of audio and video	–	
7.1	Consideration related to media packets	Specifications in the base document are applied as they are.	Sending media packets from the originating terminal, in the case that a *1xx* response to *INVITE* includes SDP answer. (Appendix Table 1-25, Item 1) Handling of media packets before completion of SDP negotiation to an initial *INVITE* (Appendix Table 1-25, Item 2)	
8.1	Codec list	The audio codec list shall contain G.711μ-law. Even when a codec in the codec list is set in an SDP offer, it may not be end-to-end negotiation, depending on a carrier's policy. A codec that is not contained in the codec list is not to be set in an SDP offer.	Codecs to be contained in the codec list other than G.711μ-law. (Appendix Table 1-16, Items 1 to 3)	

Clause of JT-Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
8.2	Packetization size	For the packetization period in the case of using G.711μ-law, follow Annex i.2.1.	–	
9.	Routing and addressing	For the URI format in the case of using a national number, follow Annex b.6. For the subaddress, follow Annex b.7.	*Request-URI* format of SIP requests outside existing dialogs, except for *REGISTER*. (Appendix Table 1-20, Items 1 and 2)	
10.1	RFCs to be supported	RFC2976, RFC3388, RFC3725, RFC3824, RFC3853, RFC3861, RFC3959, RFC3960, RFC4168, RFC4244, RFC4412, RFC4458, and RFC5031 are not to be used. Support for the *P-Media-Authorization* header specified in RFC3313 is applicable only in the direction from the SCF to the EUF. For the handling of the *Reason* header specified in RFC 3326, follow Annex f.3.1. For the handling of the path extension function specified in RFC 3327, follow Annex c.3. Support for the *Path* header is applicable only to the response in the direction from the SCF to the EUF. Support for the *Security-Client* header and *Security-Verify* header specified in RFC3329 is applicable only to the request in the direction from the EUF to the SCF, and support for the *Security-Server* header is applicable only to the response in the direction from the SCF to the EUF. Of the headers specified in RFC3455, the *P-Associated-URI* header and the *P-Called-Party-ID* header are used, which conform to Annex b. The headers *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* are not to be used. Support for the *P-Access-Network-Info* header is applicable only to the SIP messages in the direction from the EUF to the SCF. For the handling of the *Service-Route* header specified in RFC 3608, follow Annex c.3.	The followings are the list of options for each RFC. [RFC2046] Use of MIME Multipart (Appendix Table 1-10, Items 1 to 4) [RFC3310, RFC2617, and RFC3329] Terminal authentication procedures (Appendix Table 1-11, Items 1 and 2) Use of security capabilities exchange function (*sec-agree*) (Appendix Table 1-7, Item 8) [RFC3262] Use of provisional response reliability function (*100rel*) (Appendix Table 1-7, Item 2) [RFC3265] Use of *SUBSCRIBE* method and *NOTIFY* method. (Appendix Table 1-2, Items 10 to 15) [RFC3311] SDP offer by *UPDATE* (Appendix Table 1-23, Items 1, 2, 5, and 6) Media modification in early dialog (Appendix Table 1-23, Items 1 and 2) [RFC3312, RFC4032] Use of function for reserving bandwidth before session establishment (*precondition*) (Appendix Table 1-7, Item 5) [RFC3313] Use of *P-Media-Authorization head*er (Appendix Table 1-17, Item 1)	

Clause of JT-Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
		For the registration event specified in RFC 3680, follow Annex c.6. Note: To support RFCs means to follow the contents described in the RFCs. It does not mean that their capabilities are used in all sessions.	[RFC3320, RFC3485, RFC3486, RFC5049] Use of SigComp (Appendix Table 1-5, Item 1) [RFC3388, RFC3524] Use of Grouping of media (Appendix Table 1-18, Item 1) [RFC3428] Use of *MESSAGE* method (Appendix Table 1-2, Items 2 to 5) [RFC3515, RFC3892] Use of *REFER* method (Appendix Table 1-2, Items 6 to 9) [RFC3556] Use of SDP bandwidth modifier for RTCP bandwidth (Appendix Table 1-13, Item 4) [RFC3581] Allowing Hosted NAT in the lower part of UNI (Appendix Table 1-6, Item 1) [RFC3840, RFC3841] Use of terminal capabilities notification function (*pref*) (Appendix Table 1-7, Item 6) [RFC3891] Use of dialog replacement function (*replaces*) (Appendix Table 1-7, Item 3) [RFC3903] Use of *PUBLISH* method (Appendix Table 1-2, Items 16 to 19) [RFC3911] Use of conference session participation function (*join*) (Appendix Table 1-7, Item 4) [RFC4028] Session refresh by *UPDATE* method (Appendix Table 1-8, Item 1)	
10.2.1.7	SIP Messages	For maximum length of SIP messages and its elements, follow Annex h.	–	
10.2.1.7.1	Requests	*OPTIONS* method is not to be used. SIPS-URI is not to be used.	–	

Clause of JT-Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
10.2.1.7.4.1	Message body types	Specifications in the base document are applied as they are.	SDP settings for *PRACK* and *200 OK* to *PRACK*. (Appendix Table 1-22, Items 2 and 3)	
10.2.1.8.1.3	Processing responses	Specifications in the base document are applied as they are.	Terminal authentication procedures (Appendix Table 1-11, Items 1 and 2)	
10.2.1.8.3	Redirect servers	Specifications in the base document are applied as they are. The *3xx* response is applicable to requests outside existing dialogs, except for *REGISTER*.	Use of redirect functions by *3xx* response (Appendix Table 1-12, Items 1 and 2)	
10.2.1.10	Registrations	For the terminal registration procedures, follow Annex c. For the congestion control at the time of terminal registration, follow Annex f.2.	Whether or not terminal registration needed and procedures (Appendix Table 1-2, Item 1, Appendix Table 1-11, Item 1, and Appendix Table 1-24, Items 1 to 5)	
10.2.1.11	Querying for capabilities	Querying for capabilities is not supported.	–	
10.2.1.12.1	Creation of a dialog	SIPS-URI is not to be used.	–	
10.2.1.12.2	Requests within a dialog	SIPS-URI is not to be used.	–	
10.2.1.13	Initiating a session	Initial *INVITE* includes an SDP offer which contains valid media. (SDP negotiation using *2xx*/*ACK* is not to be used.) Follow Annex f.3 for congestion control at the time of call origination.	–	
10.2.1.14	Modifying an existing session	In the case of using re-*INVITE*, SDP offer is set in *INVITE* request.	Media modification after a dialog is established. (Appendix Table 1-23, Items 3 to 6)	
10.2.1.17	Transactions	For the processing at race conditions triggered by SIP signalling crossover etc., conform to [RFC5407]. Note that this standard lists a sequence between SIP-UAs, and when applying to the UNI, it should be read as sequence between network and terminal.	–	
10.2.1.19	Common message components	SIPS-URI is not to be used.	–	
10.2.1.20.7	Authorization	The Authorization header is used only when the SCF authenticates a *REGISTER* request from the EUF.	–	
10.2.1.20.11	Content-Disposition	Only the default value can be set in the parameter of the *Content-Disposition* header. Application server model as defined in RFC3959 is not to be used.	–	
10.2.1.20.27	Proxy-Authenticate	The *Proxy-Authenticate* header is used only in the *407* response when the SCF authenticates a request sent from the EUF outside existing dialogs except for *REGISTER*.	–	

Clause of JT-Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
10.2.1.20.28	Proxy-Authorization	The *Proxy-Authorization* header is used only when the SCF authenticates a request sent from the EUF outside existing dialogs except for *REGISTER*.	–	
10.2.1.20.29	Proxy-Require	The *Proxy-Require* header is applicable only in the direction from the EUF to the SCF.	–	
10.2.1.20.24	MIME-Version	Only "1.0" is supported	–	
10.2.1.20.32	Require	Application server model as defined in RFC3959 is not to be used.	Use of *timer*, *100rel,* and other SIP option tags (Appendix Table 1-7, Items 1 to 9)	
10.2.1.20.33	Retry-After	For congestion control, the *Retry-After* header is utilized as described in Annex f.2.1.	–	
10.2.1.20.34	Route	For the pre-existing route, follow Annex c.3.	–	
10.2.1.20.44	WWW-Authenticate	The *WWW-Authenticate* header is used only in *401* responses when the SCF authenticates a *REGISTER* request from the EUF.	–	
10.2.1.23	S/MIME	S/MIME is not to be used for SDP with SIP messages related to *INVITE*.	–	
10.2.2.1	Extension method	For *UPDATE* and *PRACK* requests, follow Annex d.	–	
10.2.2.2.2	P-Asserted-Identity	The *P-Asserted-Identity* header is used only in requests outside existing dialogs except for *REGISTER*. For calling line identification presentation, follow Annex b.	–	
10.2.2.2.3	P-Preferred-Identity	The *P-Preferred-Identity* header is used only in requests outside existing dialogs except for *REGISTER*. For calling line identification presentation, follow Annex b.	–	
10.2.2.2.4	Privacy	The *Privacy* header is used only in requests outside existing dialogs except for *REGISTER*. Only "*id*" and "*none*" can be used for privacy options. For calling line identification presentation, follow Annex b.	–	
10.2.3	Summary of SIP methods and headers	*OPTIONS* method is not to be used.	SIP methods to be used (Appendix Table 1-2, Items 1 to 21)	

Clause of JT-Q3402 main body		Clarifications	Options	Remarks
No.	Name of clause			
10.3.1	SDP usage	For the handling of SDP, follow Annex e. For the values specified in *b=* line, follow Annex g.	SDP lines to be used (Appendix Table 1-22, Items 4 and 5) IP version to be used for media (Appendix Table 1-3, Item 3) Use of video (*m=video*) and data communication (*m=appli cation*, *m=data*, etc.) (Appendix Table 1-14, Items 1 and 2) Use of TCP for media [RFC 4145] (Appendix Table 1-14, Item 3)	
11.1	Specifications to be supported	Specifications in the base document are applied as they are. Feedback function utilizing RTCP (RTP/AVPF)[RFC4585][RFC5104] can be used.	Use of feedback function utilizing RTCP (Appendix Table 1-19, Items 1 and 2)	
12	Call control signalling transport	UDP or TCP is used as transport protocol for sending and receiving SIP messages. TLS may be used for security.	Layer 4 protocol for call control signals (Appendix Table 1-4, Items 1 to 3)	
13	IP protocol version	Specifications in the base document are applied as they are. Refer to Annex e.4.1 for a note of IPv4/IPv6 fallback.	Layer 3 protocol for call control signals (Appendix Table 1-3, Items 1 to 4)	

Annex b. Calling line identification presentation and related headers

(This annex is a normative part of this standard.)

b.1. Overview

This annex clarifies procedures for calling line identification presentation and notification of "cause of no ID", SIP headers used for them (*P-Preferred-Identity*, *P-Asserted-Identity*, *Privacy*, and *From*) and *Request-URI*, the SIP header used for relevant network-asserted user identity (*P-Associated-URI*), and the SIP header used for called party notification (*P-Called-Party-ID*).

b.2. References

References used in this annex are as follows.

[TS-1008] "Technical Specification on ISDN Calling and Called Party Subaddress Information Transferring", TTC Technical Specification TS-1008, version 2, The Telecommunication Technology Committee, Oct 2014

b.3. Network-asserted user identity

The network-asserted user identity is the identity of a user that is asserted by the network through authentication or other means (verified by the network if provided by the terminal), and it is used for calling-party identity, etc. An example of network-asserted user identity information is a SIP-URI composed of an E.164 number reachable to the terminal. As described in clause b.7, subaddress information may be provided by the calling terminal.

Clause b.6 indicates a specific URI format for network-asserted user identity.

b.3.1. Notification when the terminal registers

In the case of using a *REGISTER* request for registration, the network may set a *P-Associated-URI* header [RFC3455] in its *200 OK* response in order to notify a network-asserted user identity to the terminal. [Appendix Table 1-24, Item 3]

A *P-Associated-URI* header lists one or more URIs which indicate network-asserted user identities allocated to the terminal. In the case that multiple network-asserted user identities are listed, the terminal recognizes the first URI as the default network-asserted user identity.

b.4. Calling party numbers

Calling party number (hereinafter referred to as calling-party identity) presentation should be realized based on JF-IETF-RFC3323[RFC3323], JF-IETF-RFC3324[RFC3324], and JF-IETF-RFC3325[RFC3325] by notifying network-asserted user identity and presentation/restriction information. Calling-party identity presentation/restriction are applied to requests outside existing dialogs except for *REGISTER* which can be sent and received over the UNI.

Calling-party identity information presentation is mainly performed by four steps as follows.

1) A calling terminal transmits the selected calling-party identity information (*P-Preferred-Identity*) and preference of presentation/restriction (*Privacy*) to a network, instructs a destination (*Request-URI*), and calls.
2) The network which has the calling party verifies and normalizes a calling-party identity that a terminal selected, takes into consideration the default presentation/restriction setting etc. regarding the subscriber, and determines a calling-party identity information transmitted in the network and through the NNI.

3) The network which has the called party takes into consideration the preference of presentation/restriction and the called party's subscription for calling-party identity presentation service, and determines a calling-party identity information to be notified to the called terminal.

4) The called terminal is notified of calling-party identity information from the network when receiving a call.

In this annex, clause b.4.1 describes step 1 and 2 as procedures on originating a call, and clause b.4.2 describes step 3 and 4 as procedures on terminating a call.

b.4.1. Procedures on originating a call

b.4.1.1. Selecting a calling-party identity

In the case that a terminal desires to explicitly select a calling-party identity among the network-asserted identities, the terminal populates the selected network-asserted user identity in *P-Preferred-Identity* header in requests outside existing dialogs. If network-asserted user identities are notified as described in clause b.3.1, the terminal selects one of the URIs listed in a *P-Associated-URI* header and populates it in the *P-Preferred-Identity* header.

The network handles a SIP-URI set in the *P-Preferred-Identity* header as calling-party identity. Note that in the case the *P-Preferred-Identity* header is not set, or a URI set in the *P-Preferred-Identity* header is not a network-asserted user identity allocated to the calling terminal, it is h to be the same as when the default network-asserted user identity is set in the *P-Preferred-Identity* header.

b.4.1.2. Setting for presentation/restriction of calling-party identity

When a terminal sends requests outside existing dialogs, calling-party identity presentation/restriction is requested using two kinds of procedures, namely, *Privacy* header [RFC3325] and 186/184 prefixes.

- Calling-party identity presentation can be requested by setting "*none*" in *Privacy* header, and restricted by setting "*id*". The *Privacy* header is set only when the terminal has the user configuration option of calling-party identity presentation/restriction, and the user completes the setting.
- In the case that the *Request-URI* is a URI composed of a national telephone number, calling-party identity presentation is specified when the 186 prefix is set, and restriction is specified when the 184 prefix is set. Whether to set the 186/184 prefix must be left to the decision of a dialling user, and a terminal must not act on its own, such as automatically putting the prefix.

The settings of the *Privacy* header and those of the 186/184 prefix are independent of each other.

In the case that the terminal sets "*id*" in a *Privacy* header, *<sip:anonymous@anonymous.invalid>* is set to the SIP-URI of a *From* header. In other cases, a URI identical to that of a *P-Preferred-Identity* header is set.

Annex Table b-1 describes the contents set in the headers above.

Annex Table b-1/JT-Q3402: Settings of headers for calling line identification presentation

Field	Privacy header		
	none	id	No header
The *user* part or *telephone-subscriber* part of a *Request-URI*	Number that a user dialled (includes 186/184 prefix if dialled)		
P-Preferred-Identity header	Calling-party's network-asserted user identity		
URI in *To* header	Same value as *Request-URI*		
name-addr in *From* header	Same value as the URI set in a *P-Preferred-Identity* header, if the header is set	<sip:anonymous@anonymous.invalid>	Same value as the URI set in a *P-Preferred-Identity* header, if the header is set

A network selects calling-party identity presentation/restriction, based on the *Privacy* header and 186/184 prefix setting, and the default calling-party identity presentation/restriction setting of a subscriber who originates a call.

- In the case that a 186/184 prefix is set at the beginning of the telephone number in the *Request-URI*, the call is treated to be calling-party identity presentation when 186 is set, and calling-party identity restriction when 184 is set, regardless of a *Privacy* header setting content.
- The default calling-party identity presentation setting of the subscriber who originates the call is applied when neither the *Privacy* header setting nor a 186/184 prefix setting exists.
- In the case that the 184 prefix is not set, it is treated to be calling-party identity presentation, regardless of a Privacy header setting content, at the time of emergency call.

Annex tables b-2 and b-3 describe the order of priority among the *Privacy* header settings, 186/184 prefix settings, and the default calling-party identity presentation/restriction setting above.

Annex Table b-2/JT-Q3402: Calling-party identity presentation/restriction selection conditions for normal call

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">Prefix of destination number</td></tr>
<tr><td>186</td><td>184</td><td>No prefix</td></tr>
<tr><td rowspan="3">Privacy</td><td>none</td><td rowspan="3">Calling-party identity presentation</td><td rowspan="3">Calling-party identity restriction</td><td>Calling-party identity presentation</td></tr>
<tr><td>id</td><td>Calling-party identity restriction</td></tr>
<tr><td>No header</td><td>Follow the default value of the network managed for each calling user</td></tr>
</table>

Annex Table b-3/JT-Q3402: Network selected conditions of presentation/restriction of calling-party identity for emergency call

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">Prefix of a destination number</td></tr>
<tr><td>186</td><td>184</td><td>No prefix</td></tr>
<tr><td rowspan="3">Privacy</td><td>none</td><td rowspan="3">Calling-party identity presentation</td><td rowspan="3">Calling-party identity restriction</td><td rowspan="3">Calling-party identity presentation</td></tr>
<tr><td>id</td></tr>
<tr><td>No header</td></tr>
</table>

In the case that the calling-party identity is restricted, "*Anonymous*" (No caller ID: rejected by user) is selected as cause of no ID out of causes described in Annex Table b-4.

b.4.2. Procedures on receiving a call

The SIP headers on the terminating side are populated according to the called-party's subscription of calling-party identity presentation/restriction.

b.4.2.1. In the case that calling-party identity, cause of no ID, etc. are notified

The calling-party identity and cause of no ID, etc. are notified by setting a *Privacy* header in requests outside existing dialogs received from a network.

In the case that "*none*" is set in the *Privacy* header, calling-party identity is notified by a *P-Asserted-Identity* header. In the *P-Asserted-Identity* header, only a SIP-URI is set or both a SIP-URI and a TEL-URI are set.

In the case that "*id*" is set in the *Privacy* header, calling-party identity is not notified by the *P-Asserted-Identity* header. Instead, cause of no ID is set in *display-name* in a *From* header. In the case that calling-party identity is not notified, a displayed content (meaning) may be provided as cause of no ID in the form indicated in Annex Table b-4. Note that the cause of no ID is not provided in the case that a format is not as shown in Annex Table b-4.

Annex Table b-4/JT-Q3402: Cause of no ID

Received content (*1)(*2)	Display content (meaning)
Anonymous	No caller ID: rejected by user
Coin line/payphone	No caller ID: call from public telephone
Interaction with other service	No caller ID: service conflict
Unavailable	No caller ID: service unavailable

(*1) It may be enclosed with a pair of double quotation marks.
(*2) A character string listed in this table may be followed by a given character string.

b.4.2.1.1. Displaying calling-party identity

A terminal displays calling-party identity notified by a *P-Asserted-Identity* header according to the order of priority described below.

1) In the case that both a SIP-URI and a TEL-URI are set in a *P-Asserted-Identity* header, the TEL-URI is preferred for display.
2) In the case that display-name is set in the URI of a *P-Asserted-Identity* header, *display-name* is preferred for display rather than *addr-spec*.

In the case that *display-name* is not set, *user* part of a SIP-URI, *local-number-digits* part or *global-number-digits* part of a TEL-URI is displayed, and this part is a character string indicated in the display content in Annex Table b-5, a display content (meaning) corresponding to each case is indicated.

Annex Table b-5/JT-Q3402: Content of caller number display

Received content (*1)	Display content (meaning)
Only numbers	Received numeric string
Starting with +81, and the part after + is composed of only numbers	Numeric string that omits +81 and starts with 0
Starting with +, the part after + is all composed of numbers, and the part next to + is not 81.	Numeric string that omits + and starts with 010

(*1) When used as *display-name*, it may be enclosed with a pair of double quotation marks.

b.4.2.2. In the case that calling-party identity, cause of no ID, etc. are not notified

A *Privacy* header and a *P-Asserted-Identity* header are not set, and a character string which indicates cause of no ID is not set in *display-name* in a *From* header.

b.5. Destination notification

A network may populate a *P-Called-Party-ID* header [RFC3455] in requests outside existing dialogs to a called terminal, and may set a URI which indicates a network-asserted user identity of the destination.

In the case that multiple network-asserted user identities are allocated, a terminal uses a *P-Called-Party-ID* header in order to identity towards which network-asserted user identity a call is directed. In the case that the *P-Called-Party-ID* header is not set, it should be recognized that the call is directed to the default network-asserted user identity.

b.6. URI format in the case that a national number is used

This clause describes a URI format for the case using a national number as network-asserted user identity and *Request-URI*. Other URI formats may be used. [Appendix Table 1-20, Item 1]

A SIP-URI or a TEL-URI is used for network-asserted user identity. Either one or multiple SIP-URIs are allocated as network-asserted user identity for each user. A SIP-URI or a TEL-URI is used for *Request-URI*.

A subaddress described in clause b.7 may be set.

b.6.1. user part and local-number-digits part

In a SIP-URI, a numeric string of national number is described in *user* part, and in a TEL-URI, a numeric string of national number is described in *local-number-digits* part. Note that letters equivalent to *visual-separator* are not to be used in either *user* part or *local-number-digits* part.

In the case of *Request-URI*, a numeric string that a user dialled is set as it is in the *user* part or in the *local-number-digits* part. In the case of network-asserted user identity, all digits of a telephone number starting with a national prefix (i.e., "0") are set.

b.6.2. hostport part and descriptor part of context

The *hostport* part of a SIP-URI and the *descriptor* part of TEL-URI *context* are to be set as domain name or host name (including IP address) that a network specifies. [Appendix 1-20, Item 2]

b.7. Subaddress

A network may provide services that are equivalent to services realized by the transfer of subaddress information that can be provided in the ISUP network through the interconnection interface as defined in JJ-90.10. [Appendix Table 1-9, Items 1 and 2]

This annex shows the usage of subaddress information in SIP messages based on [TS-1008] and complement the standard. The network and terminals, which handle subaddress information, are required to follow this clause and its subclauses. As for [TS-1008], follow the specifications for UNI in [TS-1008].

b.7.1. Subaddress information

b.7.1.1. Contents of subaddress information

The subaddress is a numeric string of 19 digits or less using numbers 0 to 9. The details are based on [RFC4715] and [TS-1008].

b.7.1.2. Formats of subaddress information

Subaddress information is applied to all the requests and responses of SIP messages and may be set in the headers that show the originating party (*From*, *P-Preferred-Identity*, *P-Asserted-Identity*), headers that show the terminating party (*To*, *P-Called-Party-ID*), and *Request-URI*. Subaddress is expressed as a numeric string following a semicolon (;) and "isub=" in the *user* part of SIP URI or TEL URI.

Annex c. Registration

(This annex is a normative part of this standard.)

c.1. Overview

This annex describes the procedures of terminal registration.

c.2. Obtaining the network address

A network provides a terminal with a means of notifying a SCF IP address and port number. The network provides DHCP/DHCPv6, presetting, and other procedures that depend on access line. [Appendix Table 1-24, Item 2]

The terminal transmits SIP messages to the obtained IP address and port number.

c.3. Registration

A terminal registers by sending to a network a *REGISTER* request in which a *Contact address* that it wants to register is set. A network may determine the setting conditions of the *q* parameter to the *Contact address*. [Appendix Table 1-24, Item 6]

The network may specify the *expires* parameter of a *Contact address* or the value set to an *Expires* header in the *REGISTER* request as a network option. [Appendix Table 1-24, Item 4]

c.3.1. path extension function and Service-Route header

A network may provide a pre-existing route using path extension function and *Service-Route* header. [Appendix Table 1-7, Item 7, Appendix Table 1-23, Item 1]

In the case that a network provides a pre-existing route, a terminal lists path extension function in *Supported* header as described in JF-IETF-RFC3327[RFC3327] and sends a *REGISTER* request. In the case that registration succeeds, a network sets a *Service-Route* header [RFC3608] in a *200 OK* response, and notifies the SIP-URI on or after the second hop of the pre-existing route.

c.3.2. pre-existing route

In the case that a pre-existing route is provided using procedures described in clause c.3.1, a terminal set the pre-existing route in *Route* header when sending requests outside existing dialogs except for *REGISTER*. The first hop of the *Route* header shall contain a SIP-URI of the obtained SCF address provided in clause c.2 with loose-routing specifier (i.e., ";lr"). The second and further hops of the *Route* header shall contain the given pre-existing route according to procedures as described in clause c.3.1. For a *REGISTER* request, pre-existing route is not provided.

c.3.3. Difference of address format retained by network

There may be a difference between a *Contact address* registered by a network and a *Contact address* set in a *REGISTER* request by a terminal. A terminal must be aware of it when verifying the *Contact address* URI.

- A URI parameter unrecognized by a network may not be retained.
- A *Contact address* may be retained in the format specifying no port number in a network, even if the default SIP port number (5060) is specified in the hostport part. The opposite could also be true that a *Contact address* may be retained in the format with the default port number (5060) in a network, even when the port number is not specified.

c.4. Refresh

In the case of receiving a *200 (OK)* response from a network indicating completion of registration or refresh, a terminal records the *Contact address* requested by the *REGISTER* request, and the retention period (Z s) returned by the *expires* parameter or in the *Expires* header field in the response.

Refresh interval (T s) MUST be set so that it does not exceed the retention period (Z s) and it does not cause frequent *REGISTER* request submissions. For example, setting the interval to a certain percentage of the retention period (Z s) is a good idea. The interval must be shorter than the value of retention period (Z s) minus Timer F (=32 s) specified in JF-IETF-RFC3261 [RFC3261] period in order to avoid expiration during resending the *REGISTER* request for refreshing. The refresh interval may be specified as a network option. [Appendix Table 1-24, Item 5]

c.5. Deletion

Considering that a terminal may experience a sudden power cutoff or a unexpected sequence during the shutdown process, the terminal should delete all *Contact address*es that it registers after startup and before starting to register. A complete deletion should be performed by sending a *REGISTER* request which specifies * in *Contact address* and 0 in *Expires* header, in the event that the deletion of certain location information previously registered in some way cannot be guaranteed.

c.5.1. Considerations on terminal halt and IP address modification

A terminal should delete or update the *Contact address* registered in a network at times of rebooting, IP address modification, or application termination (in the case of softphone), etc.

c.6. Registration event

A network may provide a registration event (*reg* event) which notifies a terminal of its change of state from registered to unregistered as defined in JF-IETF-RFC3680[RFC3680]. [Appendix Table 1-24, Item 8]

In the case that a terminal desires to receive a notification of its change of registration state after registration is completed, it can be notified by using a registration event package function.

c.6.1. Subscription to registration event

In the case that a terminal desires to receive a notification of its change of state from registered to unregistered, it sets the registration event in a *SUBSCRIBE* request and requests to the network a subscription to the change notification of registration state (i.e., *reg* event). In the case that a network provides a change notification of registration state, it accepts the subscription, sets the information of registration state in a *NOTIFY* request, and notifies a terminal in accordance with the procedure defined in JF-IETF-RFC3265[RFC3265].

c.6.2. Notification of registration event

In the case that a terminal registration state is changed to unregistered, a network sets the unregistered state information in a *NOTIFY* request and notifies the terminal that subscribes to the registration event.

Annex d. SIP capabilities exchange

(This annex is a normative part of this standard.)

d.1. Overview

This annex describes procedures for capabilities exchange with SIP messages.

d.2. Available methods

This standard requires that methods of *INVITE*, *ACK*, *BYE*, and *CANCEL* are available in any *INVITE* sessions. However, the availability of other methods the network allows terminals to send is dynamically determined through a procedure of capabilities exchange. This clause and its subclauses describes the procedure.

d.2.1. UPDATE

A terminal asserts its capabilities to receive an *UPDATE* request by listing *UPDATE* in *Allow* header of initial *INVITE* request and *18x*/*2xx* responses to the *INVITE* request.

The terminal is allowed to send the *UPDATE* request in the case that the *Allow* header is set in the initial *INVITE* request or the *18x*/*2xx* response recently received, and *UPDATE* is listed in the header. In an early dialog, a *PRACK* transaction must be completed before sending the *UPDATE* request.

d.2.2. PRACK

In the case that a *Require* header is set in a *1xx* response (excluding *100 (Trying)*) received, and *100rel* is listed in the header, the terminal sends a *PRACK* to this response.

d.3. Extension function

This clause and its subclauses describe the procedure for capabilities exchange to judge whether to be able to use extension function.

d.3.1. Session timer function (timer)

A terminal sets *timer* in a *Supported* header when sending an *INVITE* request and an *UPDATE* request, and by doing so asserts to a network that it supports the function (A *Require* header must not be set to assert the *timer* in the *INVITE* request and the *UPDATE* request).

d.3.2. Provisional response reliability function (100rel)

A terminal asserts its support of this function by listing *100rel* in a *Supported* header when sending an *INVITE* request (A *Require* header must not be set to assert the *100rel* in the *INVITE* request).

In the case that the terminal receives a *1xx* response (excluding *100 (Trying)*) to the *INVITE* request sent and the response contains *100rel* in *Require* header, the terminal enables the *100rel* extension function only for this response, and sends a *PRACK* request.

Annex e. SDP and media handling

(This annex is a normative part of this standard.)

e.1. Overview

This annex supplements JF-IETF-RFC4566[RFC4566] and JF-IETF-RFC3264[RFC3264], and describes the procedure of media establishment and media change using SDP.

e.2. Judging a media change request

e.2.1. Receiving SDP

In the case that a terminal receives a re-*INVITE* or a *UPDATE* request including SDP, the terminal determines the request means a media change only when the *sess-version* value in *o=* line of the SDP is different from that of the SDP received as either offer or answer in the previous media establishment/change.

In the case that the terminal cannot perform the requested media change, it returns a *488 (Not Acceptable Here)* response, but it will not terminate the existing session. Whether the existing session would be terminated or not is left to the judgment of the terminal which requested a media change.

e.2.2. Sending SDP

In the case that an offer is made which lists multiple codecs (offer using RTP as media and listing several payload types in the *fmt* part of *m=* line), only part of the codecs are selected in the answer. In the case that this terminal sends afterwards a re-*INVITE* or *UPDATE* request which does not request a media change such as session refresh, it does not change the *sess-version* value in *o=* line as specified in section 7.4 of JF-IETF-RFC4028[RFC4028], nor change the content of SDP excluding *sess-version* as specified in section 8 of JF-IETF-RFC3264[RFC3264] accordingly. In the case that a session refresh is performed using an *UPDATE* request, it is recommended not to use SDP, in accordance with section 7.4 of JF-IETF-RFC4028[RFC4028].

e.3. Payload type

In the case that the media is RTP and a payload type number is statically assigned to the codec in JF-IETF-STD65[RFC3551], the assigned number is used in the *fmt* part of *m=* line. For example, in the case of G.711μ-law, 0 is used in the *fmt* part.

In the case that a dynamic payload type number is specified due to the specifications of the codec, and the codec is selected as answer, the specified number in the offer is set to *m=* line of answer.

Note that a network may specify the maximum number of codecs that can be set in the *fmt* part of *m=* line. [Appendix Table 1-21, Item 3]

e.4. Fallback procedure

e.4.1. IP version incompatibility

A terminal should return a *488 (Not Acceptable Here)* response which includes a *Warning* header whose *warn-code* is *300 (Incompatible network protocol)* or *301 (Incompatible network address formats)* when it received an initial *INVITE* and determined that the requested IPv6 communication is not possible.

A terminal may receive a *488 (Not Acceptable Here)* response which includes a *Warning* header whose *warn-code* is *300 (Incompatible network protocol)* or *301 (Incompatible network address formats)* to the initial *INVITE* request it sent. In the case of receiving the above response to the session initiation with IPv6, the terminal interprets that communication using IPv6 is not possible and may try fallback with IPv4.

However, further session initiation is not conducted even if it receives a *488* response to its fallback call.

e.4.2. Media type incompatibility

If no acceptable media type is set in the received SDP, a terminal returns a *488 (Not Acceptable Here)* response. The terminal sets *304 (Media type not available)* as *warn-code* in a *Warning* header of the *488* response.

Annex f. Congestion prevention and control

(This annex is a normative part of this standard.)

f.1. Overview

This annex describes behaviours that a network and a terminal should follow in order to prevent or control congestion.

f.2. Considerations on congestion control at time of registration

When a network requires terminal registration (*REGISTER*) at the UNI, all the users in this network are bound to send *REGISTER* requests regularly, which generates a load on the network to constantly process a multitude of messages. Therefore, considerations are necessary on the terminal behaviour so that it will not generate unnecessary loads on the network at time of registration.

f.2.1. Actions on receiving an error response

After sending a *REGISTER* request, a terminal may receive an error response that includes a *Retry-After* header (a *4xx-6xx* response: in JF-IETF-RFC3261 [RFC3261], *404 (Not Found)* response, *413 (Request Entity Too Large)* response, *480 (Temporarily Unavailable)* response, *486 (Busy Here)* response, *500 (Server Internal Error)* response, *503 (Service Unavailable)* response, *600 (Busy Everywhere)* response, and a *603 (Decline)* response). In such a situation, the network may have some kind of problems such as congestion. Therefore, to avoid any further congestion, terminal registration is retried after the time interval specified in the *Retry-After* header (Note that an error response may be received again even when resending the *REGISTER* request after the specified time).

In the case that an error response is received without a *Retry-After* header, terminal registration is retried after an appropriate period of time (except on receiving a *401 (Unauthorized)* response) for the same reason.

f.2.2. Actions on receiving no response

A terminal may not be able to receive a response to a *REGISTER* request sent due to the retransmission timeout of SIP messages. An error may also occur in a layer below the SIP application layer (e.g., ICMP error notification). In such a situation, the terminal retries registration after an appropriate period of time. [Appendix Table 1-24, Item 7]

f.2.3. Considerations on registering multiple Contact addresses

Considerations should be given so that a terminal does not send a series of *REGISTER* requests in a short time in order to prevent unnecessary loads on a network triggered by the terminal registration behavior, in such cases where one terminal manages multiple AoRs, it needs to register multiple *Contact address*es in the network, and consequently it sends multiple *REGISTER* requests, etc.

f.2.4. User name or password error

In the case that a terminal receives a *401 (Unauthorized)* response from a network after sending a *REGISTER* request containing an *Authorization* header, it should refrain from retrying registration using the same user name and password (excluding the case in which the value of the *stale* parameter in the *WWW-Authenticate* header is *TRUE*) so as to avoid the submission of unnecessary *REGISTER* requests.

f.2.5. Re-registration at the occurrence of temporary faults

If a terminal detects that it cannot send or receive SIP messages for some reason but it returns later to a state in which it can, it should immediately updates registration or re-registration regardless of the change of its *Contact address* or registration retention period.

However, to avoid network congestion due to simultaneous registration behaviours caused by simultaneous terminal recoveries following a wide-area failure in the access network, and to avoid unnecessary repetition of terminal registration behaviours due to intermittent temporary faults, the submission of *REGISTER* requests following fault recovery is made only at statistically uniform time intervals within an appropriate period of time. The network may specify a period of interval to resend the *REGISTER* request in the case that the network gives no reply. [Appendix Table 1-24, Item 7]

f.3. Considerations on congestion control when originating a call

The congestion may worsen if terminals attempts to make more calls (sending of requests outside existing dialogs except for *REGISTER*) to a network which already experiences congestion and call loss. Therefore, this clause and its subclauses describe a series of procedures so that in the case of congestion, the network notifies the terminal of the congestion state, the terminal notifies the user of the information notified by the network, and by doing so, the network notifies the user of the congestion state and attempts to control and prevent the user from redialing.

This clause and its subclauses also describe call retrial conditions so that congestion is not caused by a terminal's unlimited call retrials on receiving an error response when the call is made.

f.3.1. Congestion notification

This clause and its subclauses describe the error response format of congestion notification from the network, and required actions for terminals on receiving the notification.

f.3.1.1. Notification to a terminal from a network

In the case that a network cannot provide service to any request from a terminal due to congestion, etc., a *503 (Service Unavailable)* response is sent including a *Reason* header (*protocol* is *Q.850* and *protocol-cause* is *42*: switching equipment congestion) to a request from the terminal, which means that the network cannot provide service. The network never sends to the terminal the response including the *Reason* header (*protocol* is *Q.850* and *protocol-cause* is *42*) due to a cause other than congestion.

Notification of additional information indicated in clause f.3.2.1 may be performed along with congestion notification described in this clause.

f.3.1.2. Notification from a terminal to a user

In the case that a terminal receives a *503 (Service Unavailable)* response in which a *Reason* [RFC3326] header (*protocol* is *Q.850* and *protocol-cause* is *42*: switching equipment congestion) is set, it recognizes that a network cannot provide service to any request due to congestion, etc., and then performs visible indication to notify a user of the situation, or audible sound generation, such as a guidance to notify congestion or a signal tone to indicate congestion built into the terminal. Subsequent automatic behaviour, such as automatic call retrial, must not be performed.

In the case that additional information notification indicated in clause f.3.2.1 is performed at the same time, display of additional information indicated in clause f.3.2.1 is prioritized.

f.3.2. Additional information notification

This clause and its subclauses describe a procedure to notify a terminal of additional information from a network using a *Warning* header.

f.3.2.1. Notification from a network to a terminal

In the case that a network desires to provide additional information to a user when an error occurs, etc., it can notify a terminal of the information by including a *Warning* header in a response message sent back to the terminal, setting *399 (Miscellaneous warning)* as *warn-code*, and listing given text information in *warn-text*. The network must not send to the terminal the response in which the *Warning* header is set with *warn-*

code 399, excluding the case that the information intended to be notified to the user is included.

f.3.2.2. Notification from a terminal to a user

In the case that a terminal receives a response in which a *Warning* header is set with *warn-code 399*, it should notify a user of this text information. In the case that the terminal can visibly indicate the text information, it should provide the user by actively indicating the information. In the case that the terminal can generate audible sounds, the implementation of the information e.g., giving an audio announcement of the information should be considered.

f.3.3. User name or password error

In the case that a terminal receives a *407 (Proxy Authentication Required)* response including a *Proxy-Authenticate* header from a network after sending a request, it should refrain from resending a request using the same user name and password, excluding the case in which the value of the *stale* parameter in the *Proxy-Authenticate* header is *TRUE*, or in which a *WWW-Authenticate* header or *Proxy-Authenticate* header exists that has the *realm* parameter set and has never been received.

Annex g. Bandwidth control

(This annex is a normative part of this standard.)

g.1. Overview

This annex describes a bandwidth control function which is characteristic of NGN. A signalling procedure and its relationship with a transport layer protocol are described by referring to JT-Y1221[Y.1221].

Below is written assuming that bandwidth control is performed utilizing the Resource and Admission Control Functions (RACF) described in TR-1014[TR-1014], but realizing it based on other way of implementation is allowed as far as the difference can not be visible externally. Note that even in that case, it is required that the bandwidth control function conforming to this annex is provided, and the bandwidth requested by this function is reserved inside the network.

g.2. References

References used in this annex are as follows.

[Y.1221] "Traffic control and congestion control in IP based networks", TTC standard JT-Y1221, version 2, The Telecommunication Technology Committee, Mar 2013

[Y.1540] ITU-T Recommendation Y.1540, "Internet protocol data communication service - IP packet transfer and availability performance parameters", 2007

[Y.1541] ITU-T Recommendation Y.1541, "Network performance objectives for IP-based services", 2007

[RFC2474] "Definition of Differentiated Services Field in the IPv4 and IPv6 Headers", TTC standard JF-IETF-RFC2474, version 1.0, The Telecommunication Technology Committee, May 2009

[RFC2475] "An Architecture for Differentiated Services", TTC standard JF-IETF-RFC2475, version 1.0, The Telecommunication Technology Committee, May 2009

g.3. Bandwidth control mechanism in NGN

The bandwidth control mechanism shall conform to Annex a of JT-Y1221. Supplementary specifications and option items when applying Annex a of JT-Y1221 at the UNI are as follows.

- When the token bucket size is configured without applying the proportional relationship specified in subclause a.2.3 of JT-Y1221, the configured value is determined by networks. [Appendix Table 1-13, Items 1]
- With regard to the values of rate factors at the UNI, QoS class α defined in JT-Y1221 conforms to subclause a.2.5.1 of JT-Y1221. The values applied for the other QoS classes are determined by networks. These network-determined values may differ depending on quality classes shown in clause g.5. [Appendix Table 1-13, Items 2]

g.4. SIP/SDP specifications

The SIP/SDP specifications shall conform to Annex a of JT-Y1221. Supplementary specifications and option items when applying Annex a of JT-Y1221 at the UNI are as follows.

- In accordance with subclause a.2.2 of JT-Y1221, the applied token bucket speed is the value described in "*b=*" line of the SDP. Only for audio media, it is possible to apply individual designated token bucket speed for particular codec(s) instead of the speed indicated in "*b=*" line sent from user equipment. [Appendix Table 1-13, Items 3]

- Applicability of a "*b=RR*" line and a "*b=RS*" is determined by networks. [Appendix Table 1-13, Item 4]
- In the case that both a "*b=RR*" line and a "*b=RS*" line are not used, it is recommended to set the RTCP bandwidth at 5 percent of RTP bandwidth, as specified in annex a.2.2.1 of JT-Y1221. If the bandwidth other than 5% of the RTP bandwidth is applied, in this case the RTCP bandwidth is determined by networks. [Appendix Table 1-13, Item 5]

g.5. Quality class

In an NGN, multiple services with different conditions are provided in the same network, as described in Subclause a.1.4 of JT-Y1221 and its subsequent subclauses.

For example, in the case that http communication using Web browsers, etc. and IP telephone communication with 0AJ numbers are provided in the same network, QoS (Quality of Service) provided in each service differs in general.

This annex describes about the transfer quality of IP packets. In particular, IP Packet Transfer Delay (IPTD), IP packet Delay Variation (IPDV) and IP packet Loss Ratio (IPLR), which are defined in Y.1540[Y.1540], are described. The other service-specific factors for the QoS are not discussed in this annex. The transfer quality of IP packets defined by this combination of IPTD, IPDV, and IPLR are referred to as “quality class”. Note that providing quality class is determined by a network. [Appendix Table 1-13, Item 6]

g.5.1. Multiple quality classes and DiffServ

In NGN, service oriented quality class is made possible by allocating network resources per quality class, and a quality class per service. For instance, in the example of subclause g.5, for http communication by Web browsers, a quality class as best-effort communication which does not guarantee IPTD, IPDV, and IPLR is allocated. Likewise, for IP telephone communication with a 0AJ numbers, a quality class which guarantees IPTD, IPDV, and IPLR is allocated.

To meet the conditions defined for each quality class, the quality class of IP packets used in each communication needs to be identified in the NGN access network and core network, and the IP packets are handled appropriately to each quality class. Therefore, transfer is prioritized using the DSCP value of IP packets, utilizing DiffServ [RFC2474][RFC2475] based on Y.1221[Y.1221] Appendix III. The network specifies DSCP value of DiffServ to be applied to the UNI. [Appendix Table 1-13, Item 7]

g.5.2. Setting of DSCP value

Priority control of IP packets is needed for the whole areas of UNI-UNI and UNI-NNI communication, in order to provide an NGN end-to-end quality class. Therefore, DSCP values are set to IP packets by a terminal and a network as follows.

- In order to appropriately perform priority control for the UNI zone, a terminal sets DSCP values when sending IP packets to a network
- In order to appropriately perform priority control inside a network, the network may change or normalize DSCP values when bringing inside the network IP packets received from a terminal.

Annex h. Constraints on string length and value range of SIP messages

(This annex is a normative part of this standard.)

h.1. Overview

This annex clarifies the maximum length of character string (hereinafter referred to as "string length") and value range of integer fields (hereinafter referred to as "value range") regarding SIP and SDP.

h.2. String length and value range

Indicated here are conditions that a terminal must receive and appropriately process messages from a network (terminal's receiving conditions). The terminal may be equipped with receiving capabilities higher than those described in this annex. Conditions of messages that are allowed to send from the terminal to the network are the same as those of receiving capabilities, but the network may set different conditions. The network may also add conditions to ones in this clause or make them more detailed. [Appendix Table 1-21, Items 1 and 2]

Note that the string length and value range unlisted in this annex conform to each document referred to in this standard.

h.2.1. SIP

Annex Table h-1 shows the constraints on string length and value range for SIP along with recommended conditions. In the explanation of each item, field names of the ABNF grammar as indicated in section 25.1 of JF-IETF-RFC3261[RFC3261] are used for clarification.

Annex Table h-1/JT-Q3402: String length and value range for SIP

Item		String length and value range	Remarks
General	String length per line of SIP message (*Request-Line*, *Status-Line*, *message-header*)	Equal to or less than 255 bytes including the end of line (CR+LF)	
Dialog and route management	The number of *Via* hops (the number of *via-parm* parameters)	Equal to or less than 10 hops	
	String length of the *Via* branch (*via-branch*)	Equal to or less than 128 bytes including z9hG4bK	
	String length of the *To*/*From* tag (*token* in *tag-param*)	Equal to or less than 128 bytes	
	String length of *Call-ID* (*callid*)	Equal to or less than 128 bytes	
	The number of URIs that constitute the Route Set	Equal to or less than 10 hops	
	String length per URI (*rec-route*) for *Record-Route*	Equal to or less than 128 bytes	
	String length of *Contact address* (*contact-param*)	Equal to or less than 128 bytes	
Originating and Terminating URIs	String length for the originating URI (*Request-URI*)	Equal to or less than 128 bytes	
	String length per URI of the *P-Preferred-Identity* and *P-Asserted-Identity*	Equal to or less than 128 bytes	
Terminal registration	SIP-URI to which a *REGISTER* is sent (*Request-URI* of a *REGISTER* request)	Equal to or less than 32 bytes	
	String length of *realm* at time of HTTP Digest authentication	Equal to or less than 64 bytes	
	String length of user name at time of HTTP Digest authentication	Equal to or less than 32 bytes	
	String length of password at time of HTTP Digest authentication	Equal to or less than 32 bytes	

h.2.2. SDP

Annex Table h-2 shows the constraints on string length and value range for SDP along with recommended conditions. In the explanation of each item, field names of the ABNF grammar indicated in section 9 of JF-IETF-RFC4566[RFC4566] are used for clarification.

Annex Table h-2/JT-Q3402: Character string length and set value conditions for SDP

Item		String length and value range	Remarks
General	String length per line of SDP	Equal to or less than 255 bytes including the end of a line (CR+LF)	
	Length of SDP (*session-description*)	Equal to or less than 1000 bytes (when using UDP)	
o=	String length of *username* in *o=* line	Equal to or less than 64 bytes	
	Value range of *sess-id* in *o=* line	63-bit nonnegative integer (0 to 2^{63}-1)	Section 5 in JF-IETF-RFC3264 [RFC3264]
	Value range of *sess-version* in *o=* line	63-bit nonnegative integer (0 to 2^{63}-1)	
s=	String length of *text* in *s=* line	Equal to or less than 64 bytes	

Annex i. Audio terminal behaviour

(This annex is a normative part of this standard.)

i.1. Overview

This annex describes the behaviours specific to a telephone terminal or TV telephone terminal, etc. featured out of NGN terminals.

i.2. Codec

Support for G.711 μ-law (64kbit/s) as defined in JT-G711[G711] is mandatory. It is recommended that the Packet Loss Concealment (PLC) function as defined in Appendix 1 of JT-G711 be provided.

i.2.1. Packetization period

In the case that G.711μ-law is included in SDP negotiation, a terminal must support 20ms as packetization period for G.711μ-law.

In the case that a *a=ptime* line is set in G.711μ-law for SDP offer, it is recommended to set 20ms as packetization period. A network may specify setting conditions for the *a=ptime* line and values to be set as packetization period. [Appendix Table 1-15, Items 1 and 2]

In the case that a *a=ptime* line is set in G.711μ-law for SDP answer, the packetization period set in the *a=ptime* line in the offer is specified. In the case that the *a=ptime* line is not set in the offer, 20ms is set for SDP answer. The network may specify the setting conditions for the *a=ptime* line. [Appendix Table 1-15, Item 1]

i.3. Behaviour at time of disconnection

At the time of user operation to disconnecting a call, a variety of unexpected states can be considered in SIP message sequences. For example, resending of *CANCEL* requests with no response, receiving no final response to initial *INVITE* request, resending of *BYE* requests with no *200 (OK)* response, and so on. In any cases, it must be possible for the terminal to send or receive a new initial *INVITE* request accompanying the outgoing or incoming of a new call in parallel with such states.

i.3.1. Sending a CANCEL/BYE request

After a terminal sends a *CANCEL* request to perform call cancellation caused by a user operation (at the time of an on-hook behaviour, application termination, etc.) and so forth, the terminal must be possible to create the next *INVITE* transaction and send out a new initial *INVITE* request when a new call request has been issued by the user – even if the terminal could not receive *2xx* response to the *CANCEL* request, or the terminal could not receive final response to the Initial *INVITE* request after *2xx* response of *CANCEL* request received. If a new call is issued during cancellation of the previous call, the terminal shall maintain both of them.

When the terminal detects the call disconnection of the user resource while the call is in progress, and has not received a *BYE* request, it sends a *BYE* request that releases the dialog and performs releasing the dialog/media/user resource. Regardless of the *BYE* transaction state (such as a *BYE*-request-resend state or error-response-receive state), it shall be possible to send or receive an initial *INVITE* request for a new outgoing or incoming call.

i.3.2. Receiving a CANCEL/BYE request (before final response)

In the case that a terminal receives a *CANCEL* request or a *BYE* request while still in the state that it has not sent the final response to an initial *INVITE* request, it performs stops/releases processing of the user resources after sending the response to the request and initial *INVITE* request. In this case, if a *487 (Request*

Terminated) response is in the process of being resent due to the non-receipt of an *ACK* request, the terminal must still be able to perform, in parallel, the sending or receiving of an initial *INVITE* request due to a new outgoing or incoming call.

In the case of receiving a *BYE* request while a call is in progress, the terminal sends a response to the *BYE* request, and sends the user resource a Busy Tone or performs an equivalent behaviour.

i.3.3. Receiving a CANCEL request (after final response)

Up to the time that an *ACK* request is received after a called terminal sends a *2xx* response in reply to an initial *INVITE* request, a *CANCEL* request may be received to that *INVITE* transaction or dialog. In this case, the called terminal should use the receipt of the *CANCEL* request as a trigger to send a Busy Tone (or to perform an equivalent behaviour) for the called user resource so as to notify it that a disconnect has occurred on the caller.

On receiving the *CANCEL* request after sending the *200 (OK)* response as described above, the called terminal may enter into a state in which *200 (OK)* responses are being resent due to the non-receipt of an *ACK* request or in which a *BYE* request has not yet been received after receiving the *ACK* request. In this state, the terminal must still be able to perform, in parallel, the sending or receiving of an initial *INVITE* request due to a new outgoing or incoming call.

i.3.4. Receiving a 3xx response

In the case that a terminal receives a *3xx* response to the initial *INVITE* request, and does not send an initial *INVITE* request to the destination specified in a *Contact* header included in the response, it stops calling on receiving the *3xx* response, runs a busy tone etc. to the user and notifies that a call cannot be made.

i.3.5. Receiving a 4xx to 6xx response

In the case that a terminal receives a *4xx* to *6xx* response to the initial *INVITE* request, and does not perform retransmission for authentication or fallback (restarting a call based on changed media conditions of SDP, etc.), it stops calling on receiving the *4xx* to *6xx* response and runs a Busy Tone etc. to the user and notifies that a call cannot be made.

In particular, in the case that the terminal receives a *503* response in the format indicated in clause f.3.1.1 and clause f.3.2.1, it notifies it to the user for congestion control, based on clause f.3.1.2 and clause f.3.2.2.

i.3.6. Sending a 4xx to 6xx response

In the case of sending a *4xx* to *6xx* response to the initial *INVITE* request, a terminal must be able to process the sending or receiving of an initial *INVITE* request, in parallel, when the user resource is able to process the sending or receiving of a new call in the state that it is still waiting for an *ACK* request.

i.4. Ringing tone generation and dialog management

i.4.1. Sending a 18x response

In the case that a precondition extension function is not used, a terminal must not send a *1xx* (excluding *100 (Trying)*) response until the user calling state can be ascertained (e.g., up until an extension-designation receive-completion signal is received from the user (such as a PBX) assuming that the user resource is a 2W analog interface and that a dial-in sequence is used, or up until a receive-completion signal is received from an information-receiving terminal in the case of a "Number-Display" sequence), and must send it as soon as the user calling state can be ascertained.

A network specifies whether to allow or disallow setting SDP to the sending of the *1xx* response by the terminal. [Appendix Table 1-22, Item 1]

i.4.2. Receiving a 18x response

i.4.2.1. Ringing tone generation

In the case that a *180 (Ringing)* response without SDP is received before receiving any *1xx* (excluding *100 (Trying)*) response with SDP, a terminal must generate a ringing tone using its own sound source from that point. Then, within the same dialog, the ringing tone must continue to be generated as long as any subsequently received *1xx* response does not include SDP (in other words, the ringing tone must not be restarted). However, if SDP is included in a *1xx* response, a media path must be connected as described in clause i.4.2.2 and a sound must be generated from the network.

i.4.2.2. Early media generation

In the case of receiving a *1xx* response with SDP set, a terminal must be able to establish early media by connecting a path. The received media must continue to be generated, with or without SDP in any subsequently received *1xx* response for the same dialog (i.e., reprocessing of that media must not take place).

i.4.2.2.1. Media modification by an UPDATE request

In the case that media modification specified in an offer from the network by an *UPDATE* request is acceptable to the terminal, the terminal must return a *200 (OK)* response including an appropriate answer and modify the media. In the case that the specified media modification cannot be performed, it must return a *488 (Not Acceptab*le Here) response. Note that disconnection processing of the existing session is not performed from the terminal after returning the *488 (Not Acceptable Here)* response.

A network specifies whether to allow or disallow sending the *UPDATE* in the early dialog by the terminal. [Appendix Table 1-23, Item 1]

i.4.2.2.2. Management of multiple dialogs and media

Because a terminal may receive multiple *1xx* (excluding *100 (Trying)*) responses whose *To*-tags are different from each other, the terminal must be able to establish multiple dialogs for one initial *INVITE* request. In addition to any existing dialog (or dialogs), a terminal must create a new dialog when it receive a response with a new *To*-tag.

The terminal must also be able to accommodate multiple dialogs using different media.

Annex Table i-1 summarizes the mandatory or recommended implementation of calling terminal taking the above requirements into account.

Annex Table i-1/JT-Q3402: Management of multiple dialogs and media (Calling SIP terminal)

	Existing dialog	New dialog	Processing
1	Early dialog	Early dialog	- On receiving a new response, the terminal may select a dialog used to its user interface under a certain policy. The policy takes into account the presence of SDP, the content of SDP, etc. If using *100rel*, however, a *2xx* response may be received without an SDP answer, in which case it is recommended that all media information be saved or send *BYE* requests to disconnect the early dialogs explicitly. If there are no information for making a decision, the newer dialog is selected (taking into account call forwarding no reply, etc.).

i.4.3. Receiving a 2xx response

In the case that an SDP answer was received by a *1xx* response belonging to the same dialog as a *2xx* response before the terminal received the *2xx* response, the content of the SDP included in the *2xx* response is expected to be the same as the previously established media and is therefore ignored. If an SDP answer was not received before receiving the *2xx* response, the session is established according to the SDP answer included in the *2xx* response.

i.4.3.1. Management of multiple dialogs and media

Because a terminal may receive multiple *2xx* responses whose *To*-tags are different from each other, the terminal must be able to establish multiple dialogs for one initial *INVITE* request. In addition to any existing dialog (or dialogs), a terminal must create a new dialog when it receives a response with a new *To*-tags.

The terminal must also be able to accommodate multiple dialogs using different media.

Annex Table i-2 summarizes the mandatory or recommended implementation of calling terminal taking the above requirements into account.

Annex Table i-2/JT-Q3402: Management of multiple dialogs and media (Calling SIP terminal)

	Existing dialog	New dialog	Processing
1	Early dialog	Confirmed dialog	- Changes the media according to the content of the confirmed dialog. The remaining early dialog is either explicitly disconnected by sending a *BYE* request or its content is abandoned after 64 x T1.
2	Confirmed dialog	Confirmed dialog	- On receiving a new response, the terminal may select a dialog under a certain policy. The policy takes into account SDP content, etc. When the terminal select a dialog, the other dialog should be explicitly released by sending a *BYE* request (no return of *ACK* requests will result in more retransmissions of *2xx* responses).

i.5. Media change

i.5.1. IP address and port number

When receiving a media-change request involving the changing of IP addresses or port numbers (or both), the terminal must be equipped with the capability of making those changes.

Annex j. CUG/PNP

(This annex is a normative part of this standard.)

j.1. References

[TS-1018] "Technical Specification on SIP Interface for CUG/PNP over NGN", TTC Technical specification TS-1018, version 2.0, The Telecommunication Technology Committee, Mar 2015

j.2. UNI condition

If the CUG/PNP service is provided, the UNI interface conditions shall conform to [TS-1018].

Appendix i. Option items

(This appendix does not form an integral part of this standard.)

i.1. Introduction

The following tables show the option items of the main body, annexes, and appendices of JT-Q3402. The objective of this table is improvement of interoperability between NGN and SIP terminals through UNI. NGN carriers are allowed to select each "UNI condition" option item, and terminals are allowed to select each "Terminal selection" option item as far as the choice is allowed by "UNI condition" selected by the NGN carrier the terminal is willing to connect to.

The reader should consult the relevant clauses shown in "Relevant items" for more detailed information of each option item.

Note that any interaction among the options are not always described in these tables.

Note also that information given in the main document overrides that in this option item table in the event of any discrepancies.

i.2. Option item extraction policy

Option items are extracted from a following viewpoint:

The option items are extracted to improve interoperability of SIP terminals connected to the network through the UNI, and classified into different categories for ease of reference.

i.3. Option item table format

Appendix Table 1-1 shows and explains the format of the option item table presented here.

Appendix Table 1-1/JT-Q3402: Format example

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items
(Clausess referred, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">1</td><td rowspan="3">IPv4</td><td rowspan="3">Provides IPv4 connection</td><td>Terminal is required to be equipped with IPv4 connection function</td><td>May connect with IPv4</td><td rowspan="3">Clause 13</td><td rowspan="3"></td><td rowspan="3"></td></tr>
<tr><td rowspan="2">Terminal may be equipped with IPv4 connection function</td><td>May connect with IPv4</td></tr>
<tr><td>Not connect with IPv4</td></tr>
</table>

Name of option: shows option items.
UNI condition: shows patterns that a network can select as UNI conditions.
Terminal selection: shows patterns that a terminal can select compared to network selection.
Relevant items: shows for each option item, relevant clauses of the JT-Q3402 main body, annex or appendix.
Special notes: shows option items that should be determined in addition to "UNI condition" and "Terminal selection" columns. Special notes for "UNI condition" and "Terminal selection" are shown within the brackets of [ ] and << >>, respectively.

i.4. Option item table

Option item tables are shown in Appendix Table 1-2 to Appendix Table 1-25. Items specified that they shall be supported in the main body and annexes are not explicitly shown in each table.

Appendix Table 1-2/JT-Q3402: SIP methods

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	*REGISTER* [Terminal sends]	Terminal is required to register by *REGISTER*	–	Clause 10.2.1.10 Clause 10.2.3	[In case of using *REGISTER*, *Contact address* types and the number of them are listed here.]	
		Terminal is required not to register by *REGISTER*	–			
2	*MESSAGE* (outside existing dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3428 Clause 10.2.3	<<In the case that terminal sends, *Content-Type* and message body format are listed here.>>	
			Not send			
		Disallow	Not send			
3	*MESSAGE* (outside existing dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3428 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, *Content-Type* and message body format are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
4	*MESSAGE* (inside existing dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3428 Clause 10.2.3	<<In the case that terminal sends, *Content-Type* and message body format are listed here.>>	
			Not send			
		Disallow	Not send			
5	*MESSAGE* (inside existing dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3428 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, *Content-Type* and message body format are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
6	*REFER* (outside existing dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3515 Clause 10.2.3		
			Not send			
		Disallow	Not send			
7	*REFER* (outside existing dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3515 Clause 10.2.3		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
8	*REFER* (inside existing dialogs) [Terminal sends]s	Allow	May send	Clause 10.1 Table 3 / RFC3515 Clause 10.2.3		
			Not send			
		Disallow	Not send			
9	*REFER* (inside existing dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2 Table 3 / RFC3515 Clause 10.2.3		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
10	*SUBSCRIBE* (outside *INVITE* dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3265 Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
11	*SUBSCRIBE* (outside *INVITE* dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3265 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
12	*SUBSCRIBE* (inside *INVITE* dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3265 Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
13	*SUBSCRIBE* (inside *INVITE* dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3265 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
14	*NOTIFY* [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3265 Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
15	*NOTIFY* [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3265 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
16	*PUBLISH* (outside *INVITE* dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3903 Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
17	*PUBLISH* (outside *INVITE* dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3903 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
18	*PUBLISH* (inside *INVITE* dialogs) [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3903 Clause 10.2.3	<<In the case that terminal sends, the event names are listed here.>>	
			Not send			
		Disallow	Not send			
19	*PUBLISH* (inside *INVITE* dialogs) [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3903 Clause 10.2.3	<<In the case that terminal is equipped with receiving function, the event names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
20	Other methods [Terminal sends]	Allow	May send	Clause 10.2.3	[In the case that network allows the use, the method name are listed here.] <<In the case that terminal sends, the method names are listed here.>>	
			Not send			
		Disallow	Not send			
21	Other methods [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2.3	[In the case that network requests that terminal is equipped with receiving function, the method names are listed here.] <<In the case that terminal is equipped with receiving function, the method names are listed here.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Appendix Table 1-3/JT-Q3402: IP version and IP extension function

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	IPv4	Provide IPv4 connection	Terminal is required to be equipped with IPv4 connection function	May connect with IPv4	Clause 13		
			Terminal may be equipped with IPv4 connection function	May connect with IPv4			
				Not connect with IPv4			
2	IPv6	Provide IPv6 connection	Terminal is required to be equipped with IPv6 connection function	May connect with IPv6	Clause 13		
			Terminal is not required to be equipped with IPv6 connection function	May connect with IPv6			
				Not connect with IPv6			
		Not provide IPv6 connection	Terminal does not connect with IPv6	–			
3	IP versions of call control signals and media	Allow only the same IP version		Use the same IP version	Clause 13		
		Allow the same or different IP version		Use the same IP version			
				Use the same or different IP version			
4	Use of IPsec for call control signals	Provide IPsec connection	Terminal is required to be equipped with IPsec connection function, and always use IPsec.	–	Clause 13	[In the case that IPsec connection is provided, conditions are listed here.]	
			Terminal is not required to be equipped with IPsec connection function.	May connect with IPsec			
				Not connect with IPsec			
		Not provide IPsec connection	Terminal does not connect with IPsec.	–			

Appendix Table 1-4/JT-Q3402: Layer 4 protocol for call control signals

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	UDP	Provide UDP connection	Terminal is required to be equipped with UDP connection function.	May connect with UDP	Clause 12	[In the case that a port number other than the default number (5060) is used for sending or receiving, describe the port number here.]	
			Terminal is not required to be equipped with UDP connection function.	May connect with UDP			
				Not connect with UDP			
		Not provide UDP connection	Terminal does not connect with UDP.	–			
2	TCP (no TLS)	Provide TCP connection	Terminal is required to be equipped with TCP connection function.	May connect with TCP	Clause 12	[In the case that a port number other than the default number (5060) is to be listened, describe the port number here.]	
			Terminal is not required to be equipped with TCP connection function.	May connect with TCP			
				Not connect with TCP			
		Not provide TCP connection	Terminal does not connect with TCP.	–			
3	TCP (with TLS)	Provide TLS connection*1	Terminal is required to be equipped with TLS connection function.	May connect with TLS	Clause 12	[In the case that a port number other than the default number (5061) is used for listen, describe the port number here.]	
			Terminal is not required to be equipped with TLS connection function.	May connect with TLS			
				Not connect with TLS			
		Not provide TLS connection	Terminal does not connect with TLS.	–			

*1 In the case that authentication is performed when using TLS connection, HTTP Digest authentication must be selected as authentication procedure in Appendix Table 1-11, Items 1 and 2.

Appendix Table 1-5/JT-Q3402: SigComp

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Use of SigComp	Use in all sessions	Terminal is required to be equipped with this function, and performs sending and receiving using this function in all messages.	–	Clause 10.1 Table 3 / RFC3320 Table 3 / RFC3485 Table 3 / RFC3486 Table 3 / RFC5049		
		Use in each session as necessary	Terminal has receiving function of signals using this function.	May send signals using this function			
				Not send signals using this function			
		Not use	Terminal does not send signals using this function, and if received, ignore them.	–			

Appendix Table 1-6/JT-Q3402: Hosted NAT

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Allowing Hosted NAT in the lower part of the UNI (inside the user's residence)	Allow	Use Hosted NAT	Clause 10.1 Table 3 / RFC3581		
			Not use Hosted NAT			
		Disallow	Not use Hosted NAT			

Appendix Table 1-7/JT-Q3402: SIP option tags

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Session timer function (*timer*)	Use in all sessions	Terminal is required to be equipped[*1] with this function, accepts if required [*2], assert[*3], and requires[*4] if asserted.	–	Clause 10.2.1.20.32	[In the case of specifying a session timeout period, describe the *delta-seconds* values here.]	
		Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	Assert, and require if asserted			
				May not assert, or may not require.			

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
2	Provisional response reliability function (*100rel*)	Use in all sessions	Terminal is required to be equipped with this function, accepts if required, assert, and required if asserted.	–	Clause 10.1 Table 3 / RFC3262 Clause 10.2.1.20.32		
		Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	Assert, and require if asserted			
				May assert and may require			
			Terminal is not required to be equipped with this function.	Assert, and require if asserted			
				May assert and may require			
3	Dialog replacement function (*replaces*)	Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	May assert and may require	Clause 10.1 Table 3 / RFC3891		
				Not assert and not require			
			Terminal is not required to be equipped with this function.	May assert and may require			
				Not assertand not require			
		Not use	Terminal does not assert and require this function, and rejects*5 if required.	–			
4	Conference session participation function (*join*)	Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	May assert and may require	Clause 10.1 Table 3 / RFC3911		
				Not assert and not require			
			Terminal is not required to be equipped with this function.	May assert and not require			
				Not assert and not require			
		Not use	Terminal does not assert and require this function, and rejects if required.	–			
5	Bandwidth reservation function before establishment (*precondition*)	Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	May assert and may require	Clause 10.1 Table 3 / RFC3312 Table 3 / RFC4032		
				Not assert and not require			
			Terminal is not required to be equipped with this function.	May assert and may require			
				Not assert and not require			
		Not use	Terminal does not assert and require this function, and rejects if required.	–			

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
6	Terminal capabilities notification function (*pref*)	Use in each session as necessary	Terminal is required to be equipped with this function, and accepts if required.	May assert and may require	Clause 10.1 Table 3 / RFC3840 Table 3 / RFC3841		
				Not assert and not require			
			Terminal is not required to be equipped with this function.	May assert and not require			
				Not assert and not require			
		Not use	Terminal does not assert and require this function, and rejects if required.	–			
7	*REGISTER* route recording function (*path*)	Use	Terminal is required to be equipped with this function, and always asserts in registration.	–	Clause 10.1 Table 3 / RFC3327		
		Not use	Terminal does not assert this function.	–			
8	Security capabilities exchange function (*sec-agree*)	Use	Terminal is required to be equipped with this function, and always requires it.	–	Clause 10.1 Table 3 / RFC3329	[In the case of use, the security capabilities are listed here.] <<In the case of use, the security capabilities with which terminal is equipped are listed here.>>	
		Not use	Terminal does not require this function.	–			
9	Other SIP option tags	Use in each session as necessary	Terminal is required to be equipped with the functions of other option tags the network specifies.	–	Clause 10.2.1.20.32	[In the case of use, describe the names of SIP option tags and use conditions.]	
			Terminal is not required to be equipped with functions of other option tags.	–			
		Not use	Terminal does not assert or require other functions, and rejects if required.	–			

*1 "Equipped" with the function means that the function is implemented in the terminal (not necessarily meaning to perform the function).
*2 "Accept" means to perform this function in the case it is specified in the Require header.
*3 "Assert" means to indicate in the Supported header to notify the peer or the network of information that the function is equipped.
*4 "Require" means to indicate in the Require header to require for the peer or the network to perform the function.
*5 "Reject " means to return a 420 response and not accept the requirement if the function is required in the Require header of a request.

Appendix Table 1-8/JT-Q3402: timer

Item	Name of option	UNI condition		Terminal Selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Session refresh by *UPDATE* method	Use	Terminal is required to be equipped with this function, and uses the function if it can.	–	Clause 10.1 Table 3 / RFC4028		
		Not use	Terminal does not refresh a session by *UPDATE*	–			

Appendix Table 1-9/JT-Q3402: Subaddress

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Originating subaddress	Provides originating subaddress function	Terminal is required to be equipped with originating subaddress receiving function at time of terminating a call.	May use originating subaddress at time of originating a call	Annex b.7		
				Not use originating subaddress at time of originating a call			
		Not provide originating subaddress function	Terminal does not use originating subaddress and, if received, ignores it.	–			
2	Terminating subaddress	Provide terminating subaddress function	Terminal is required to be equipped with terminating subaddress receiving function at time of terminating a call	May use terminating subaddress at time of originating a call	Annex b.7		
				Not use terminating subaddress at time of originating a call			
		Not provide terminating subaddress function	Terminal does not use terminating subaddress and, if received, ignores it.	–			

Appendix Table 1-10/JT-Q3402: MIME Multipart

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Use of MIME Multipart in *INVITE* requests [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC2046	<<In the case that terminal sends, the contents of Multipart are listed here.>>	
			Not send			
		Disallow	Not send			
2	Use of MIME Multipart in *INVITE* requests [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC2046	[The contents of Multi-part are listed here that terminal is required to be equipped with receiving function.] <<The contents of Multipart are listed here that terminal is equipped with receiving function.>>	
		Terminal are not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
3	Use of MIME Multipart in a *MESSAGE* request [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC2046	<<In the case that ter-minal sends, the contents of Multipart are listed here.>>	
			Not send			
		Disallow	Not send			

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
4	Use of MIME Multipart in a *MESSAGE* request [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC2046	[The content of Multipart are listed here that terminal is required to be equipped with receiving function.] <<The contents of Multipart are listed here that terminal is equipped with receiving function.>>	
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving a request, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Appendix Table 1-11/JT-Q3402: Authentication

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Authentication (*REGISTER*)	Perform HTTP Digest authentication	Terminal is required to be equipped with HTTP Digest authentication function.	–	Clause 10.1 Table 3 / RFC2617 Table 3 / RFC3310 Table 3 / RFC3329		
		Perform AKA authentication[*1]	Terminal is required to be equipped with AKA authentication function.	–			
		Not perform (perform access-line based authentication)	–	–			
2	Authentication (Requests outside existing dialogs except for *REIGSTER*)	Perform HTTP Digest authentication	Terminal is required to be equipped with HTTP Digest authentication function.	–	Clause 10.1 Table 3 / RFC2617 Table 3 / RFC3310 Table 3 / RFC3329		
		Perform AKA authentication[*1]	Terminal is required to be equipped with AKA authentication function.	–			
		Not perform (perform access-line based authentication	–	–			

*1 In the case of performing AKA authentication, IPsec connection needs to be provided in Appendix Table 1-3, Item 4.

Appendix Table 1-12/JT-Q3402: Redirection

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Use of redirection by *3xx* response [Terminal sends]	Provide redirection function	May send	Clause 10.2.1.8.3	[In the case that redirection is allowed, methods and response codes are listed here.]	
			Not send			
		Not provide redirection function	Not send			

<table>
<tr><th>Item</th><th>Name of option</th><th>UNI condition</th><th>Terminal selection</th><th>Relevant items (Clauses referred, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Use of redirection by 3xx response [Terminal receives]</td><td>Terminal is required to perform redirection at time of receiving 3xx response.</td><td>–</td><td rowspan="2">Clause 10.2.1.8.3</td><td rowspan="2">[In the case that redirection is allowed, methods and response codes are listed here.]</td><td rowspan="2"></td></tr>
<tr><td>Terminal is required not to perform redirection at time of receiving 3xx response</td><td>–</td></tr>
<tr><td colspan="7"></td></tr>
</table>

Appendix Table 1-13/JT-Q3402: Bandwidth control

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (Clauses referred, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="2">1</td><td rowspan="2">Individual designation of token bucket size</td><td colspan="2">Designate</td><td>–</td><td rowspan="2">Annex g.3</td><td rowspan="2">[If the token bucket size is designated, upper and lower limits are designated.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Not designate</td><td>–</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Rate coefficient</td><td colspan="2">Rate coefficient is specified per quality class.</td><td>–</td><td rowspan="2">Annex g.3</td><td rowspan="2">[Values of rate coef-ficients are designated.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Single rate coefficient is specified.</td><td>–</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Token buket speed corresponding to codec</td><td colspan="2">Use</td><td>–</td><td rowspan="2">Annex g.3</td><td rowspan="2">[In the case of use, show conditions per codec.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Not use</td><td>–</td></tr>
<tr><td rowspan="4">4</td><td rowspan="4">Specifying RTCP bandwidth using b=RR / b=RS</td><td rowspan="3">Use</td><td rowspan="2">Terminal is equipped with receiving function of b=RR / b=RS.</td><td>Use</td><td rowspan="4">Annex g.4</td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td>Not use</td></tr>
<tr><td>Terminal may ignore b=RR / b=RS at time of receiving messages.</td><td>Not use</td></tr>
<tr><td>Not use</td><td>Terminal ignores b=RR / b=RS at time of receiving messages.</td><td>Not use</td></tr>
<tr><td rowspan="2">5</td><td rowspan="2">RTCP bandwidth at time of unspecified b=RR / b=RS</td><td colspan="2">Set to be 5% of RTP bandwidth</td><td>–</td><td rowspan="2">Clause 10.1
Table 3 / RFC3556
Annex g.4</td><td rowspan="2">[In the case of using bandwidth other than 5%, show methods to determine the bandwidth.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Use a value except for 5%</td><td>–</td></tr>
<tr><td rowspan="2">6</td><td rowspan="2">Quality class</td><td colspan="2">Provide multiple quality classes</td><td>–</td><td rowspan="2">Annex g.5</td><td rowspan="2">[In the case of specifying quality class, quality class for each factor is listed.]
<<Terminal lists quality class to use.>></td><td rowspan="2"></td></tr>
<tr><td colspan="2">Provide single quality class</td><td>–</td></tr>
<tr><td rowspan="2">7</td><td rowspan="2">DSCP value per quality class</td><td colspan="2">Specify</td><td>–</td><td rowspan="2">Annex g.5.1</td><td rowspan="2">[In the case of speci-fying the DSCP value, it is listed here.]</td><td rowspan="2"></td></tr>
<tr><td colspan="2">Not specify</td><td>–</td></tr>
<tr><td colspan="8"></td></tr>
</table>

Appendix Table 1-14/JT-Q3402: Media

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Video (*m=video*)	Allow	May use	Clause 10.3.1 / Table 9		
			Not use			
		Disallow	Not use			
2	Data communication (*m=application*, *m=data*, etc.)	Allow	May use	Clause 10.3.1 / Table 9	[Determine the *media* type (*m=* line of SDP) to allow.] <<In the case that terminal uses, *media* type is listed here.>>	
			Not use			
		Disallow	Not use			
3	Media TCP connection	Allow	May offer	Clause 10.3.1 / Table 9	[Determine the *media* type (*m=* line of SDP) and the *proto* part that allow TCP.] <<In the case that terminal uses, the *media* type and the *proto* part are listed here.>>	
			Not offer			
		Disallow	Not offer			

Appendix Table 1-15/JT-Q3402: Conditions when using G.711 μ-law

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Settings for *a=ptime* line in the case of using G.711 μ-law	Mandatory	Set	Annex i.2.1		
		Not mandatory	Set			
			Not set			
2	Packetization period in the case of offering G.711 μ-law	Allow only 20ms	–	Annex i.2.1	[In the case of allowing values other than 20ms, the allowed packetization period is listed here.]	
		Allow values other than 20ms	–			

Appendix Table 1-16/JT-Q3402: Codecs to be included in codec list /Protocols for data communication

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Voice band codec other than G.711 μ-law	Allow voice band codecs other than G.711 μ-law	Use voice band codec other than G.711μ-law	Clause 8.1	[In the case of allowing codecs other than G.711 μ-law, they are listed.] <<In the case that terminal uses codecs other than G.711 μ-law, they are listed here.>>	
			Not use voice band codec other than G.711 μ-law			
		Disallow voice band codec other than G.711 μ-law	Not use voice band codec other than G.711 μ-law			
2	Video codec	Allow	Use	Clause 8.1	[In the case video codecs are allowed, codec names are listed.] <<In the case that terminal uses video codecs, codec names are listed here.>>	
			Not use			
		Disallow	Not use			

<table>
<tr><th>Item</th><th>Name of option</th><th>UNI condition</th><th>Terminal selection</th><th>Relevant items (Clauses referred, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="3">3</td><td rowspan="3">Data communica-tion</td><td rowspan="2">Allow</td><td>Use</td><td rowspan="3">Clause 8.1</td><td rowspan="3">[In the case of allowing data communication, protocol names are listed here.]
<<In the case that terminal uses data communication, protocol names are listed here.>></td><td rowspan="3"></td></tr>
<tr><td>Not use</td></tr>
<tr><td>Disallow</td><td>Not use</td></tr>
<tr><td colspan="7"></td></tr>
</table>

Appendix Table 1-17/JT-Q3402: Media-related SIP headers

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (Clauses referred, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="4">1</td><td rowspan="4">P-Media-Authorization header</td><td rowspan="3">Use</td><td>Terminal is required to be equipped with capabilities to receive messages.</td><td>Not send</td><td rowspan="4">Clause 10.1
Table 3 / RFC3313</td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with capabilities to receive messages.</td><td>Not send, and on receiving messages, behave according to the header content</td></tr>
<tr><td>Not send, and on receiving messages, ignore it.</td></tr>
<tr><td>Not use</td><td>Terminal does not send, and on receiving messages, ignores it.</td><td>–</td></tr>
<tr><td colspan="8"></td></tr>
</table>

Appendix Table 1-18/JT-Q3402: Media grouping

<table>
<tr><th>Item</th><th>Name of option</th><th colspan="2">UNI condition</th><th>Terminal selection</th><th>Relevant items (Clauses referred, etc.)</th><th>Special notes</th><th>Remarks</th></tr>
<tr><td rowspan="5">1</td><td rowspan="5">Media grouping (a=group line, a=mid line)</td><td rowspan="4">Use</td><td rowspan="2">Terminal is required to be equipped with capabilities to receive messages.</td><td>May send</td><td rowspan="5">Clause 10.1
Table 3 / RFC3388
Table 3 / RFC3524</td><td rowspan="5">[In the case of use, available semantics is listed here.]
<<In the case that terminal uses, semantics to be used is listed here.>></td><td rowspan="5"></td></tr>
<tr><td>Not send</td></tr>
<tr><td rowspan="2">Terminal is not required to be equipped with capabilities to receive messages.</td><td>May send</td></tr>
<tr><td>Not send</td></tr>
<tr><td>Not use</td><td>On receiving messages, terminal ignores it.</td><td>Not send</td></tr>
<tr><td colspan="8"></td></tr>
</table>

Appendix Table 1-19/JT-Q3402: Feedback control using RTCP

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	RTCP packets for feedback control using RTCP (RTPFB, PSFB)	Allow	–	May use	Clause 11.1	<<In the case that terminal uses, feedback format is listed here.>>	
				Not use			
		Disallow	On receiving messages, terminal ignores it.	Not use			
2	Use of SDP description for feedback control using RTCP (RTP/AVPF)	Allow	–	May use	Clause 11.1	<<In the case that terminal uses, feedback format is listed here.>>	
				Not use			
		Disallow	In the case that terminal receives, return an appropriate error response.	Not use			

Appendix Table 1-20/JT-Q3402: URI format

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	*Request-URI* format when using numbers other than national numbers (requests outside existing dialogs except for *REGISTER*)	Allow	May use	Clause 9 Annex b.6	[In the case it is allowed, URI format is listed.] <<URI format to be used is listed here.>>	
			Not use			
		Disallow	Not use			
2	The *hostport* part of a SIP-URI and the *descriptor* part of *context* in a TEL-URI when using national numbers	Specifies domain	–	Clause 9 Annex b.6.2	[Shows domain name or IP address.]	
		Specifies IP address	–			

Appendix Table 1-21/JT-Q3402: SIP/SDP character string length and set value range

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Conditions on SIP string length and value range unspecified in Annex h.	Set	–	Annex h.2.1	[In the case of setting, show specific conditions on sending/receiving messages.]	
		Not set	–			
2	Conditions on SDP string length and value range unspecified in Annex h.	Set	–	Annex h.2.2	[In the case of setting, show specific conditions on sending/receiving messages.]	
		Not set	–			
3	Number of payload types that can be set in the *fmt* part of *m=* line	Network specifies the maximum value.	–	Annex e.3	[In the case of specifying the maximum value, the value is described here.] <<In the case that terminal offers, the maximum payload value to be described in the *fmt* part is described here.>>	
		Network does not specify the maximum value.	–			

Appendix Table 1-22/JT-Q3402: Media negotiation

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	SDP settings to a *1xx* response [Terminal sends]	Allow	May set	Annex g.4.1		
			Not send			
		Disallow	Not send			
2	SDP offer by a *PRACK* request [Terminal sends]	Allow	May set	Clause 10.2.1.7.4.1		
			Not set			
		Disallow	Not set			
3	SDP offer by a *PRACK* request [Terminal receives]	Terminal is required to be equipped with capabilities to receive messages	–	Clause 10.2.1.7.4.1		
		Terminal is not required to be equipped with capabilities to receive messages.	Equipped with capabilities to receive messages			
			Not equipped with capabilities to receive messages			
4	Optional SDP lines [Terminal sends]	Use	–	Clause 10.3.1 Table 9	[SDP lines to be used are listed here.] <<SDP lines to be sent are listed here.>>	
		Not use	–			
5	Optional SDP lines [Terminal receives]	Use	–	Clause 10.3.1 Table 9	[SDP lines to be used to are listed here.] <<SDP lines to support receiving are listed here.>>	
		Not use	–			

Appendix Table 1-23/JT-Q3402: Media modification

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Media modification in early dialog [Terminal sends]	Allow	May send	Clause 10.1 Table 3 / RFC3311		
			Not send			
		Disallow	Not send			
2	Media modification in early dialog [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.1 Table 3 / RFC3311		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving messages, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
3	Media modification by re-*INVITE* after dialog establishment [Terminal sends]	Allow	May send	Clause 10.2.1.14		
			Not send			
		Disallow	Not send			

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
4	Media modification by re-*INVITE* after dialog establishment [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2.1.14		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving messages, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			
5	Media modification by *UPDATE* after dialog establishment [Terminal sends]	Allow	May send	Clause 10.2.1.14		
			Not send			
		Disallow	Not send			
6	Media modification by *UPDATE* after dialog establishment [Terminal receives]	Terminal is required to be equipped with receiving function.	–	Clause 10.2.1.14		
		Terminal is not required to be equipped with receiving function.	Equipped with receiving function			
			On receiving messages, return an appropriate error response.			
		In the case that terminal receives, return an appropriate error response.	–			

Appendix Table 1-24/JT-Q3402: Registration

Item	Name of option	UNI condition		Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	Providing pre-existing route at time of registration (*Service-Route* header)*1	Provide	Terminal uses provided pre-existing route.	–	Annex c.3.1		
		Not provide	Terminal does not set pre-existing route.	–			
2	Obtaining SCF address	Provide IP address/port number of SCF by DHCP/DHCPv6.		–	Annex c.2	[Procedures are listed here in the case of procedures other than DHCP and presettings.]	
		Preset IP address/port number of SCF in the terminal		–			
		Provide IP address/port number by methods other than the above		–			
3	Notifying network-asserted user identity at time of *REGISTER*	May notify		In the case of receiving notification, use the received SIP-URI.	Annex b.3.1	[In the case of notifying, conditions are listed here.]	
		Not notify		–			
4	The *expires* parameter value in the *Contact* header or the value in the *Expires* header at time of registration	Network specifies a fixed value		Set specified value	Annex c.3	[In the case of specifying the set value, the value is listed here.]	
		Network does not specify a fixed value		Set any value			
				Not set			
5	The *expires* parameter value in the *Contact* header or the value in the *Expires* header at time of refresh	Network specifies		Set specified value	Annex c.4	[In the case of specifying calculation formula or fixed value, it is listed here.]	
		Network does not specify		Set any value			
				Not set			

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
6	Setting the *q* parameter to the *Contact address*	Allow	Set	Annex c.3	[In the case it is allowed by the network, the setting conditions are listed here.]	
			Not set			
		Disallow	Not set			
7	Interval to send a *REGISTER* request at time of no reply by the network	Network specifies	Send specified value	Annex f.2.5	[In the case of being specified by the net-work, the interval is listed here.] <<In the case of not being specified by the network, the interval of sending from the ter-minal is listed here.>>	
		Network does not specify	Send according to terminal implementation			
8	Registration state notification (*reg* event) function of the terminal	Provide	May subscribe to registration notification	Annex c.6		
			Not subscribe to registration notification			
		Not provide	Not subscribe to registration notification			
*1 In order to use this procedure, the terminal capabilities notification function (path) in Appendix Table 1-7, Item 7 must be used.						

Appendix Table 1-25/JT-Q3402: Sending and receiving RTP packets

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	RTP sending behaviour of the terminal when receiving a *1xx* response to an *INVITE* request	Start sending	–	Clause 7.1		
		May start sending	Send			
			Not send			
		Not start sending	–			
2	Handling of media packets before performing final SDP negotiation to an initial *INVITE*	May start sending to terminal	–	Clause 7.1		
		Not start sending to terminal	–			

Appendix Table 1-26/JT-Q3402: CUG/PNP

Item	Name of option	UNI condition	Terminal selection	Relevant items (Clauses referred, etc.)	Special notes	Remarks
1	CUG/PNP	Provide	Use	Annex j		
			Not use			
		Not provide	Not use			

Appendix ii. Response code usage

(This appendix does not form an integral part of this standard.)

ii.1. Introduction

NGN is used in various forms of communication, such as message communication and data communication, in addition to speech communication. In the traditional speech communication, when connection fails to be established, the audio guidance is simply run to the user. However, in message communication and data communication, etc., notification based on SIP response codes must be delivered to the user, instead of the audio guidance. Also in the case of softphone and other highly functional terminals with display capabilities, though the terminal may be intended to be used for speech communication, it is considered desirable to display cause of error on the display according to response codes.

For the terminal to appropriately display cause of error based on SIP response codes, the information that the response codes represent must match between the network and the terminal. However, the definitions of response codes indicated in JF-IETF-RFC3261[RFC3261] do not represent actual incidents occurred in the real world of NGN communication. Therefore, it may run the risk of generating discrepancies between the specific incidents and response codes and not displaying properly to the user.

For this reason, this Appendix shows the specific examples of response code usage so that it may help interpret the meaning of response codes. Note that usage of response codes that is not shown in this Appendix may be allowed by the network.

ii.2. 4xx response

ii.2.1. 403 Forbidden

In the case that connection is attempted to be made to a resource which forbids access from a subscriber or a terminal e.g., when a destination specified by the terminal is not allowed to the subscriber, a network returns a *403 (Forbidden)* response.

In the case that a terminal rejects receiving a call judging from the calling-party's identity, it returns a *403 (Forbidden)* response. In the case that the *403 (Forbidden)* is received, it should be interpreted that the call was rejected by the network or the terminal on the terminating side ("Connection is rejected").

ii.2.2. 404 Not Found

In the case that a specified subscriber does not exist, no route towards the subscriber is available, or the *Request-URI* is inappropriate e.g., when a destination numeric string is too long, a network may return a *404 (Not Found)* response, instead of providing an audio guidance.

In the case that a terminal which accepts a call with a subaddress specified by the network does not exist, it returns a *404 (Not Found)* response. In the case that the *404 (Not Found)* response is received, it should be interpreted that the destination was inappropriate ("Unallocated number or no destination").

ii.2.3. 410 Gone

In the case that the specified destination by a subscriber has been changed to a URI different from the original but no redirection instruction is given to the terminal, the network may return a *410 (Gone)* response, instead of playing an audio guidance to notify the relocation. In other cases, the *410 (Gone)* response should not be returned.

The terminal should not send unnecessary *410* responses in order to avoid confusion with the relocation. In the case that the *410 (Gone)* is received, it should be interpreted that the URI has been changed ("Relocated") due to the relocation of the destination, etc.

ii.2.4. 433 Anonymity Disallowed

A network which provides a service to reject an anonymous call may return a *433 (Anonymity Disallowed)* response specified in JF-IETF-RFC5079[RFC5079], instead of providing an audio guidance, in the case of rejecting with the service.

In the case of rejecting the call for the reason that the calling-party's identity is anonymous, a terminal returns a *433 (Anonymity Disallowed)* response. In the case that the *433 (Anonymity Disallowed)* is received, it should be interpreted that the call was rejected for the reason of the undisclosed identity ("Rejection for anonymous calls").

ii.2.5. 480 Temporarily Unavailable

In the case that a specified subscriber does exist but communication is impossible for the reason that a terminal is disconnected etc. (in cases that the terminal is unregistered or the registration is expired, etc.), a network may return a *480 (Temporarily Unavailable)* instead of providing an audio guidance.

In the case that a terminal receives the *480 (Temporarily Unavailable)*, it should be interpreted that the terminal on the terminating side is temporarily unable to receive the call for the reason that the terminal is disconnected ("Terminal is unavailable "), etc.

ii.2.6. 486 Busy Here

In the case that call connection is about to be made exceeding the number of sessions allowed for calling subscriber or called subscriber, a network returns a *486 (Busy Here)* response.

In the case that a called terminal is already engaged in other communication and cannot receive a call, it returns a *486 (Busy Here)* response. In the case that the *486 (Busy Here)* response is received, it should be interpreted that the number of sessions of the network or the called terminal necessary for the call connection is insufficient ("Busy"). It should be noted that the *486 (Busy Here)* response may be returned to requests such as *MESSAGE*, *SUBSCRIBE*, and *REGISTER*, in addition to an *INVITE* request.

ii.2.7. 487 Request Terminated

In the case of terminating an unestablished call while still calling, a network may return a *487 (Request Terminated)* response, regardless of whether it receives a *CANCEL* request from a terminal. This is applied to the cases that time to try establishing the call exceeds a certain amount of time or a guidance is terminated, etc.

In the case that the terminal receives the *487 (Request Terminated)* response, it should be interpreted that the events such as written above happened.

ii.2.8. 488 Not Acceptable Here

In the case that the contents of SDP set in an *INVITE* or *UPDATE* request sent from a terminal are unacceptable (i.e., communication using media type, codec, bandwidth, IP version, etc. set in the SDP is impossible), a network returns a *488 (Not Acceptable Here)* response. In other cases, the *488 (Not Acceptable Here)* should not be returned.

In the case that the contents of SDP set in the *INVITE* or *UPDATE* request sent from the terminal are unacceptable, the terminal returns the *488 (Not Acceptable Here)* response. In other cases, the *488 (Not Acceptable Here)* should not be returned. In the case that the *488 (Not Acceptable Here)* is received, it should be interpreted that the network or the terminal on the terminating side did not accept the SDP.

ii.3. 5xx response

ii.3.1. 503 Service Unavailable

In the case that a network cannot provide service to a terminal due to the states as congestion or failure, it returns a *503 (Service Unavailable)* response as described in Annex f.

The terminal should not send unnecessary *503 (Service Unavailable)* responses in order to avoid confusion with the network congestion or failure. In the case that the *503 (Service Unavailable)* is received, it behaves as described in Annex f.

Appendix iii. Mapping SDP description to QoS classes

(This appendix does not form an integral part of this standard.)

iii.1. Overview

This appendix shows a way of mapping of QoS classes corresponding to SDP media description contents in order to determine QoS classes specified in Annex g. The mapping of QoS classes at the UNI are not limited to examples shown in this appendix.

iii.2. Concept

In the case that a network provides multiple QoS classes, it is necessary to select a QoS class that is appropriate to the nature of media. This appendix introduces an implicit rule of selecting a QoS class as below. In the rule, correspondence to QoS class is determined by the media description in SDP, which describes the nature of the media.

The nature of media regarding IP packet transfer quality is composed of media type and direction.

Media types fall into the following communication types: audio (*m=audio*), video (*m=video*), and data (*m=application*, etc), and it is indicated in the *proto* of *m=* line in SDP.

For audio, it is desirable to keep low the level of transfer delay, variation, and loss ratio (for the reason to provide quality required by the regulation for 0AJ). Even for video, the delay, variation and loss ratio which is the same level as audio could be considered desirable, taking the lip-sync with audio into account. On the other hand, data communication is not in general required to keep the level of delay or variation as low as audio or video. For the loss ratio, the packet loss could often be recovered by retransmission in the case of the data communication. In this way, taking the media type into account, it is considered to be appropriate to assign higher priority of QoS class to audio and video,media and assign lower priority of QoS class to data media.

Media direction falls into the following communication types: bidirectional (*a=sendrecv*) or unidirectional (*a=recvonly* / *a=sendonly*), and it is indicated in direction attributes in SDP.

In bidirectional communication (e.g., audio telephone, television telephone), delay in the network is directly felt by user as round-trip time to return a response to the information received from a party on the other side of communication. On the other hand, in unidirectional communication (e.g., streaming), the delay in the network is not so obvious because it takes only sending to or receiving from the party on the other side. Therefore, it is considered to be appropriate to assign higher priority of QoS class to unidirectional communication and assign lower priority of QoS class to bidirectional communication.

iii.3. Example of correspondence

This clause shows examples of QoS class corresponding to each media from SDP media description contents based on media type and direction.

iii.3.1. SDP

The media type of audio (*m=audio*) and video (*m=video*) is given high priority and the media type of data (*m=application*) is given low priority. For the media of audio and video which is highly prioritized, the higher priority is given in the case that the media direction attribute is bidirectional (*a=sendrecv*), and the lower priority is given in the case that the media direction attribute is unidirectional (*a=recvonly* / *a=sendonly*).

One of the three types of QoS classes is selected from the SDP description according to the above way of mapping. (Appendix Table 2-1)

Appendix Table 2-1 / JT-Q3402: Example of QoS class corresponding to SDP description

QoS class	SDP description of media		Service example
	Type	Direction attribute	
Highest priority class	Audio (*m=audio*) Video (*m=video*)	Bidirectional (*a=sendrecv*)	Audio telephone, television telephone
High priority class	Audio (*m=audio*) Video (*m=video*)	Unidirectional (*a=recvonly* / *a=sendonly*)	Video streaming
Priority class	Data (*m=application*)	Bidirectional or Unidirectional (*a=sendrecv* / *a=recvonly* / *a=sendonly*)	Data communication, remote control of device

Note that for communication that does not require quality, the best-effort class is assumed to be set as a QoS class lower than "priority class" shown in Appendix Table 2-1 where resource admission control using SIP/SDP is not performed.

Appendix iv. Security considerations

(This appendix does not form an integral part of this standard.)

iv.1. Overview

This appendix shows examples of solutions expected to be effective in meeting requirements indicated in clause 14 regarding security over the UNI.

iv.2. Requirements for the UNI

The following items should be considered from the security standpoint in the UNI.

1) Prevention of tampering

   SIP messages transferred over the UNI shall not be tampered with by a third party.

2) Prevention of spoofing

   SIP messages that a terminal receives shall be forwarded safely from the SIP trust domain without the occurrence of any spoofing.

3) Hiding of user information

   Information which specifies a user shall not be unnecessarily notified to the opposing terminal

iv.3. Solution examples

iv.3.1. Filtering with source IP address

The processing to filter incoming packets with the source IP address listed below as an example is expected to be effective for the prevention of spoofing.

- Packet filtering is performed by some means at the UNI to ensure that a SIP message packet which is sent to a terminal and has a source IP address corresponding to a network boundary (group) is indeed a packet from a network boundary (group). This prevents spoofing with respect to the source IP address.
- The terminal judges that a received SIP message is sent from a valid SIP trust domain only in the case that its source IP address is the same as a previously acquired address of a network boundary (group), and accepts the connection.

iv.3.2. Limiting the port for use

The processing to limit the port for use listed below as an example is expected to be effective for the prevention of spoofing.

- The port number that a terminal uses to send or receive SIP messages is limited to specific ports.
- Packet filtering is performed by some means at the UNI to ensure that a packet which is received by the terminal and has a destination port number corresponding to the specific port set in the previous item is indeed a packet from a network boundary (group). This prevents specified ports from being used by other parties.

Note that in this case the above specified ports can no longer be used for other purposes.

iv.3.3. Randomization of a Contact header (on terminal registration)

In the case that a network has a structure in which a terminal may receive a SIP messages directly from ouside of the SIP trust domain, the terminal is recommended to set a random string which cannot be guessed easily from a third party in the *user* part of a *Contact address* specified at the time of terminal registration for the reasons stated below.

- When receiving requests outside existing dialogs, a terminal judges the validity of the received requests by comparing the *Request-URI* and registered *Contact address*. In the case that values are easy-to-guess (e.g., user name or his phone number), it runs a high risk of suffering from a prank call (e.g., "spit") caused by invalid requests outside existing dialogs not transmitted through the SIP trust domain.
- In the case that a network has a structure that configures IP addresses of terminals dynamically (e.g., DHCP, PPPoE) and the IP address is changed every time a terminal acquires it, the network retains the *Contact address* in the event of an unexpected failure (e.g., power blackout) at the terminal. In this situation and the case that the IP address has been assigned to another terminal, a request may end up being sent to the terminal different from the one that experiences the unexpected failure to which the request was originally intended to be sent. But a malfunctioning behaviour can be prevented on the surface by checking if the *user* part is the same when the terminal receives the requests outside existing dialogs.

iv.3.4. Randomization of a Contact header (on initiating sessions)

In the case that a network has a structure in which a terminal may receive SIP messages directly from outside of the SIP trust domain, it is desirable that the terminal generates a unique string which cannot be guessed easily from a third party and use it for *user* part of *Contact address* in requests outside existing dialogs. It is also desirable that the *user* part is different from that of a *Contact address* in a *REGISTER* request at the time of registration. Note that the string is not modified in subsequent transactions in the same dialog.

iv.3.5. Considerations on transparent transfer of SIP messages

The SIP/SDP information set by a terminal may not be filtered or rewritten in a network, and may be notified transparently to the UNI or NNI on the terminating side. Therefore, strings involved with user identity should not be set in SIP headers not indicated in Annex b or SDP constituent elements.

Appendix v. Discovery procedure of the SCF

(This appendix does not form an integral part of this standard.)

v.1. Overview

This appendix shows an example of procedures for obtaining the SCF address used in the terminal registration specified in Annex c.3. Note that procedures to obtain the SCF address are not limited to the example shown in this appendix.

v.2. References

References used in this appendix are as follows.

[RFC2131] "Dynamic Host Configuration Protocol", TTC standard JF-IETF-RFC2131, version 1.0, The Telecommunication Technology Committee, May 2009

[RFC3315] "Dynamic Host Configuration Protocol for IPv6", TTC standard JF-IETF-RFC3315, version 1.0, The Telecommunication Technology Committee, May 2009

[RFC3319] "DHCPv6 Options for Session Initiation Protocol Servers", TTC standard JF-IETF-RFC3319, version 1.0, The Telecommunication Technology Committee, May 2009

[RFC3361] "DHCP Options for Session Initiation Protocol Servers", TTC standard JF-IETF-RFC3361, version 1.0, The Telecommunication Technology Committee, May 2009

v.3. DHCP/DHCPv6

In the case that a network provides IPv4 connectivity, it provides procedures using DHCP[RFC2131] to IPv4 terminals. In the case of using DHCP, the IPv4 address and the port number of the SCF is provided by the terminal requesting the option 120[RFC3361]. In the case that a domain list is returned to the option 120 request, the IPv4 address and the port number need to be resolved using DNS, following further the specifications of JF-IETF-RFC3263 [RFC3263].

In the case that the network provides IPv6 connectivity, it provides procedures using DHCPv6[RFC3315] to IPv6 terminals. In the case of using DHCPv6, the IPv6 address and the port number of the SCF is provided by the terminal requesting the option 22[RFC3319] or the option 21[RFC3319]. In the case that the domain list is returned to the option 21, the IPv6 address and the port number need to be resolved using DNS, following further the specifications of JF-IETF-RFC3263[RFC3263].

v.4. Terminal preconfiguration

The terminals are preconfigured with the IP address and the port number of the SCF.

Appendix vi. Signalling rule of SIP messages and headers

(This appendix does not form an integral part of this standard.)

This appendix describes header information setting conditions for request and response messages for each SIP method by dynamic view.

vi.1. Dynamic view and static view

vi.1.1. Static view

Static view refers to the form which can be seen in Annex A of 3GPP TS24.229, where "sending" and "receiving" SIP entities' functional implementation is expressed as M (Mandatory), O (Optional), etc. in regard to application conditions of each header.

Functions are categorized into M (Mandatory) or O (Optional) in static view, from the standpoint of whether SIP entities at both ends of an interface reference point understand the header information or not, in other words, whether they recognize the contents and implement the functions to behave in accordance with specifications such as RFCs. Therefore, M (Mandatory) does not mean that the corresponding header always appears in a SIP message.

vi.1.2. Dynamic view

Dynamic view refers to the header application condition table which can be seen in RFC3261, where it indicates M (Mandatory), O (Optional), etc. from the point of view that if the headers do appear and exist as information items for signalling over an interface between SIP entities, instead of using application categorization such as "sending" and "receiving" sides as in static view.

Dynamic view shows the possible appearance of information as regards whether certain headers exist on the involved interface reference point or not, and if M (Mandatory) is indicated, the header must be included in the corresponding message.

vi.1.3. Adoption of dynamic view for this appendix

This appendix adopts dynamic view presentation for the purpose of the clarification of an interface specification.

vi.1.4. Definition of notation codes in the tables in this appendix

The definition of the notation codes described in the columns of "RFC status" and "Status in this standard" for each table is identical to that of RFC3261.

Appendix Table 6-1/JT-Q3402: Definition of notation codes

Notation code	Definition
m	The header field is mandatory. A mandatory header field MUST be present in a request, and MUST be understood by the UAS receiving the request message. Likewise, a mandatory response header field MUST be present in the response, and the header field MUST be understood by the UAC processing the response.
m*	The header field should be present, but clients or servers need to be prepared to receive messages without that header field. Carriers may clarify "m" or "o".
t	The header field should be present, but clients or servers need to be prepared to receive messages without that header field. If TCP is used as a transport, then the header field is mandatory and MUST be sent.
o	The header field is optional. Optional means that the header field MAY be present in a request or response, and if present in the request or response, it MUST be understood by the receiving side, and the corresponding processing MUST be performed, according to the RFC. Carriers may clarify "m" or "–". (Note) If specially specified, the header field present in the request or response may be allowed to be ignored. These specifications are noted in "Application conditions" and "Remarks" columns. In the case that option items regarding the header field are selected, the header field conforms to the specifications described in option items.
–	The header field is not applicable. The header field that is not applicable MUST NOT be present in a request or response.
c	Application of the header field depends on the context of the message. (Note) In this standard, conditions regarding the application of header fields are described in "Application conditions" column, but it does not affect the "c" classification in the RFC. "c" in this standard means that there are cases that the header field is necessary in the context of signalling. Carriers may clarify "m" or "–". For the header fields which need to be set according to the conditions for the use of signalling, notes are included in "Application conditions" and "Remarks" columns with consideration to RFC specifications.
*	The header field is required if the message body is not empty.

vi.2. ACK

This message is transferred in the forward direction in the case of receiving the final response to an *INVITE* request.

vi.2.1. Supported headers in the ACK request

Appendix Table 6-2/JT-Q3402: Supported headers in the ACK request

Message type: Request

Method: ACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Allow-Events	RFC3265	o	o	o	c2 (Appendix Table 1-2, Items 10 to 15)	c2 (Appendix Table 1-2, Items 10 to 15)	
Authorization	RFC3261	o	–	–	c3	c3	
Call-ID	RFC3261	m	m	m			
Contact	RFC3261	o	o	o			
Content-Disposition	RFC3261	o	–	–	c4	c4	
Content-Encoding	RFC3261	o	–	–	c4	c4	
Content-Language	RFC3261	o	–	–	c4	c4	
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	–	–	c4	c4	
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	–	–	c4	c4	
P-Media-Authorization	RFC3313	o	–	–	c5	c6	
Privacy	RFC3323	o	–	–	c7	c7	
Proxy-Authorization	RFC3261	o	o	–	c8 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c9	
			–	–	c8 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c9	
Reason	RFC3326	o	o	o			(Note 1)
Record-Route	RFC3261	o	o	o			(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Route	RFC3261	c	c	–		c10	
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261	o	–	–	c4	c4	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c3: The *Authorization* header is used only when *REGISTER* requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c4: The message body is not to be used because SDP negotiation by *ACK* is not performed, according to 10.2.1.13 of Annex Table a-1 in Annex a.3.

c5: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c6: Notification of the authentication token using the *P-Media-Authorization* header is not performed because SDP negotiation by *ACK* is not performed, according to 10.2.1.13 of Annex Table a-1 in Annex a.3.

c7:	The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c8:	To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)
c9:	The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.
c10:	The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.
Note 1	Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.2.2. Supported headers in the ACK response

The response message to an *ACK* request message is not specified.

vi.3. BYE

This message is used for releasing the call after a requested call started (either in early dialog or in confirmed dialog).

vi.3.1. Supported headers in the BYE request

Appendix Table 6-3/JT-Q3402: Supported headers in the BYE request

Message type: Request

Method: BYE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o	c2 (Appendix Table 1-2, Items 10 to 15)	c2 (Appendix Table 1-2, Items 10 to 15)	
Authorization	RFC3261	o	–	–	c3	c3	
Call-ID	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			(Note 1)
Content-Encoding	RFC3261	o	o	o			(Note 1)
Content-Language	RFC3261	o	o	o			(Note 1)
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			(Note 1)
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455	o	o	–		c4	(Note 1)
P-Asserted-Identity	RFC3325	o	–	–	c5	c5	
P-Charging-Function-Addresses	RFC3455	o	–	–	c6	c6	
P-Charging-Vector	RFC3455	o	–	–	c6	c6	
P-Preferred-Identity	RFC3325	o	–	–	c7	c7	
Privacy	RFC3323	o	–	–	c8	c8	
Proxy-Authorization	RFC3261	o	o	–	c9 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c10	
			–	–	c9 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c10	
Proxy-Require	RFC3261	o	o	–		c11	
Reason	RFC3326	o	o	o			(Note 1)
Record-Route	RFC3261	o	o	o			(Note 1)
Referred-By	RFC3892	o	o	o	c12 (Appendix Table 1-2, Items 6 to 9)	c12 (Appendix Table 1-2, Items 6 to 9)	(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	c	c	c			
Route	RFC3261	c	c	–		c13	
Security-Client	RFC3329	o	o	–	c14 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c15	

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Security-Verify	RFC3329	o	o	–	c14 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c15	
Supported	RFC3261	o	o	o			(Note 1)
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261	o	o	o			(Note 1)

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c3: The *Authorization* header is used only when *REGISTER* requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.

c6: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.

c8: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c10: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c11: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c12: The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c13: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c14 To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c15: The *Security-Client* and *Security-Verify* headers are not applicable to requests in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.3.2. Supported headers in the BYE response

Appendix Table 6-4/JT-Q3402: Supported headers in the BYE response

Message type: Response

Method: BYE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	RFC3261	c	c	c			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o	c1 (Appendix Table 1-2, Items 10 to 15)	c1 (Appendix Table 1-2, Items 10 to 15)	
Authentication-Info	2xx	RFC3261	o	–	–	c2	c2	
Call-ID		RFC3261	m	m	m			
Contact	3xx	RFC3261	o	-	-	c3	c3	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			(Note 1)
Content-Encoding		RFC3261	o	o	o			(Note 1)
Content-Language		RFC3261	o	o	o			(Note 1)
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			(Note 1)
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c4	(Note 1)
P-Asserted-Identity		RFC3325	o	–	–	c5	c5	
P-Charging-Function-Addresses		RFC3455	o	–	–	c6	c6	
P-Charging-Vector		RFC3455	o	–	–	c6	c6	
P-Preferred-Identity		RFC3325	o	–	–	c7	c7	
Privacy		RFC3323	o	–	–	c8	c8	
Proxy-Authenticate	401	RFC3261	o	–	–	c9	c10	
Proxy-Authenticate	407	RFC3261	m	–	m	c9		

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	18x 2xx	RFC3261	o	o	o			(Note 1)
Require		RFC3261	c	c	c			(Note 1)
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Security-Server	421 494	RFC3329	o	–	o	c11	c12 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Supported	2xx	RFC3261	o	o	o			(Note 1)
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c13	c13	
WWW-Authenticate	407	RFC3261	o	–	–	c13	c13	
Message body		RFC3261	o	o	o			(Note 1)

c1: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c2: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.

c3: Redirection using *3xx* responses is not to be used, according to 10.2.1.8.3 of Annex Table a-1 in Annex a.3.

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.

c6: The *P-Access-Network-Info*, *P-Charging-Vector*, and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3

c7: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.

c8: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c9: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c10: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3. In other words, *401* response itself is not to be used.

c11: The *Security-Server* header is not applicable to responses from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c12: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c13: The *WWW-Authenticate* header is applicable only to the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401*/*407* responses themselves are not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.4. CANCEL

This message is used for terminating the request from the originating side before the establishment of a requested call.

vi.4.1. Supported headers in the CANCEL request

Appendix Table 6-5/JT-Q3402: Supported headers in the CANCEL request

Message type: Request

Method: CANCEL

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Authorization	RFC3261	o	–	–	c2	c2	
Call-ID	RFC3261	m	m	m			
Content-Length	RFC3261	t	t	t			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
Privacy	RFC3323	o	–	–	c3	c3	
Reason	RFC3326	o	o	o			(Note 1)
Record-Route	RFC3261	o	o	o			(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Route	RFC3261	c	c	–		c4	
Supported	RFC3261	o	o	o			(Note 1)
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The *Authorization* header is used only when *REGISTER* requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c3: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c4: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.4.2. Supported headers in the CANCEL response

Appendix Table 6-6/JT-Q3402: Supported headers in the CANCEL response

Message type: Response

Method: CANCEL

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Call-ID		RFC3261	m	m	m			
Content-Length		RFC3261	t	t	t			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
Privacy		RFC3323	o	–	–	c1	c1	
Proxy-Authenticate	401	RFC3261	o	–	–	c2	c2	
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	18x 2xx	RFC3261	o	o	o			(Note 1)
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Server		RFC3261	o	o	o			(Note 1)
Supported	2xx	RFC3261	o	o	o			(Note 1)
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)

c1: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c2: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, nor be used in *401* responses in the direction from the SCF to the EUF, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3. In other words, *401* response itself is not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.5. INVITE

This message is used for call initiation.

vi.5.1. Supported headers in the INVITE request

Appendix Table 6-7/JT-Q3402: Supported headers in the INVITE request

Message type: Request

Method: INVITE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Alert-Info	RFC3261	o	o	o			(Note 1)
Allow	RFC3261	o	m* / o	m* / o	c2	c2	
Allow-Events	RFC3265	o	o	o	c3 (Appendix Table 1-2, Items 10 to 15)	c3 (Appendix Table 1-2, Items 10 to 15)	
Authorization	RFC3261	o	–	–	c4	c4	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			(Note 1)
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
Expires	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
In-Reply-To	RFC3261	o	o	o			(Note 1)
Join	RFC3911	o	o	o	c5 (when Appendix Table 1-7, Item 4 states that UNI condition are "Used in each session as necessary".)	c5 (when Appendix Table 1-7, Item 4 states that UNI condition are "Used in each session as necessary".)	
			–	–	c5 (when Appendix Table 1-7, Item 4 is stated "Not use" for UNI condition.)	c5 (when Appendix Table 1-7, Item 4 is stated "Not use" for UNI condition.)	
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o	c6	c6	
Min-SE	RFC4028	o	o	o	c7	c7	
Organization	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455	o	o	–		c8	(Note 1)
P-Asserted-Identity	RFC3325	o	–	o / –	c9	c9	
P-Called-Party-ID	RFC3455	o	–	o / –	c10	c10	
P-Charging-Function-Addresses	RFC3455	o	–	–	c11	c11	
P-Charging-Vector	RFC3455	o	–	–	c11	c11	
P-Media-Authorization	RFC3313	o	–	o	c12	c13 (when Appendix Table 1-17, Item 1 is stated "Use" for UNI condition.)	
			–	–	c12	c13 (when Appendix Table 1-17, Item 1 is stated "Not use" for UNI condition.)	
P-Preferred-Identity	RFC3325	o	o / –	–	c14	c14	
P-Visited-Network-ID	RFC3455	o	–	–	c11	c11	
Priority	RFC3261	o	o	o			(Note 1)
Privacy	RFC3323	o	o / –	o / –	c15	c15	

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	
Proxy-Authorization	RFC3261	o	o	–	c16 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c17	
			–	–	c16 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c17	
Proxy-Require	RFC3261	o	o	–		c18	
Reason	RFC3326	o	– / o	– / o	(Note 2)	(Note 2)	(Note 1)
Record-Route	RFC3261	o	o	o			
Referred-By	RFC3892	o	o	o	c19 (Appendix Table 1-2, Items 6 to 9)	c19 (Appendix Table 1-2, Items 6 to 9)	
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Replaces	RFC3891	o	o	o	c20 (when Appendix Table 1-7, Item 3 states that UNI condition are "Used in each session as necessary".)	c20 (when Appendix Table 1-7, Item 3 states that UNI condition are "Used in each session as necessary".)	
			–	–	c21 (when Appendix Table 1-7, Item 3 is stated "Not use" for UNI condition.)	c21 (when Appendix Table 1-7, Item 3 is stated "Not use" for UNI condition.)	
Reply-To	RFC3261	o	o	o			(Note 1)
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	c	c	c	c22	c22	
Route	RFC3261	c	m / c	–	c23 (when Appendix Table 1-24, Item 1 is stated "Use" for UNI condition.)	c24	
			– / c	–	c23 (when Appendix Table 1-24, Item 1 is stated "Not use" for UNI condition.)	c24	
Security-Client	RFC3329	o	o	–	c24 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c25	
Security-Verify	RFC3329	o	o	–	c24 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c25	
Session-Expires	RFC4028	o	m	m	c7 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	c7 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	
			o	o	c7 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	c7 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	
Subject	RFC3261	o	o	o			(Note 1)
Supported	RFC3261	m*	m*	m*	c21	c21	
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261	o	m	m	c26	c26	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The setting of *Allow* header is necessary for initial *INVITE*, according to clause 10.2.1.20.5. (Note that the initial *INVITE* without the setting is not handled as error when received.)

c3: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c4: The *Authorization* header is used only when *REGISTER* requests from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c5: In the case that the conference session participation function (*join*) is available over the UNI, the header can be used. (Appendix Table 1-7, Item 4)

c6: In the case that MIME Multipart is used in a message body, the header information is handled as valid information. (Appendix Table 1-10, Items 1 and 2)

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF SCF Send	

c7: The header must be used as specified in clause 10.2.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary.

c8: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c9: The *P-Asserted-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messagess from the SCF to the EUF except for *REGISTER*, and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to initial-*INVITE*, but not to be set to re-*INVITE*.)

c10: The *P-Called-Party-ID* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and performs the notification of the called-party, according to Annex b. (It can be set to initial-*INVITE*, but not to be set to re-*INVITE*.)

c11: The *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c12: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c13: In the case that a message body is set and the notification of an authorization token is performed by the *P-Media-Authorization* header, the header information is handled as valid information. (Appendix Table 1-17, Item 1)

c14: The *P-Preferred-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the EUF to the SCF except for *REGISTER*, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to initial-*INVITE*, but not to be set to re-*INVITE*.)

c15: The *Privacy* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) except for *REGISTER*, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (It can be set to initial-*INVITE*, but not to be set to re-*INVITE*.)

c16: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c17: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c18: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.29 in the main body.

c19: The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c20: In the case that the dialog replacement function (*replaces*) is available over the UNI, the header information can be used. (Appendix Table 1-7, Item 3)

c21: "*timer*" needs to be set to the *Require* header and the *Supported* header in terms of the context, according to clause 10.2.1.20.32 and clause 10.2.1.20.37 in the main body. ("*timer*" should be contextually set to the *Supported* header of initial *INVITE* and re-*INVITE*.)

c22: In the case that the pre-existing route function is used over the UNI, the setting of the *Route* header in an initial *INVITE* is necessary. (Appendix Table 1-24, Item 1)

c23: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c24: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c25: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 Annex Table a-1 in Annex a.3.

c26: SDP offer is described in the body part of an *INVITE* request, according to 10.2.1.13 and 10.2.1.14 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 The *Reason* header is specified in RFC3326, and it is applicable to all the requests inside existing dialogs, *CANCEL*, and all responses, according to the specification. Therefore, it can be used in re-*INVITE*, but cannot be used in initial *INVITE*.

vi.5.2. Supported headers in the INVITE response

Appendix Table 6-8/JT-Q3402: Supported headers in the INVITE response

Message type: Response

Method: INVITE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	2xx	RFC3261	o	o	o			
Accept	415	RFC3261	c	c	c			
Accept-Encoding	2xx	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	2xx	RFC3261	o	o	o			
Accept-Language	415	RFC3261	c	c	c			
Alert-Info	180	RFC3261	o	o	o			(Note 1)
Allow	2xx	RFC3261	m*	m*	m*			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o	c1 (Appendix Table 1-2, Items 10 to 15)	c1 (Appendix Table 1-2, Items 10 to 15)	
Authentication-Info	2xx	RFC3261	o	–	–	c2	c2	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			(Note 1)
Contact	1xx	RFC3261	o	o	o	c3	c3	
Contact	2xx	RFC3261	m	m	m			
Contact	3xx	RFC3261	o	o	o			(Note 2)
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
Expires		RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o	c4	c4	

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Min-SE	422	RFC4028	m	m	m	c5 (Appendix Table 1-7, Item 1)	c5 (Appendix Table 1-7, Item 1)	
Organization		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c6	(Note 1)
P-Asserted-Identity		RFC3325	o	–	–	c7	c7	
P-Charging-Function-Addresses		RFC3455	o	–	–	c8	c8	
P-Charging-Vector		RFC3455	o	–	–	c8	c8	
P-Media-Authorization	101-199	RFC3313	o	–	o	c9	c10 (when Appendix Table 1-17, Item 1 is stated "Use" for UNI condition.)	
				–	–	c9	c10 (when Appendix Table 1-17, Item 1 is stated "Not use" for UNI condition.)	
P-Media-Authorization	2xx	RFC3313	o	–	o	c9		
P-Preferred-Identity		RFC3325	o	–	–	c11	c11	
Privacy		RFC3323	o	–	–	c12	c12	
Proxy-Authenticate	401	RFC3261	o	–	–	c13	c14	
Proxy-Authenticate	407	RFC3261	m	–	m	c13		
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	18x 2xx	RFC3261	o	o	o	c3	c3	
Reply-To		RFC3261	o	o	o			(Note 1)
Require		RFC3261	c	c	c	c3, c5	c3, c5	
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
RSeq	1xx	RFC3262	o	o	o	c3	c3	
Security-Server	421 494	RFC3329	o	–	o	c15	c16 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Session-Expires	2xx	RFC4028	o	m	m	c5 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	c5 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	
				o	o	c5 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	c5 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	
Supported	2xx	RFC3261	m*	m*	m*			
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning	488	RFC3261	o	o	o	c17	c17	
Warning	others	RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c18	c18	
WWW-Authenticate	407	RFC3261	o	–	–	c18	c18	
Message body		RFC3261	o	o	o			

c1: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c2: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.

c3: In the case of providing a reliable provisional response, the setting of "*100rel*" to the *Require* header and the setting of the *RSeq* header are necessary, according to clause 10.2.2.2.6 in the main body. The setting of the *Contact* header is necessary to receive a subsequent *PRACK* request. In the case that the *Record-Route* header is set to the *2xx* response to an *INVITE* request, the *Record-Route* header of the same content should be set to the reliable provisional response as well.

c4: In the case that MIME Multipart is used in a message body, the header information is handled as valid information. (Appendix Table 1-10, Items 1 and 2)

c5: The header must be used as specified in clause 10.2.1.20.32, 10.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary. In the case that the refresher is "*uac*", the setting of "*timer*" to the *Require* header is necessary. (Appendix Table 1-7, Item 1)

c6: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.

c8: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c9: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c10: In the case that a message body is set and the notification of an authorization token is performed by the *P-Media-Authorization* header, the header information is handled as valid information. (Appendix Table 1-17, Item 1)

c11: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.

c12: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c13: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c14: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.

c15: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c16: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c17: Incompatibility of IP version or media type can be notified by setting the *Warning* header in the *488 (Not Acceptable Here)* response and using the set values in Annex e, according to 13 of Annex Table a-1 in Annex a.3 and Annex e.

c18: The *WWW-Authenticate* header is applicable only to the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401*/*407* responses themselves are not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 In the case that the redirection function of the *3xx* response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table 1-12, Items 1 and 2)

vi.6. MESSAGE

This message is used for stateless short message services. *MESSAGE* can be used outside existing dialogs.

vi.6.1. Supported headers in the MESSAGE request

Appendix Table 6-9/JT-Q3402: Supported headers in the MESSAGE request

Message type: Request

Method: MESSAGE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF sends	SCF sends	
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Allow	RFC3261	o	o	o			
Authorization	RFC3261	o	–	–	c2	c2	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			(Note 1)
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
Expires	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
In-Reply-To	RFC3261	o	o	o			(Note 1)
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261		o	o	c3	c3	
Organization	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455	o	o	–		c4	(Note 1)
P-Asserted-Identity	RFC3325		–	o / –	c5	c5	
P-Called-Party-ID	RFC3455	o	–	o / –	c6	c6	
P-Charging-Function-Addresses	RFC3455	o	–	–	c7	c7	
P-Charging-Vector	RFC3455	o	–	–	c7	c7	
P-Preferred-Identity	RFC3325		o / –	–	c8	c8	
P-Visited-Network-ID	RFC3455	o	–	–	c7	c7	
Priority	RFC3261	o	o	o			(Note 1)
Privacy	RFC3323	o	o / –	o / –	c9	c9	
Proxy-Authorization	RFC3261	o	o	–	c10 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication" for UNI condition.)	c11	
			–	–	c10 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication" for UNI condition.)	c11	
Proxy-Require	RFC3261	o	o	–		c12	
Reason	RFC3326	o	– / o	- / o	(Note 2)	(Note 2)	(Note 1)
Referred-By	RFC3892		o	o	c13 (Appendix Table 1-2, Items 6 to 9)	c13 (Appendix Table 1-2, Items 6 to 9)	(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Reply-To	RFC3261	o	o	o			(Note 1)
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	c	c	c			
Route	RFC3261	c	m / c	–	c14 (when Appendix Table 1-24, Item 1 is stated "Use" for UNI condition.)	c15	
			– / c	–	c14 (when Appendix Table 1-24, Item 1 is stated "Not use" for	c15	

Header	Reference	RFC status	Status in this standard: EUF Send	Status in this standard: SCF Send	Application conditions: EUF sends	Application conditions: SCF sends	Remarks
					UNI condition.)		
Security-Client	RFC3329	o	o	–	c16 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c17	
Security-Verify	RFC3329	o	o	–	c16 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c17	
Subject	RFC3261	o	o	o			(Note 1)
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261		o	o			

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c3: In the case that MIME Multipart is used in a message body, the header information is handled as valid information. (Appendix Table 1-10, Items 3 and 4)

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Asserted-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to *MESSAGE* requests outside existing dialogs, but not to be set to *MESSAGE* requests inside existing dialogs.)

c6: The *P-Called-Party-ID* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and performs the notification of the called-party, according to Annex b. (It can be set to MESSAGE requests outside existing dialogs, but not to be set to *MESSAGE* requests inside existing dialogs.)

c7: The *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c8: The *P-Preferred-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the EUF to the SCF except for *REGISTER*, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to initial-*INVITE*, but not to be set to re-*INVITE*.)

c9: The *Privacy* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) except for *REGISTER*, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (It can be set to *MESSAGE* requests outside existing dialogs, but not to be set to *MESSAGE* requests inside existing dialogs.)

c10: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c11: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c12: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c13: The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c14: In the case that the pre-existing route function is used over the UNI, the setting of the *Route* header in a *MESSAGE* requests outside existing dialogs is necessary. (Appendix Table 1-24, Item 1)

c15: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c16: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c17: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 The *Reason* header is specified in RFC3326, and it is applicable to all the requests inside existing dialogs, *CANCEL*, and all responses, according to the specification. Therefore, it can be used in *MESSAGE* requests inside existing dialogs, but cannot be used in *MESSAGE* requests outside existing dialogs.

vi.6.2. Supported headers in the MESSAGE response

Appendix Table 6-10/JT-Q3402: Supported headers in the MESSAGE response

Message type: Response

Method: MESSAGE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	RFC3261	m*	m*	m*			
Accept-Encoding	415	RFC3261	m*	m*	m*			
Accept-Language	415	RFC3261	m*	m*	m*			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Authentication-Info	2xx	RFC3261	o	–	–	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			(Note 1)
Contact	3xx	RFC3261	o	o	o			(Note 2)
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			(Note 1)
Content-Encoding		RFC3261	o	o	o			(Note 1)
Content-Language		RFC3261	o	o	o			(Note 1)
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			(Note 1)
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
Expires		RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
MIME-Version	4xx-6xx	RFC3261		o	o	c2	c2	(Note 1)
Organization		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c3	(Note 1)
P-Charging-Function-Addresses		RFC3455	o	–	–	c4	c4	
P-Charging-Vector		RFC3455	o	–	–	c4	c4	
Privacy		RFC3323	o	–	–	c5	c5	
Proxy-Authenticate	401	RFC3261	o	–	–	c6	c7	
Proxy-Authenticate	407	RFC3261	m	–	m	c6		

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Reason		RFC3326	o	o	o			(Note 1)
Reply-To		RFC3261	o	o	o			(Note 1)
Require		RFC3261	c	c	c			(Note 1)
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Security-Server	421 494	RFC3329	o	–	o	c8	c9 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	(Note 3)	(Note 3)	
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c10	c10	
WWW-Authenticate	407	RFC3261	o	–	–	c10	c10	
Message body	2xx-3xx	RFC3261	–	–	–			
Message body	4xx-6xx	RFC3261	o	o	o			(Note 1)

c1: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.

c2: In the case that MIME Multipart is used in a message body, the header information is handled as valid information. (Appendix Table 1-10, Items 3 and 4)

c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c4: The *P-Charging-Vector* and P-Charging-Function-Addresses headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c6: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c7: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.

c8: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c9: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c10: The *WWW-Authenticate* header is applicable only to the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401*/*407* responses themselves are not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifiesas the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 In the case that the redirection function of the *3xx* response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table 1-12, Items 1 and 2)

Note 3 Although specified as "o" in RFC3903, the *Unsupported* header is set to be "m" based on RFC3261.

vi.7. NOTIFY

This message is used to notify event-related information within an event subscription (event dialog). *NOTIFY* is used in conjunction with a particular event subscription.

The event subscription is established based on the use of *SUBSCRIBE* method, *REFER* method, or other implicit subscriptions.

vi.7.1. Supported headers in the NOTIFY request

Appendix Table 6-11/JT-Q3402: Supported headers in the NOTIFY request

Message type: Request

Method: NOTIFY

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o			
Authorization	RFC3261	o	–	–	c2	c2	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261		–	–	(Note 2)	(Note 2)	
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
Event	RFC3265	m	m	m			
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
P-Access-Network-Info	RFC3455	o	o	–		c3	(Note 1)
P-Asserted-Identity	RFC3325	o	–	–	c4	c4	
P-Charging-Function-Addresses	RFC3455	o	–	–	c5	c5	
P-Charging-Vector	RFC3455	o	–	–	c5	c5	
P-Preferred-Identity	RFC3325	o	–	–	c6	c6	
Privacy	RFC3323	o	–	–	c7	c7	
Proxy-Authorization	RFC3261	o	o	–	c8 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication".)	c9	
			–	–	c8 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c9	
Proxy-Require	RFC3261	o	o	–		c10	
Reason	RFC3326	o	o	o			(Note 1)
Record-Route	RFC3261	o	o	o			(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	o	o	o			
Route	RFC3261	c	c	–		c11	
Security-Client	RFC3329	o	o	–	c12 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c13	

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Security-Verify	RFC3329	o	o	–	c12 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c13	
Subscription-State	RFC3265	m	m	m			
Supported	RFC3261	o	o	o			
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Warning	RFC3261	o	o	o			(Note 1)
Message body	RFC3261		o	o	(Note 3)	(Note 3)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c4: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.

c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex Table a-1.

c6: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.

c7: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (*NOTIFY* is used within a subscription (equivalent to a dialog). Therefore, the header is not applicable.)

c8: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c9: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c10: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c11: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c12: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c13: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 The *Call-Info* header shows additional information about the sender of the messages. There is no description of the application of the header into *NOTIFY* in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in *NOTIFY*. Furthermore, security risks of *Call-Info* are noted in RFC3261. An ill-prepared use of the header should be avoided.

Note 3 It is used when additional information is present. Formatting and other features depend on *Content-Type*.

vi.7.2. Supported headers in the NOTIFY response

Appendix Table 6-12/JT-Q3402: Supported headers in the NOTIFY response

Message type: Response

Method: NOTIFY

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	o	o	o			
Accept-Language	415	RFC3261	o	o	o			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o			
Allow-Events	489	RFC3265	m	m	m			
Authentication-Info	2xx	RFC3261	o	–	–	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261		–	–	(Note 2)	(Note 2)	
Contact	1xx	RFC3261	o	o	o			
Contact	2xx	RFC3261	o	o	o			
Contact	3xx	RFC3261	m	–	–	c2	c2	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			(Note 1)
Content-Encoding		RFC3261	o	o	o			(Note 1)
Content-Language		RFC3261	o	o	o			(Note 1)
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			(Note 1)
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c3	(Note 1)
P-Asserted-Identity		RFC3325	o	–	–	c4	c4	
P-Charging-Function-Addresses		RFC3455	o	–	–	c5	c5	
P-Charging-Vector		RFC3455	o	–	–	c5	c5	

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
P-Preferred-Identity		RFC3325	o	–	–	c6	c6	
Privacy		RFC3323	o	–	–	c7	c7	
Proxy-Authenticate	407	RFC3261	m	–	m	c8		
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	2xx 401 484	RFC3261	o	o	o			(Note 1)
Require		RFC3261	o	o	o			
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
RSeq	1xx	RFC3261	o	–	–	(Note 3)	(Note 3)	
Security-Server	421 494	RFC3329	o	–	–	c9	c10 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	(Note 4)	(Note 4)	
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c11	c11	
Message body		RFC3261		o	o	(Note 5)	(Note 5)	(Note 1)

c1: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.
c2: Redirection using *3xx* responses is not to be used, according to 10.2.1.8.3 of Annex Table a-1 in Annex a.3.
c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c4: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.
c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.
c6: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.
c7: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c8: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, the *407* response itself is not to be used.
c9: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c10: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)
c11: The *WWW-Authenticate* header is applicable only for the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401* response itself is not to be used.
Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	

message to send is dependent on the policy of the NGN carrier.

Note 2 The *Call-Info* header shows additional information about the sender of the messages. There is no description of the application of the header into *NOTIFY* in RFCs and other documents. Therefore, it is difficult to define its reaction when using the header in *NOTIFY*. Furthermore, security risks of *Call-Info* are noted in RFC3261. An ill-prepared use of the header should be avoided.

Note 3 The *100rel* option (*PRACK*) is not to be used in NOTIFY.

Note 4 Although specified as "o" in RFC3265, the Unsupported header is set to be "m" based on RFC3261.

Note 5 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

vi.8. PRACK

This message is used for providing a reliable provisional response message (*100rel*) in call establishment.

vi.8.1. Supported headers in the PRACK request

Appendix Table 6-13/JT-Q3402: Supported headers in the PRACK request

Message type: Request

Method: PRACK

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o	c2 (Appendix Table 1-2, Items 10 to 15)	c2 (Appendix Table 1-2, Items 10 to 15)	
Authorization	RFC3261	o	–	–	c3	c3	
Call-ID	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
P-Access-Network-Info	RFC3455	o	o	–		c4	(Note 1)
P-Charging-Function-Addresses	RFC3455	o	–	–	c5	c5	
P-Charging-Vector	RFC3455	o	–	–	c5	c5	
P-Media-Authorization	RFC3313	o	–	o	c6	c7	
Privacy	RFC3323	o	–	–	c8	c8	
Proxy-Authorization	RFC3261	o	o	–	c9 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	RFC3261	o	o	–		c11	
RAck	RFC3262	m	m	m			
Reason	RFC3326	o	o	o			(Note 1)
Record-Route	RFC3261	o	o	o			(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	c	c	c			
Route	RFC3261	c	c	–		c12	
Supported	RFC3261	o	o	o			(Note 1)
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261		o	o	c13 (Appendix Table 1-22, Items 2 to 3)	c13 (Appendix Table 1-22, Items 2 to 3)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2:	In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)
c3:	The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.
c4:	The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c5:	The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.
c6:	Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c7:	In the case that SDP offer is performed by *PRACK*, the header information is handled as valid information. (Appendix Table 1-22, Item 3)
c8:	The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c9:	To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)
c10:	The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.
c11:	The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.
c12:	The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.
c13:	The message body part of *PRACK* should be supported, according to clause 10.2.1.7.4.1 in the main body. In the case that the SDP setting of the body part is available over the UNI, the message body information is handled as valid information. (Appendix Table 1-22, Items 2 to 3)
Note 1	Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.8.2. Supported headers in the PRACK response

Appendix Table 6-14/JT-Q3402: Supported headers in the PRACK response

Message type: Response

Method: PRACK

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				SCF Send	EUF Send	EUF Send	SCF Send	
Accept	415	RFC3261	c	c	c			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events	2xx	RFC3265	o	o	o	c1 (Appendix Table 1-2, Items 10 to 15)	c1 (Appendix Table 1-2, Items 10 to 15)	
Authentication-Info	2xx	RFC3261	o	–	–	c2	c2	
Call-ID		RFC3261	m	m	m			
Contact	3xx	RFC3261	o	–	–	c3	c3	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
P-Access-Network-Info		RFC3455	o	o	–		c4	(Note 1)
P-Charging-Function-Addresses		RFC3455	o	–	–	c5	c5	
P-Charging-Vector		RFC3455	o	–	–	c5	c5	
P-Media-Authorization	2xx	RFC3313	o	–	o	c6	c7	
Privacy		RFC3323	o	–	–	c8	c8	
Proxy-Authenticate	401	RFC3261	o	–	–	c9	c10	
Proxy-Authenticate	407	RFC3261	m	–	m	c9		
Reason		RFC3326	o	o	o			(Note 1)

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				SCF Send	EUF Send	EUF Send	SCF Send	
Record-Route	18x 2xx	RFC3261	o	o	o			(Note 1)
Require		RFC3261	c	c	c			
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Server		RFC3261	o	o	o			(Note 1)
Supported	2xx	RFC3261	o	o	o			(Note 1)
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c11	c11	
Message body		RFC3261		o	o	c12	c12	

c1: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c2: Update of authentication information by the Authentication-Info header is not performed because the *Authorization* header is not to be used in the corresponding request.

c3: Redirection using *3xx* responses is not to be used, according to 10.2.1.8.3 of Annex Table a-1 in Annex a.3.

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: In the case that SDP offer is performed by *PRACK*, the header information is handled as valid information. (Appendix Table 1-22, Item 3)

c8: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c9: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c10: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.

c11: The *WWW-Authenticate* header is applicable only for the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401* response itself is not to be used.

c12: The message body part of *PRACK* should be supported, according to clause 10.2.1.7.4.1 in the main body. In the case that the SDP setting of the body part is available over the UNI, the message body information is handled as valid information. (Appendix Table 1-22, Items 2 to 3)

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.9. PUBLISH

This message is used in the case of newly issuing or updating the subscribed information, such as presence information.

vi.9.1. Supported headers in the PUBLISH request

Appendix Table 6-15/JT-Q3402: Supported headers in the PUBLISH request

Message type: Request

Method: PUBLISH

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o	c2 (Appendix Table 1-2, Items 10 to 15)	c2 (Appendix Table 1-2, Items 10 to 15)	
Authorization	RFC3261	o	–	–	c3	c3	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			(Note 1)
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
Event	RFC3265	m	m	m			
Expires	RFC3261	o	o	o			
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Organization	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455		o	–		c4	(Note 1)
P-Asserted-Identity	RFC3325		–	o / –	c5	c5	
P-Called-Party-ID	RFC3455		–	o / –	c6	c6	
P-Charging-Function-Addresses	RFC3455		–	–	c7	c7	
P-Charging-Vector	RFC3455		-	–	c7	c7	
P-Preferred-Identity	RFC3325		o / –	–	c8	c8	
P-Visited-Network-ID	RFC3455		–	–	c7	c7	
Priority	RFC3261	o	o	o			(Note 1)
Privacy	RFC3323		o / –	o / –	c9	c9	
Proxy-Authorization	RFC3261	o	o	–	c10 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication".)	c11	
			–	–	c10 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c11	
Proxy-Require	RFC3261	o	o	–		c12	
Reason	RFC3326	o	– / o	– / o	(Note 2)	(Note 2)	(Note 1)
Referred-By	RFC3892		o	o	c13 (Appendix Table 1-2, Items 6 to 9)	c13 (Appendix Table 1-2, Items 6 to 9)	(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	o	o	o			

Header	Reference	RFC status	Status in this standard: EUF Send	Status in this standard: SCF Send	Application conditions: EUF Send	Application conditions: SCF Send	Remarks
Route	RFC3261	c	m / c	–	c14 (when Appendix Table 1-24, Item 1 is stated "Use" for UNI condition.)	c15	
			– / c	–	c14 (when Appendix Table 1-24, Item 1 is stated "Not use" for UNI condition.)	c15	
Security-Client	RFC3329		o	–	c16 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c17	
Security-Verify	RFC3329		o	–	c16 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c17	
SIP-If-Match	RFC3261	o	o	o			
Subject	RFC3261	o	o	o			(Note 1)
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261		o	o			

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)

c3: The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Asserted-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to *PUBLISH* requests outside *INVITE* dialogs, but not to be set to *PUBLISH* requests inside *INVITE* dialogs.)

c6: The *P-Called-Party-ID* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and performs the notification of the called-party, according to Annex b. (It can be set to *PUBLISH* requests outside *INVITE* dialogs, but not to be set to *PUBLISH* requests inside *INVITE* dialogs.)

c7: The *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c8: The *P-Preferred-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the EUF to the SCF except for *REGISTER*, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to *PUBLISH* requests outside *INVITE* dialogs, but not to be set to *PUBLISH* requests inside *INVITE* dialogs.)

c9: The *Privacy* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) except for *REGISTER*, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (It can be set to *PUBLISH* requests outside *INVITE* dialogs, but not to be set to *PUBLISH* requests inside *INVITE* dialogs.)

c10: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c11: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c12: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c13: The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c14: In the case that the pre-existing route function is used over the UNI, the setting of the *Route* header in *PUBLISH* requests outside *INVITE* dialogs is necessary. (Appendix Table 1-24, Item 1)

c15: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c16: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c17: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 The *Reason* header is specified in RFC3326, and it is applicable to all the requests inside existing dialogs, *CANCEL*, and all responses, according to the specification. Therefore, it can be used in *PUBLISH* requests inside *INVITE* dialogs, but cannot be used in *PUBLISH* requests outside *INVITE* dialogs.

vi.9.2. Supported headers in the PUBLISH response

Appendix Table 6-16/JT-Q3402: Supported headers in the PUBLISH response

Message type: Response

Method: PUBLISH

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	RFC3261	m*	m*	m*			
Accept-Encoding	415	RFC3261	m*	m*	m*			
Accept-Language	415	RFC3261	m*	m*	m*			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events	489	RFC3261	m	m	m			
Authentication-Info	2xx	RFC3261	o	–	–	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			(Note 1)
Contact	3xx	RFC3261	o	o	o			(Note 2)
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			(Note 1)
Content-Encoding		RFC3261	o	o	o			(Note 1)
Content-Language		RFC3261	o	o	o			(Note 1)
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			(Note 1)
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
Expires	2xx	RFC3261	m	m	m			
Expires	others	RFC3261	o	o	o			
From		RFC3261	m	m	m			
Min-Expires	423	RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			(Note 1)
Organization		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455		o	–		c2	(Note 1)
P-Charging-Function-Addresses		RFC3455		–	–	c3	c3	
P-Charging-Vector		RFC3455		–	–	c3	c3	
Privacy		RFC3323		–	–	c4	c4	

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Proxy-Authenticate	401	RFC3261	o	–	–	c5	c6	
Proxy-Authenticate	407	RFC3261	m	–	m	c5		
Reason		RFC3326	o	o	o			(Note 1)
Require		RFC3261	o	o	o			
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Security-Server	421 494	RFC3329		–	o	c7	c8 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
SIP-ETag	2xx	RFC3261	m	m	m			
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	(Note 3)		
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c9	c9	
WWW-Authenticate	407	RFC3261	o	–	–	c9	c9	
Message body		RFC3261		o	o			(Note 1)

c1: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.

c2: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c3: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c4: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c5: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c6: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.

c7: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c8: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c9: The *WWW-Authenticate* header is applicable only to the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401*/*407* responses themselves are not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 In the case that the redirection function of the *3xx* response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table 1-12, Items 1 and 2)

Note 3 Although specified as "o" in RFC3903, the Unsupported header is set to be "m" based on RFC3261.

vi.10. REFER

The message is used either inside or outside existing dialogs, and for requesting action to the recipient of the message, such as call origination specified in *Refer-To*.

vi.10.1. Supported headers in the REFER request

Appendix Table 6-17/JT-Q3402: Supported headers in the REFER request

Message type: Request

Method: REFER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265		o	o	(Note 2)	(Note 2)	
Authorization	RFC3261	o	–	–	c2	c2	
Call-ID	RFC3261	m	m	m			
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	o	t	t	(Note 3)		
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
Expires	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Organization	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455	o	o	–		c3	(Note 1)
P-Asserted-Identity	RFC3325	o	–	o / –	c4	c4	
P-Called-Party-ID	RFC3455	o	–	o / –	c5	c5	
P-Charging-Function-Addresses	RFC3455	o	–	–	c6	c6	
P-Charging-Vector	RFC3455	o	–	–	c6	c6	
P-Preferred-Identity	RFC3325	o	o / –	–	c7	c7	
P-Visited-Network-ID	RFC3455	o	–	–	c6	c6	
Privacy	RFC3323	o	o / –	o / –	c8	c8	
Proxy-Authorization	RFC3261	o	o	–	c9 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	RFC3261	o	o	–		c11	
Reason	RFC3326	o	– / o	– / o	(Note 4)	(Note 4)	(Note 1)
Record-Route	RFC3261	o	o	o			
Refer-To	RFC3515	m	m	m			
Referred-By	RFC3892		o	o	c12 (Appendix Table 1-2, Items 6 to 9)	c12 (Appendix Table 1-2, Items 6 to 9)	
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	c	c	c			

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Route	RFC3261	c	m / c	–	c13 (when Appendix Table 1-24, Item 1 is stated "Use" for UNI condition.)	c14	
			– / c	–	c13 (when Appendix Table 1-24, Item 1 is stated "Not use" for UNI condition.)	c14	
Security-Client	RFC3329		o	–	c15 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c16	
Security-Verify	RFC3329		o	–	c15 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c16	
Supported	RFC3261	o	o	o			
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261		o	o	(Note 5)	(Note 5)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c4: The *P-Asserted-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to *REFER* outside existing dialogs, but not to be set to *REFER* inside existing dialogs.)

c5: The *P-Called-Party-ID* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and performs the notification of the called-party, according to Annex b. (It can be set to *REFER* outside existing dialogs, but not to be set to *REFER* inside existing dialogs.)

c6: The *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: The *P-Preferred-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the EUF to the SCF except for *REGISTER*, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to *REFER* outside existing dialogs, but not to be set to *REFER* inside existing dialogs.)

c8: The *Privacy* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) except for *REGISTER*, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (It can be set to *REFER* requests outside existing dialogs, but not to be set to *REFER* requests inside existing dialogs.)

c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c10: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c11: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c12: The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c13: In the case that the pre-existing route function is used over the UNI, the setting of the *Route* header in *REFER* requests outside existing dialogs is necessary. (Appendix Table 1-24, Item 1)

c14: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c15: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c16: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in theSIP message to send is dependent on the policy of the NGN carrier.

Note 2 UA sending *REFER* is considered to support "*refer*" event option and there may be a possibility of related information being set. Therefore, although there are no RFC specifications, it is indicated as optional.

Note 3 Although specified as "o" in RFC3515, the *Content-Length* header is set to be "t" based on RFC3261.

Note 4 The *Reason* header is specified in RFC3326, and it is applicable to all the requests inside existing dialogs, *CANCEL*, and all responses, according to the specification. Therefore, it can be used in *REFER* inside existing dialogs, but cannot be used in *REFER* outside existing dialogs.

Note 5 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

vi.10.2. Supported headers in the REFER response

Appendix Table 6-18/JT-Q3402: Supported headers in the REFER response

Message type: Response

Method: REFER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	415	RFC3261	c	c	c			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events		RFC3265		o	o	(Note 2)	(Note 2)	
Authentication-Info	2xx	RFC3261	o	–	–	c1	c1	
Call-ID		RFC3261	m	m	m			
Contact	2xx	RFC3261	m	m	m			
Contact	3xx-6xx	RFC3261	o	o	o			(Note 3)
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	o	t	t	(Note 4)	(Note 4)	
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	3xx-6xx	RFC3261	o	o	o			(Note 1)
Expires		RFC3261	o	o	o			
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
Organization		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c2	(Note 1)
P-Asserted-Identity		RFC3325	o	–	–	c3	c3	
P-Charging-Function-Addresses		RFC3455	o	–	–	c4	c4	
P-Charging-Vector		RFC3455	o	–	–	c4	c4	
P-Preferred-Identity		RFC3325	o	–	–	c5	c5	
Privacy		RFC3323	o	–	–	c6	c6	

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Proxy-Authenticate	401	RFC3261	o	–	–	c7	c8	
Proxy-Authenticate	407	RFC3261	m	–	m	c7		
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	18x 2xx	RFC3261	o	o	o			
Require		RFC3261	c	c	c			
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Security-Server	421 494	RFC3329		–	o	c9	c10 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	(Note 5)	(Note 5)	
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c11	c11	
WWW-Authenticate	407	RFC3261	o	–	–	c11	c11	
Message body		RFC3261		o	o	(Note 6)	(Note 6)	

c1: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.

c2: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c3: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.

c4: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.

c6: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c7: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c8: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.

c9: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c10: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c11: The *WWW-Authenticate* header is applicable only to the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401*/*407* responses themselves are not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 UA receiving *REFER* is considered to support "*refer*" event options and there may be a possibility of the information being set. Therefore, although there are no RFC specifications, it is indicated as optional.

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	

Note 3 In the case that the redirection function of the *3xx* response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table 1-12, Items 1 and 2)

Note 4 Although specified as "o" in RFC3515, the *Content-Length* header is set to be "t" based on RFC3261.

Note 5 Although specified as "o" in RFC3515, the *Unsupported* header is set to be "m" based on RFC3261.

Note 6 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

vi.11. REGISTER

This message is used for terminal registration, deletion, or registration update.

vi.11.1. Supported headers in the REGISTER request

Appendix Table 6-19/JT-Q3402: Supported headers in the REGISTER request

Message type: Request

Method: REGISTER

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o				
Accept-Encoding	RFC3261	o	o				
Accept-Language	RFC3261	o	o				
Allow	RFC3261	o	o				
Allow-Events	RFC3265	o	o		c1		
Authorization	RFC3261	o	o		c2 (when Appendix Table 1-11, Item 1 is stated other than "Not perform" for UNI condition.)		
			–		c2 (when Appendix Table 1-11, Item 1 is stated "Not perform" for UNI condition.)		
Call-ID	RFC3261	m	m				
Call-Info	RFC3261	o	o				(Note 1)
Contact	RFC3261	o	o				
Content-Disposition	RFC3261	o	o				(Note 1)
Content-Encoding	RFC3261	o	o				(Note 1)
Content-Language	RFC3261	o	o				(Note 1)
Content-Length	RFC3261	t	t				
Content-Type	RFC3261	*	*				(Note 1)
CSeq	RFC3261	m	m				
Date	RFC3261	o	o				(Note 1)
Expires	RFC3261	o	o				
From	RFC3261	m	m				
Max-Forwards	RFC3261	m	m				
MIME-Version	RFC3261	o	o				(Note 1)
Organization	RFC3261	o	o				(Note 1)
P-Access-Network-Info	RFC3455	o	o				(Note 1)
P-Charging-Function-Addresses	RFC3455	o	–		c3		
P-Charging-Vector	RFC3455	o	–		c3		
P-Visited-Network-ID	RFC3455	o	–		c3		
Path	RFC3327	o	–		c4		
Privacy	RFC3323	o	–		c5		
Proxy-Authorization	RFC3261	o	–		c6		
Proxy-Require	RFC3261	o	o				
Referred-By	RFC3892	o	o		c7 (Appendix Table 1-2, Items 6 to 9)		(Note 1)
Request-Disposition	RFC3841	o	o		c8 (Appendix Table 1-7, Item 6)		
Require	RFC3261	c	c				
Route	RFC3261	c	–		c9		
Security-Client	RFC3329	o	o		c10 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)		
Security-Verify	RFC3329	o	o		c11 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)		
Supported	RFC3261	o	o		c12		
Timestamp	RFC3261	o	o				(Note 1)
To	RFC3261	m	m				
User-Agent	RFC3261	o	o				(Note 1)
Via	RFC3261	m	m				
Message body	RFC3261	o	o				(Note 1)

c1:	In the case that the terminal capabilities notification function, Caller Preferences (pref tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)
c2:	To be used in the case that the HTTP Digest authentication or AKA authentication is performed to *REGISTER* requests (Appendix Table 1-11, Item 1)
c3:	The *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.
c4:	The *Path* header is not applicable to a request in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c5:	The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c6:	The *Proxy-Authorization* header is not applicable to *REGISTER* requests, according to 10.2.1.20.28 of Annex Table a-1 in Annex a.3.
c7:	The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.
c8:	In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)
c9:	The pre-existing route is not to be provided to *REGISTER* requests, according to 10.2.1.20.34 of Annex Table a-1 in Annex a.3 and Annex c.3.2.
c10:	The *Security-Client* and *Security-Verify* headers are to be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used, according to 10.1 of Annex Table a-1 in Annex a.3. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)
c11:	In the case that the *REGISTER* route record function (*path*) is used, "*path*" needs to be listed. (Appendix Table 1-24, Item 1)
Note 1	Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.11.2. Supported headers in the REGISTER response

Appendix Table 6-20: Supported headers in the REGISTER response

Message type: Response

Method: REGISTER

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
Accept	2xx	RFC3261	o		o			
Accept	415	RFC3261	c		c			
Accept-Encoding	2xx	RFC3261	o		o			
Accept-Encoding	415	RFC3261	c		c			
Accept-Language	2xx	RFC3261	o		o			
Accept-Language	415	RFC3261	c		c			
Allow	2xx	RFC3261	o		o			
Allow	405	RFC3261	m		m			
Allow	others	RFC3261	o		o			
Allow-Events	2xx	RFC3265	o		o		c1 (Appendix Table 1-2, Items 10 to 15)	
Authentication-Info	2xx	RFC3261	o		o			
Call-ID		RFC3261	m		m			
Call-Info		RFC3261	o		o			
Contact	2xx	RFC3261	o		o			
Contact	3xx	RFC3261	o		–		c2	
Contact	485	RFC3261	o		o			
Content-Disposition		RFC3261	o		o			
Content-Encoding		RFC3261	o		o			
Content-Language		RFC3261	o		o			
Content-Length		RFC3261	t		t			
Content-Type		RFC3261	*		*			
CSeq		RFC3261	m		m			
Date		RFC3261	o		o			
Error-Info	300-699	RFC3261	o		o			
Expires		RFC3261	o		o			
From		RFC3261	m		m			
Min-Expires	423	RFC3261	m		m			
MIME-Version		RFC3261	o		o			
Organization		RFC3261	o		o			

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
P-Access-Network-Info		RFC3455	o		–		c3	
P-Associated-URI	2xx	RFC3455	o		o		c4 (when Appendix Table 1-24, Item 3 is stated "May notify" for UNI condition.)	
					–		c4 (when Appendix Table 1-24, Item 3 is stated "Not notify" for UNI condition.)	
P-Charging-Function-Addresses		RFC3455	o		–		c5	
P-Charging-Vector		RFC3455	o		–		c5	
Path	2xx	RFC3327	o		o			
Privacy		RFC3323	o		–		c6	
Proxy-Authenticate	401	RFC3261	o		–		c7	
Proxy-Authenticate	407	RFC3261	m		–		c7	
Reason		RFC3326	o		o			
Require		RFC3261	c		c			
Retry-After	404 413 480 486	RFC3261	o		o			
Retry-After	500 503	RFC3261	o		o			
Retry-After	600 603	RFC3261	o		o			
Security-Server	421 494	RFC3329	o		o		c8 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Service-Route	2xx	RFC3608	o		o		c9 (when Appendix Table 1-24, Item 1 is stated "Provide" for UNI condition.)	
					–		c9 (when Appendix Table 1-24, Item 1 is stated "Not provide" for UNI condition.)	
Server		RFC3261	o		o			
Supported	2xx	RFC3261	o		o			
Timestamp		RFC3261	o		o			
To		RFC3261	m		m			
Unsupported	420	RFC3261	m		m			
User-Agent		RFC3261	o		o			
Via		RFC3261	m		m			
Warning		RFC3261	o		o			
WWW-Authenticate	401	RFC3261	m		m			
WWW-Authenticate	407	RFC3261	o		o			

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF sends	EUF sends	SCF sends	
Message body		RFC3261	o		o			

c1: In the case that *SUBSCRIBE*/*NOTIFY* is available over the UNI, the header information is handled as valid information. (Appendix Table 1-2, Items 10 to 15)
c2: Redirection using *3xx* responses is not to be used, according to 10.2.1.8.3 of Annex Table a-1 in Annex a.3.
c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c4: To be used in the case that the notification of network-asserted user identity using the *P-Associated-URI* header is performed. (Appendix Table 1-24, Item 3)
c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.
c6: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c7: The *Proxy-Authenticate* header is not to be used in a *REGISTER* request, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.
c8: The *Security-Server* header applicable in the case that AKA authentication is used or TLS connection of call control signals is used, according to 10.1 of Annex Table a-1 in Annex a.3. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)
c9: In the case that the pre-existing route function is used over the UNI, the setting is necessary. (Appendix Table 1-24, Item 1)

vi.12. SUBSCRIBE

This message is used to establish an event subscription (event dialog).

vi.12.1. Supported headers in the SUBSCRIBE request

Appendix Table 6-21/JT-Q3402: Supported headers in the SUBSCRIBE request

Message type: Request

Method: SUBSCRIBE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Allow-Events	RFC3265	o	o	o			
Authorization	RFC3261	o	–	–	c2	c2	
Call-ID	RFC3261	m	m	m			
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
Event	RFC3265	m	m	m			
Expires	RFC3261	o	o	o			
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Organization	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455	o	o	–		c3	(Note 1)
P-Asserted-Identity	RFC3325	o	–	o / –	c4	c4	
P-Called-Party-ID	RFC3455	o	–	o / –	c5	c5	
P-Charging-Function-Addresses	RFC3455	o	–	–	c6	c6	
P-Charging-Vector	RFC3455	o	–	–	c6	c6	
P-Preferred-Identity	RFC3325	o	o / -	–	c7	c7	
P-Visited-Network-ID	RFC3455	o	–	–	c6	c6	
Priority	RFC3261	o	o	o			(Note 1)
Privacy	RFC3323	o	o / -	o / -	c8	c8	
Proxy-Authorization	RFC3261	o	o	–	c9 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	RFC3261	o	o	–		c11	
Reason	RFC3326	o	– / o	– / o	(Note 2)	(Note 2)	(Note 1)
Record-Route	RFC3261	o	o	o			
Referred-By	RFC3892	o	o	o	c12 (Appendix Table 1-2, Items 6 to 9)	c12 (Appendix Table 1-2, Items 6 to 9)	
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	o	o	o			

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Route	RFC3261	c	m / c	–	c13 (when Appendix Table 1-24, Item 1 is stated "Use" for UNI condition.)	c14	
			– / c	–	c13 (when Appendix Table 1-24, Item 1 is stated "Not use" for UNI condition.)	c14	
Security-Client	RFC3329	o	o	–	c15 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c16	
Security-Verify	RFC3329	o	o	–	c15 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c16	
Supported	RFC3261	o	o	o			
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261		o	o	(Note 3)	(Note 3)	

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c4: The *P-Asserted-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and transmits the calling-party's information, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to initial-*SUBSCRIBE*, but not to be set to re-*SUBSCRIBE*.)

c5: The *P-Called-Party-ID* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the SCF to the EUF except for *REGISTER*, and performs the notification of the called-party, according to Annex b. (It can be set to initial-*SUBSCRIBE* outside *INVITE* dialogs, but not to be set to *SUBSCRIBE* requests inside *INVITE* dialogs or re-*SUBSCRIBE* inside existing subscriptions.)

c6: The *P-Charging-Vector*, *P-Charging-Function-Addresses*, and *P-Visited-Network-ID* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: The *P-Preferred-Identity* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) only in the direction of messages from the EUF to the SCF except for *REGISTER*, and transmits the calling-party's information that the EUF requests of notification, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3 and Annex b. (It can be set to initial *SUBSCRIBE*, but not to be set to re-*SUBSCRIBE*.)

c8: The *Privacy* header can be set in requests outside existing dialogs (not to be used inside existing dialogs) except for *REGISTER*, and transmits the presentation/restriction information of the calling-party's information, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3. (It can be set to initial *SUBSCRIBE* outside *INVITE* dialogs, but not to be set to *SUBSCRIBE* requests inside INVITE dialogs or re-*SUBSCRIBE* inside existing subscriptions.)

c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c10: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c11: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c12: The *Referred-By* header may be used as a result of using *REFER* (Appendix Table 1-2, Items 6 to 9). In the case that *REFER* is available over the UNI, the header information may be handled as valid information. It does not guarantee that the *Referred-By* header is used as a result of using *REFER*.

c13: In the case that the pre-existing route function is used over the UNI, the setting of the *Route* header in an initial *SUBSCRIBE* outside *INVITE* dialogs is necessary. (Appendix Table 1-24, Item 1)

c14: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c15: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c16: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Note 2 The *Reason* header is specified in RFC3326, and it is applicable to all the requests inside existing dialogs, *CANCEL*, and all responses, according to the specification. Therefore, it can be used in a *SUBSCRIBE* requests inside *INVITE* dialogs or re-*SUBSCRIBE* inside existing subscriptions, but cannot be used in initial *SUBSCRIBE* outside *INVITE* dialogs.

Note 3 It is used when notification information is present. Formatting and other features depend on *Content-Type*.

vi.12.2. Supported headers in the SUBSCRIBE response

Appendix Table 6-22: Supported headers in the SUBSCRIBE response

Message type: Response

Method: SUBSCRIBE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF sends	SCF sends	
Accept	415	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	o	o	o			
Accept-Language	415	RFC3261	o	o	o			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Allow-Events	489	RFC3265	m	m	m			
Authentication-Info	2xx	RFC3261	o	–	–	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261		–	–	(Note 2)	(Note 2)	
Contact	1xx	RFC3261	o	o	o			
Contact	2xx	RFC3261	m	m	m			
Contact	3xx	RFC3261	m	m	m			(Note 3)
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
Expires	2xx	RFC3261	m	m	m			
From		RFC3261	m	m	m			
Min-Expires	423	RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
Organization		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c3	(Note 1)
P-Asserted-Identity		RFC3325	o	–	–	c4	c4	

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF sends	SCF sends	
P-Charging-Function-Addresses		RFC3455	o	–	–	c5	c5	
P-Charging-Vector		RFC3455	o	–	–	c5	c5	
P-Preferred-Identity		RFC3325	o	–	–	c6	c6	
Privacy		RFC3323	o	–	–	c2	c2	
Proxy-Authenticate	407	RFC3261	m	–	m	c7		
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	2xx 401 484	RFC3261	o	o	o			
Require		RFC3261	o	o	o			
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
RSeq	1xx	RFC3262	o	–	–	(Note 4)	(Note 4)	
Security-Server	421 494	RFC3329	o	–	–	c8	c9 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	o	m	m	(Note 5)	(Note 5)	
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c10	c10	
Message body		RFC3261		o	o	(Note 6)	(Note 6)	

c1: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.
c2: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.
c3: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c4: The *P-Asserted-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.2 of Annex Table a-1 in Annex a.3.
c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.
c6: The *P-Preferred-Identity* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.3 of Annex Table a-1 in Annex a.3.
c7: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *407* response itself is not to be used.
c8: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.
c9: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

<table>
<tr><th rowspan="2">Header</th><th rowspan="2">Appli-cation</th><th rowspan="2">Reference</th><th rowspan="2">RFC status</th><th colspan="2">Status in this standard</th><th colspan="2">Application conditions</th><th rowspan="2">Remarks</th></tr>
<tr><th>EUF Send</th><th>SCF Send</th><th>EUF sends</th><th>SCF sends</th></tr>
<tr><td>c10:</td><td colspan="8">The WWW-Authenticate header is applicable only for the REGISTER request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, 401 response itself is not to be used.</td></tr>
<tr><td>Note 1</td><td colspan="8">Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.</td></tr>
<tr><td>Note 2</td><td colspan="8">Call-Info shows additional information about the sender of the messages. There is no description of the application of the header into SUBSCRIBE in RFCs and other documents. Therefore, it is difficult to define its reaction in the case of using the header in SUBSCRIBE. Furthermore, security risks of Call-Info are noted in RFC3261. An ill-prepared use of the header should be avoided.</td></tr>
<tr><td>Note 3</td><td colspan="8">In the case that the redirection function of the 3xx response is available over the UNI, the header information is handled as valid information, according to clause 10.2.1.8.3 in the main body. (Appendix Table 1-12, Items 1 and 2)</td></tr>
<tr><td>Note 4</td><td colspan="8">The 100rel option (PRACK) is not to be used in SUBSCRIBE.</td></tr>
<tr><td>Note 5</td><td colspan="8">Although specified as "o" in RFC3265, the Unsupported header is set to be "m" based on RFC3261.</td></tr>
<tr><td>Note 6</td><td colspan="8">It is used when notification information is present. Formatting and other features depend on Content-Type.</td></tr>
</table>

vi.13. UPDATE

This message is used for refreshing a call (Session-Timer) and modifying media stream setting information during a call.

vi.13.1. Supported headers in the UPDATE request

Appendix Table 6-23/JT-Q3402: Supported headers in the UPDATE request

Message type: Request

Method: UPDATE

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Accept	RFC3261	o	o	o			
Accept-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Accept-Encoding	RFC3261	o	o	o			
Accept-Language	RFC3261	o	o	o			
Allow	RFC3261	o	o	o			
Authorization	RFC3261	o	–	–	c2	c2	
Call-ID	RFC3261	m	m	m			
Call-Info	RFC3261	o	o	o			(Note 1)
Contact	RFC3261	m	m	m			
Content-Disposition	RFC3261	o	o	o			
Content-Encoding	RFC3261	o	o	o			
Content-Language	RFC3261	o	o	o			
Content-Length	RFC3261	t	t	t			
Content-Type	RFC3261	*	*	*			
CSeq	RFC3261	m	m	m			
Date	RFC3261	o	o	o			(Note 1)
From	RFC3261	m	m	m			
Max-Forwards	RFC3261	m	m	m			
MIME-Version	RFC3261	o	o	o			
Min-SE	RFC4028	o	o	o	c3	c3	
Organization	RFC3261	o	o	o			(Note 1)
P-Access-Network-Info	RFC3455	o	o	–		c4	(Note 1)
P-Charging-Function-Addresses	RFC3455	o	–	–	c5	c5	
P-Charging-Vector	RFC3455	o	–	–	c5	c5	
P-Media-Authorization	RFC3313	o	–	o	c6	c7	
Privacy	RFC3323	o	–	–	c8	c8	
Proxy-Authorization	RFC3261	o	o	–	c9 (when Appendix Table 1-11, Item 2 is stated "Perform HTTP Digest authentication".)	c10	
			–	–	c9 (when Appendix Table 1-11, Item 2 is stated other than "Perform HTTP Digest authentication".)	c10	
Proxy-Require	RFC3261	o	o	–		c11	
Reason	RFC3326	o	o	o			(Note 1)
Record-Route	RFC3261	o	o	o			(Note 1)
Reject-Contact	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Request-Disposition	RFC3841	o	o	o	c1 (Appendix Table 1-7, Item 6)	c1 (Appendix Table 1-7, Item 6)	
Require	RFC3261	c	c	c	c12	c12	
Route	RFC3261	c	c	–		c13	
Security-Client	RFC3329	o	o	–	c14 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c15	
Security-Verify	RFC3329	o	o	–	c14 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	c15	

Header	Reference	RFC status	Status in this standard		Application conditions		Remarks
			EUF Send	SCF Send	EUF Send	SCF Send	
Session-Expires	RFC4028	o	m	m	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	
			o	o	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	
Supported	RFC3261	o	o	o	c12	c12	
Timestamp	RFC3261	o	o	o			(Note 1)
To	RFC3261	m	m	m			
User-Agent	RFC3261	o	o	o			(Note 1)
Via	RFC3261	m	m	m			
Message body	RFC3261	o	o	o			

c1: In the case that the terminal capabilities notification function, Caller Preferences (*pref* tag), is available over the UNI, the header information is handled as valid information. (Appendix Table 1-7, Item 6)

c2: The *Authorization* header is used only when a *REGISTER* request from the SCF to the EUF is authenticated, according to 10.2.1.20.7 of Annex Table a-1 in Annex a.3.

c3: The header must be used as specified in clause 10.2.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary.

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: In the case that SDP offer is performed by *UPDATE*, the header information is handled as valid information. (Appendix Table 1-23, Item 6)

c8: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c9: To be used in the case of performing HTTP Digest authentication to requests outside existing dialogs except for *REGISTER* (Appendix Table 1-11, Item 2)

c10: The *Proxy-Authorization* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.28 in the main body.

c11: The *Proxy-Require* header is not to be used in the direction from the SCF to the EUF, according to 10.2.1.20.29 of Annex Table a-1 in Annex a.3.

c12: "*timer*" needs to be set to the *Require* header and the *Supported* header in terms of the context, according to clause 10.2.1.20.32 and clause 10.2.1.20.37 in the main body. ("*timer*" should be contextually set to the *Supported* header in an *UPDATE* request.)

c13: The *Route* header is not to be used in the direction from the SCF to the EUF, according to clause 10.2.1.20.34 in the main body.

c14: To be handled as valid in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c15: The *Security-Client* and *Security-Verify* headers are not applicable to a request in the direction from the SCF to the EUF, according to 10.1 of Annex Table a-1 in Annex a.3.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

vi.13.2. Supported headers in the UPDATE response

Appendix Table 6-24/JT-Q3402: Supported headers in the UPDATE response

Message type: Response

Method: UPDATE

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
Accept	2xx	RFC3261	o	o	o			
Accept	415	RFC3261	c	c	c			
Accept-Encoding	2xx	RFC3261	o	o	o			
Accept-Encoding	415	RFC3261	c	c	c			
Accept-Language	2xx	RFC3261	o	o	o			
Accept-Language	415	RFC3261	c	c	c			
Allow	2xx	RFC3261	o	o	o			
Allow	405	RFC3261	m	m	m			
Allow	others	RFC3261	o	o	o			
Authentication-Info	2xx	RFC3261	o	–	–	c1	c1	
Call-ID		RFC3261	m	m	m			
Call-Info		RFC3261	o	o	o			(Note 1)
Contact	1xx	RFC3261	o	o	o			
Contact	2xx	RFC3261	m	m	m			
Contact	3xx	RFC3261	o	–	–	c2	c2	
Contact	485	RFC3261	o	o	o			
Content-Disposition		RFC3261	o	o	o			
Content-Encoding		RFC3261	o	o	o			
Content-Language		RFC3261	o	o	o			
Content-Length		RFC3261	t	t	t			
Content-Type		RFC3261	*	*	*			
CSeq		RFC3261	m	m	m			
Date		RFC3261	o	o	o			(Note 1)
Error-Info	300-699	RFC3261	o	o	o			(Note 1)
From		RFC3261	m	m	m			
MIME-Version		RFC3261	o	o	o			
Min-SE	422	RFC4028	m	m	m	c3 (Appendix Table 1-7, Item 1)	c3 (Appendix Table 1-7, Item 1)	
Organization		RFC3261	o	o	o			(Note 1)
P-Access-Network-Info		RFC3455	o	o	–		c4	(Note 1)

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	
P-Charging-Function-Addresses		RFC3455	o	–	–	c5	c5	
P-Charging-Vector		RFC3455	o	–	–	c5	c5	
P-Media-Authorization	2xx	RFC3313	o	–	o	c6	c7	
Privacy		RFC3323	o	–	–	c8	c8	
Proxy-Authenticate	401	RFC3261	o	–	–	c9	c10	
Proxy-Authenticate	407	RFC3261	m	–	m	c9		
Reason		RFC3326	o	o	o			(Note 1)
Record-Route	18x 2xx	RFC3261	o	o	o			(Note 1)
Require		RFC3261	c	c	c	c3	c3	
Retry-After	404 413 480 486	RFC3261	o	o	o			(Note 1)
Retry-After	500 503	RFC3261	o	o	o			(Note 1)
Retry-After	600 603	RFC3261	o	o	o			(Note 1)
Security-Server	421 494	RFC3329	o	–	o	c11	c12 (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)	
Server		RFC3261	o	o	o			(Note 1)
Session-Expires	2xx	RFC4028	o	m	m	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in all sessions".)	
				o	o	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	c3 (when Appendix Table 1-7, Item 1 states that UNI condition are "Used in each session as necessary".)	
Supported	2xx	RFC3261	o	o	o			
Timestamp		RFC3261	o	o	o			(Note 1)
To		RFC3261	m	m	m			
Unsupported	420	RFC3261	m	m	m			
User-Agent		RFC3261	o	o	o			(Note 1)
Via		RFC3261	m	m	m			
Warning		RFC3261	o	o	o			(Note 1)
WWW-Authenticate	401	RFC3261	m	–	–	c13	c13	
WWW-Authenticate	407	RFC3261	o	–	–	c13	c13	
Message body		RFC3261		o	o			

c1: Update of authentication information by the *Authentication-Info* header is not performed because the *Authorization* header is not to be used in the corresponding request.

c2: Redirection using *3xx* responses is not to be used, according to 10.2.1.8.3 of Annex Table a-1 in Annex a.3.

c3: The header must be used as specified in clause 10.2.1.20.32, 10.2.2.1 and 10.2.2.2.7 in the main body. In the case that Session-Timer is used, at least the setting of value to the *Session-Expires* header (*delta-seconds*) is necessary. In the case that the refresher is "*uac*", the setting of "*timer*" to the *Require* header is necessary. (Appendix Table 1-7, Item 1)

Header	Appli-cation	Reference	RFC status	Status in this standard		Application conditions		Remarks
				EUF Send	SCF Send	EUF Send	SCF Send	

c4: The *P-Access-Network-Info* header is applicable to SIP messages only in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c5: The *P-Charging-Vector* and *P-Charging-Function-Addresses* headers are not to be used, according to 10.1 of Annex Table a-1 in Annex a.3.

c6: Not to be used in the direction from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c7: In the case that SDP offer is performed by *UPDATE*, the header information is handled as valid information. (Appendix Table 1-23, Item 6)

c8: The *Privacy* header is applicable only to requests outside existing dialogs except for *REGISTER*, according to 10.2.2.2.4 of Annex Table a-1 in Annex a.3.

c9: The *Proxy-Authenticate* header is not to be used in the direction from the EUF to the SCF, according to clause 10.2.1.20.27 in the main body. In other words, *401*/*407* responses themselves are not to be used.

c10: The *Proxy-Authenticate* header is not to be used in *401* responses, according to 10.2.1.20.27 of Annex Table a-1 in Annex a.3.

c11: The *Security-Server* header is not applicable to the response from the EUF to the SCF, according to 10.1 of Annex Table a-1 in Annex a.3.

c12: To be used in the case that AKA authentication is used or TLS connection of call control signals is used. (Appendix Table 1-11, Items 1 and 2, Appendix Table 1-4, Item 3)

c13: The *WWW-Authenticate* header is applicable only to the *REGISTER* request authentication, according to 10.2.1.20.44 of Annex Table a-1 in Annex a.3. In other words, *401*/*407* responses themselves are not to be used.

Note 1 Whether the SCF behaves as expected or provides the capabilities for the behaviours when the EUF specifies as the header in the SIP message to send is dependent on the policy of the NGN carrier.

Appendix vii. Message examples

(This appendix does not form an integral part of this standard.)

This appendix provides examples of call sequences corresponding to typical call origination and termination in SIP call establishment.

Note that the sequence examples listed here are intended to be a help for system implementation, and behaviors different from sequences listed in this appendix may be needed due to actual service contents and/or terminal functions of each carrier. Note also that the contents of these sequence examples do not guarantee call connectivity or quality.

Appendix Table 7-1/JT-Q3402: List of sequence examples

N	Sequence Name	Corresponding clauses and figures
1	Terminal registration (access-line based authentication)	Appendix vii.1.1
2	Terminal registration (HTTP Digest authentication)	Appendix vii.1.2
3	Deletion of terminal registration (access-line based authentication)	Appendix vii.1.3
4	Call origination to disconnection (IPv4, Use of *timer* and *100rel*, G.711 μ-law)	Appendix vii.1.4
5	Call origination to disconnection (IPv4, Use of *timer* and *100rel*, G.711 μ-law, HTTP Digest authentication)	Appendix vii.1.5
6	Call termination to disconnection (IPv4, Use of *timer* and *100rel*, G.711 μ-law)	Appendix vii.1.6
7	Call cancellation	Appendix vii.1.7
8	Busy on the terminating side	Appendix vii.1.8
9	Hearing the guidance	Appendix vii.1.9
10	Connection after hearing the guidance (using *UPDATE*)	Appendix vii.1.10
11	Sending *MESSAGE* (IPv6)	Appendix vii.1.11
12	Receiving *MESSAGE* (IPv6)	Appendix vii.1.12
13	Subscription to registration event	Appendix vii.1.13
14	Notification of registration event (on deletion of terminal registration)	Appendix vii.1.14

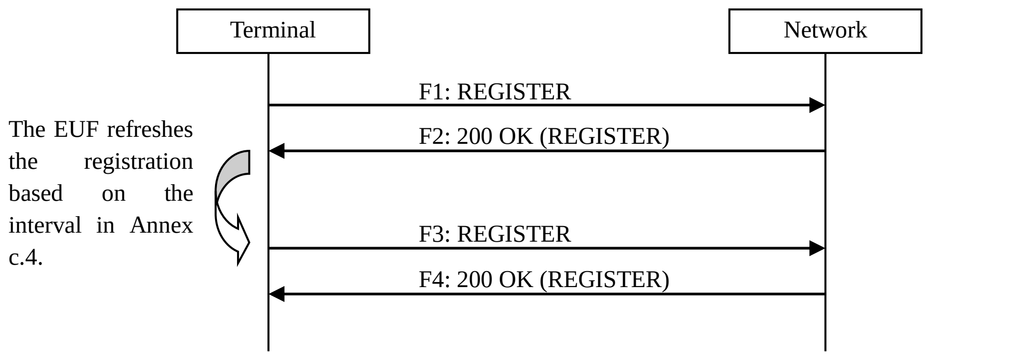
vii.1. Sequence examples

vii.1.1. Terminal registration (access-line based authentication)

This clause shows an example message flow in the case that a network requires a *REGISTER* from a terminal, and access-line based terminal authentication is performed. An IPv4 address and an IPv6 address are used as *Contact address*, and *REGISTER* is performed by IPv4 UDP. The network notifies the pre-existing route by a *Service-Route* header and the available network-asserted user identity by a *P-Associated-URI* header.

In the example of terminal registration such as the one shown below, a SIP-URI composed of a telephone number is used as the URI to be specified in *From* header and *To* header at the time of terminal registration like the example of the caller number shown in clause vii.1.4 etc. Note that there may be a case of using a SIP-URI which is not composed of the telephone number according to the policy of NGN carriers.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP): 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345 IP (SIP): 192.0.1.10, 2001:db8::1



Appendix Figure 7-1/JT-Q3402: Terminal registration (access-line based authentication)

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345
]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
```

```
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:f
e01:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345
]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

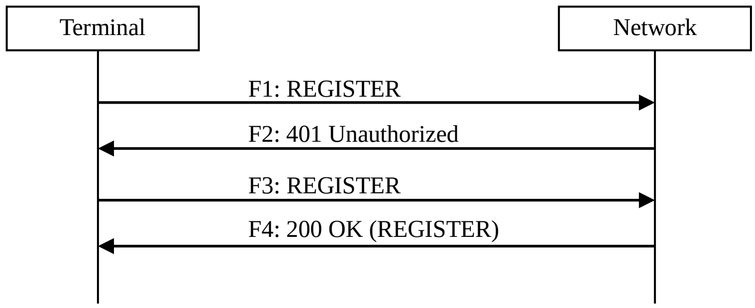
F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:f
e01:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

vii.1.2. Terminal registration (HTTP Digest authentication)

This clause shows an example message flow in the case that the network performs terminal authentication using HTTP Digest authentication, which is different from the sequence in clause vii.1.1.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP): 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345   IP (SIP): 192.0.1.10, 2001:db8::1



Appendix Figure 7-2/JT-Q3402: Terminal registration (HTTP Digest authentication)

F1: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345
]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Content-Length: 0
```

F2: 401 Unauthorized

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111111
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101010
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111111
Call-ID: qwertyuiop11111111@192.0.1.1
CSeq: 1 REGISTER
Supported: path
WWW-Authenticate: Digest realm="example1.ne.jp",nonce="M5vIfYzRWDkD3E-iFxCJBfk8c68JXm5s
",algorithm=MD5
Content-Length: 0
```

F3: REGISTER

```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
```

```
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abce-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>,<sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345
]>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 3600
Supported: path
Authorization: Digest realm="example1.ne.jp",nonce="M5vIfYzRWDkD3E-iFxCJBfk8c68JXm5s",u
ri="sip:example1.ne.jp",username="0311111111",response="70849961c8f5513ca19cbfc44c147c3
5",algorithm=MD5
Content-Length: 0
```

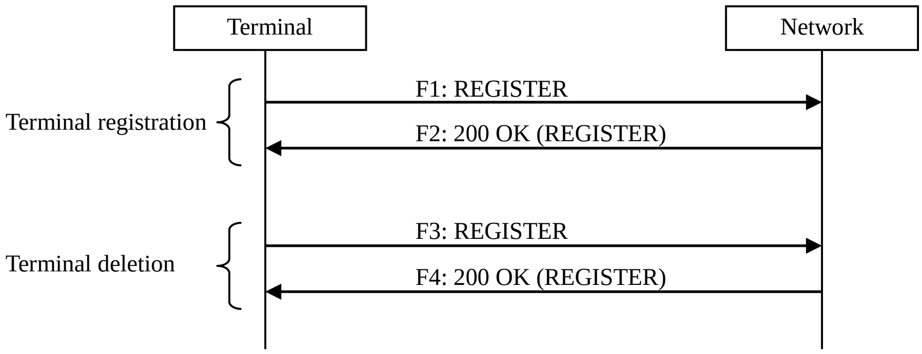
F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxv-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abce-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: <sip:qwertyui@192.0.1.1>;expires=3600,<sip:asdfghjk@[2001:db8:1234:5678:48ff:f
e01:2345]>;expires=3600
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

vii.1.3. Deletion of terminal registration (access-line based authentication)

This clause shows an example message flow in the case that terminal registration is deleted under the same condition of option item selection as clause vii.1.1, assuming that the old registration of the terminal remain in the network when the power of the terminal turns on, and so forth.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP): 192.0.1.1, 2001:db8:1234:5678:acde:48ff:fe01:2345 IP (SIP): 192.0.1.10, 2001:db8::1



Appendix Figure 7-3/JT-Q3402: Deletion of terminal registration (access-line based authentication)

F1 to F2 are omitted because they are the same as those of clause vii.1.1.

F3: REGISTER

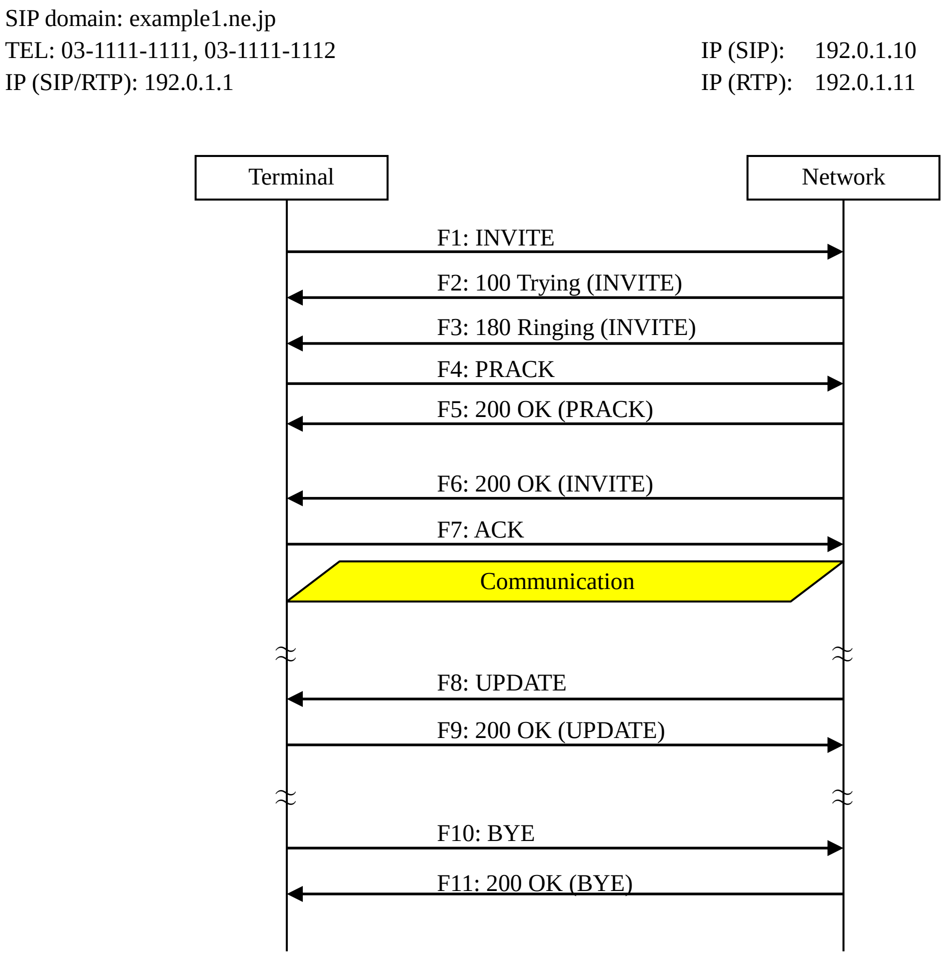
```
REGISTER sip:example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Max-Forwards: 70
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Contact: *
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE,MESSAGE
Expires: 0
Supported: path
Content-Length: 0
```

F4: 200 OK (REGISTER)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111112
Path: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101011
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111112
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 2 REGISTER
Supported: path
Service-Route: <sip:s-cscf.example1.ne.jp;lr>
P-Associated-URI: <sip:0311111111@example1.ne.jp>,<sip:0311111112@example1.ne.jp>
Content-Length: 0
```

vii.1.4. Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ-law)

This clause shows an example message flow of a call connection sequence on the originating side in the case that *timer* and *100rel* are enabled on both originating and terminating sides. IPv4 is used for call control signals and media, UDP is used for call control, and G.711 μ-law is used as audio media. Session refresh is performed by *UPDATE*, and disconnection (by the originating side) is finally performed by *BYE*.



Appendix Figure 7-4/JT-Q3402: Call origination to disconnection

(IPv4, Use of timer and 100rel, G.711 μ-law) (access-line based authentication)

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195
```

```
v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK (PRACK)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 PRACK
Content-Length: 0
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
```

```
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

F11: 200 OK (BYE)

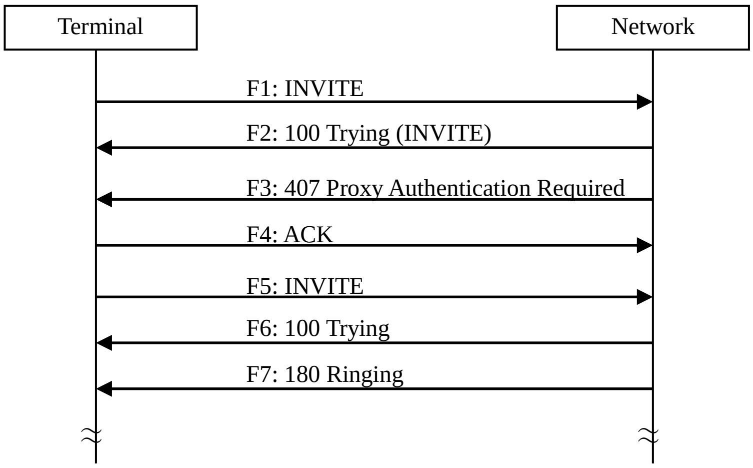
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK5678-11111124
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 3 BYE
Content-Length: 0
```

vii.1.5. Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ-law, HTTP Digest authentication)

This clause shows an example message flow in the case that HTTP Digest authentication is performed to an *INVITE* request, which is different from the sequence in clause vii.1.4.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11



Appendix Figure 7-5/JT-Q3402: Call origination to disconnection (IPv4, Use of timer and 100rel, G.711 μ-law) (HTTP Digest authentication)

F1: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:zxcvbnm@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F3: 407 Proxy Authentication Required

```
SIP/2.0 407 Proxy Authentication Required
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Proxy-Authenticate: Digest realm="example1.ne.jp",nonce="rBqRaPCEcljUN-VQ9wS97fgQHOs9Ig
4k",algorithm=MD5
Content-Length: 0
```

F4: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK2345678-11111121
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

F5: INVITE

```
INVITE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Proxy-Authorization: Digest username="0311111111",realm="example1.ne.jp",nonce="rBqRaPC
EcljUN-VQ9wS97fgQHOs9Ig4k",uri="tel:0322222222;phone-context=example1.ne.jp",response="
0cd3f053fe2295036b73613dce5b2fa3",algorithm=MD5
Contact: <sip:xcvbnmz@192.0.1.1>
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82664419518 82664419518 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
```

```
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F6: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Content-Length: 0
```

F7: 180 Ringing

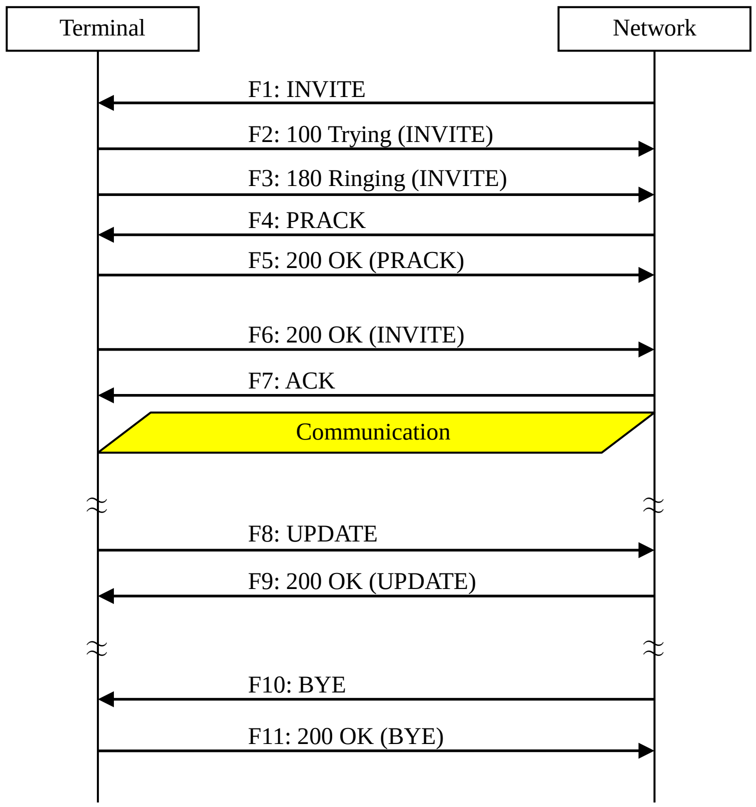
```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111122
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101021
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111122
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 2 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

vii.1.6. Call termination to disconnection (IPv4, Use of timer and 100rel, G.711 μ-law)

This clause shows an example message flow on the terminating side under the same condition of option item selections as clause vii.1.4. After receiving a call from the network, session refresh is performed by *UPDATE*, and disconnection (by the terminating side) is performed by *BYE*. The network notifies the calling-party's identity information by the *P-Asserted-Identity* header, and the called-party's information by the *P-Called-Party-ID* header to the called terminal.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11



Appendix Figure 7-6/JT-Q3402: Call termination to disconnection

(IPv4, Use of timer and 100rel, G.711 μ-law)

F1: INVITE

```
INVITE sip:qwertyui@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:lkjhgfds@192.0.1.10>
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223" <tel:032
2222223;phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
```

```
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: 100rel,timer
Session-Expires: 300
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82664482616 82664482616 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 40000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F2: 100 Trying

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
To: <sip:0311111112@example1.ne.jp>
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Content-Length: 0
```

F3: 180 Ringing

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Length: 0
```

F4: PRACK

```
PRACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
RAck: 1 1 PRACK
Content-Length: 0
```

F5: 200 OK (PRACK)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101021
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
```

```
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 102 PRACK
Content-Length: 0
```

F6: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101020
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101020@192.0.1.10
CSeq: 101 INVITE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Type: application/sdp
Content-Length: 195

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 30000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: ACK

```
ACK sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-10101022
Max-Forwards: 70
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 101 ACK
Content-Length: 0
```

F8: UPDATE

```
UPDATE sip:lkjhgfds@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:asdfghjk@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F9: 200 OK (UPDATE)

```
SIP/2.0 200 OK
```

```
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111125
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 201 UPDATE
Contact: <sip:lkjhgfds@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uac
Content-Length: 0
```

F10: BYE

```
BYE sip:asdfghjk@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
Max-Forwards: 70
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

F11: 200 OK (BYE)

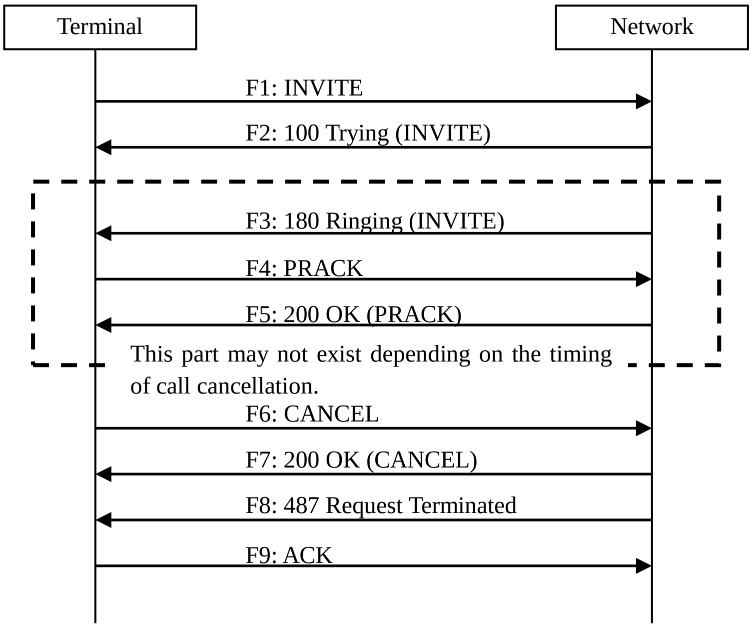
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-11111124
To: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-11111121
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-10101020
Call-ID: poiuytrewq101010@192.0.1.10
CSeq: 103 BYE
Content-Length: 0
```

vii.1.7. Call cancellation (disconnection while ringing)

This clause shows an example message flow for call cancellation by the originating side under the same condition of option item selections as clause vii.1.4.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11



Appendix Figure 7-7/JT-Q3402: Call cancellation (disconnection while ringing)

F1 to F5 are omitted because they are the same as those of clause vii.1.4.

F6: CANCEL

```
CANCEL tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F7: 200 OK (CANCEL)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 CANCEL
Content-Length: 0
```

F8: 487 Request Terminated

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F9: ACK

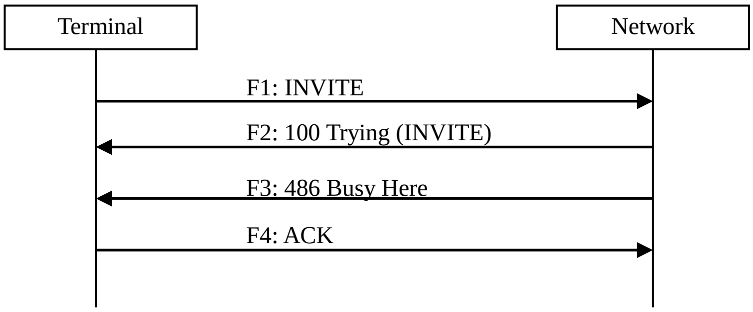
```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.8. Busy on the terminating side

This clause shows an example message flow in the case that the destination is busy (short of empty sessions) under the same condition of option item selections as clause vii.1.4.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11



Appendix Figure 7-8/JT-Q3402: Busy on the terminating side

F1 to F2 are omitted because they are the same as those of clause vii.1.4.

F3: 486 Busy Here

```
SIP/2.0 486 Busy Here
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F4: ACK

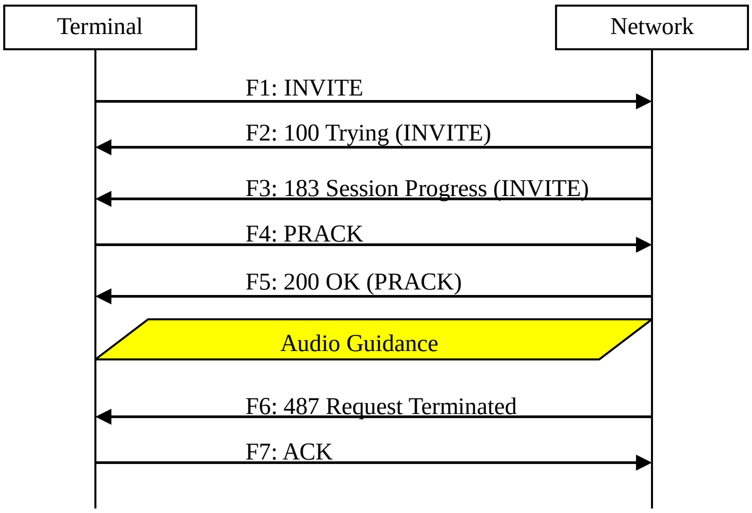
```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.9. Hearing the guidance

This clause shows an example message flow in the case that the call is terminated after audio guidance is provided under the same condition of option item selections as clause vii.1.4.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11



Appendix Figure 7-9/JT-Q3402: Hearing the guidance

F1 to F2 are omitted because they are the same as those of clause vii.1.4.

F3: 183 Session Progress (INVITE)

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: 100rel
RSeq: 1
Content-Type: application/sdp
Content-Length: 197

v=0
o=- 82917391739 82917391739 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.11
t=0 0
m=audio 20000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F4 to F5 are omitted because they are the same as those of clause vii.1.4.

F6: 487 Request Terminated

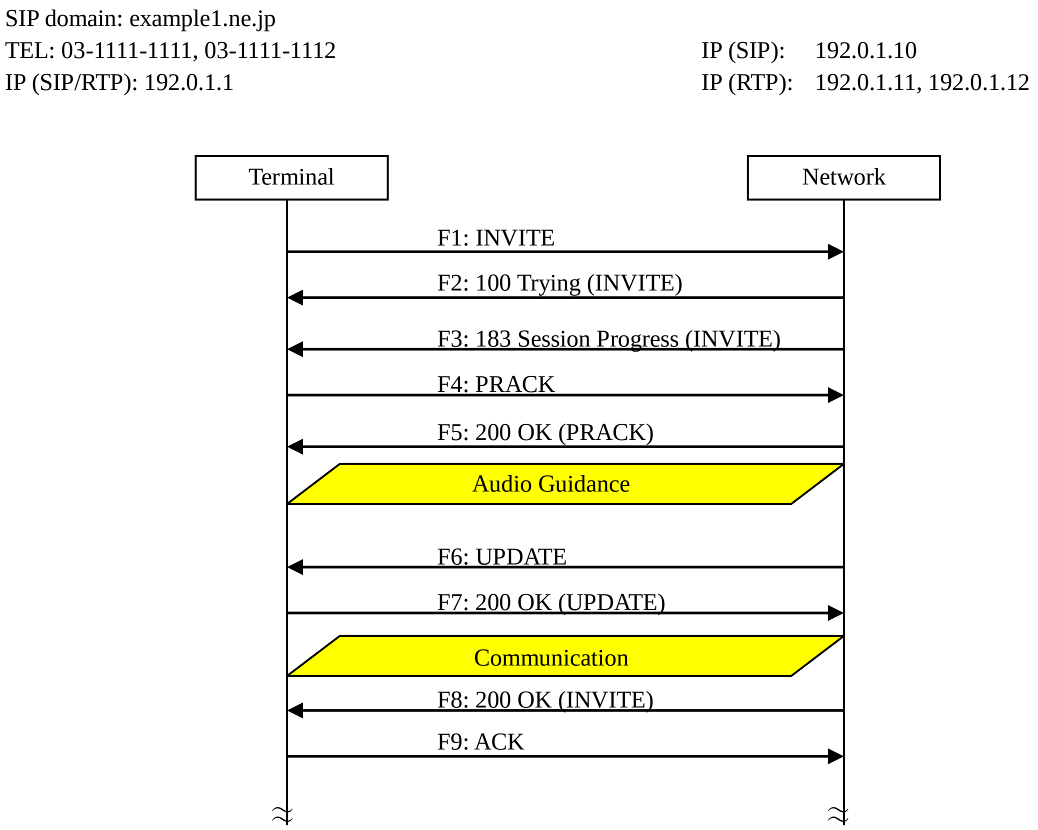
```
SIP/2.0 487 Request Terminated
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 INVITE
Content-Length: 0
```

F7: ACK

```
ACK tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111111@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.10. Connection after hearing the guidance (using UPDATE)

This clause shows an example message flow in the case that a communication takes place by getting connected to the final called-party after the guidance is provided from the network in a sequence same as clause vii.1.9. In switching from the guidance to the final called-party, an *UPDATE* request in the early dialog is used.



Appendix Figure 7-10/JT-Q3402: Connection after hearing the guidance (using UPDATE)

F1 to F5 are omitted because they are the same as those of clause vii.1.9.

F6: UPDATE

```
UPDATE sip:zxcvbnm@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
From: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Supported: timer,100rel
Content-Length: 197

v=0
o=- 82917391739 82917391740 IN IP4 192.0.1.11
s=-
c=IN IP4 192.0.1.12
t=0 0
m=audio 21000 RTP/AVP 0 96
```

```
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F7: 200 OK (UPDATE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK87654321-22222222
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111121
From: <sip:0322222222@example1.ne.jp>;tag=9876zyxw-10101020
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 100 UPDATE
Contact: <sip:zxcvbnm@192.0.1.1>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Content-Length: 195

v=0
o=- 82664419472 82664419472 IN IP4 192.0.1.1
s=-
c=IN IP4 192.0.1.1
t=0 0
m=audio 10000 RTP/AVP 0 96
a=rtpmap:0 PCMU/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
```

F8: 200 OK (INVITE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111121
Record-Route: <sip:192.0.1.10;lr>
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 INVITE
Contact: <sip:mnbvcxz@192.0.1.10>
Allow: INVITE,ACK,BYE,CANCEL,PRACK,UPDATE
Require: timer
Session-Expires: 300;refresher=uas
Content-Length: 0
```

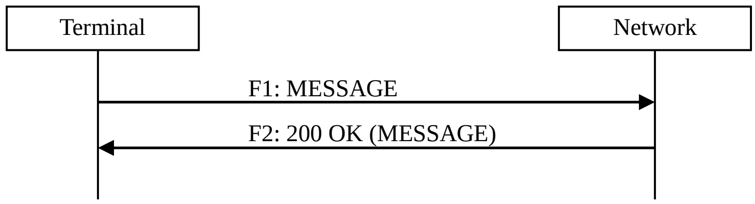
F9: ACK

```
ACK sip:mnbvcxz@192.0.1.10 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111123
Route: <sip:192.0.1.10;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101020
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111121
Call-ID: qwertyuiop111112@192.0.1.1
CSeq: 1 ACK
Content-Length: 0
```

vii.1.11. Sending MESSAGE (using IPv6)

This clause shows an example message flow to send a short text message by using a *MESSAGE* request. SIP messages are sent and received by using IPv6 UDP.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 2001:db8:1234:5678:acde:48ff:fe01:2345 IP (SIP): 2001:db8::1



Appendix Figure 7-11/JT-Q3402: Sending MESSAGE (using IPv6)

F1: MESSAGE

```
MESSAGE tel:0322222222;phone-context=example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:2345]:5060;branch=z9hG4bK12345678-1
1111131
Route: <sip:[2001:db8::1];lr>,<sip:s-cscf.example1.ne.jp;lr>
Max-Forwards: 70
To: <tel:0322222222;phone-context=example1.ne.jp>
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
Call-ID: qwertyuiop111113@[2001:db8:1234:5678:acde:48ff:fe01:2345]
CSeq: 1001 MESSAGE
P-Preferred-Identity: <sip:0311111112@example1.ne.jp>
Privacy: none
Content-Type: text/plain;charset=utf-8
Content-Length: 13

foo bar baz
```

F6: 200 OK (MESSAGE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8:1234:5678:acde:48ff:fe01:2345]:5060;branch=z9hG4bK12345678-1
1111131
To: <tel:0322222222;phone-context=example1.ne.jp>;tag=9876zyxw-10101030
From: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
Call-ID: qwertyuiop111113@[2001:db8:1234:5678:acde:48ff:fe01:2345]
CSeq: 1001 MESSAGE
Content-Length: 0
```

vii.1.12. Receiving MESSAGE (using IPv6)

This clause shows an example message flow to receive a short text message by using a *MESSAGE* request. SIP messages are sent and received by using IPv6 UDP.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 2001:db8:1234:5678:acde:48ff:fe01:2345 IP (SIP): 2001:db8::1

Appendix Figure 7-12/JT-Q3402: Receiving MESSAGE (using IPv6)

F1: MESSAGE

```
MESSAGE sip:asdfghjk@[2001:db8:1234:5678:acde:48ff:fe01:2345] SIP/2.0
Via: SIP/2.0/UDP [2001:db8::1]:5060;branch=z9hG4bK87654321-10101030
Max-Forwards: 64
To: <sip:0311111112@example1.ne.jp>
From: <sip:03122222223@example1.ne.jp>;tag=9876zyxw-10101030
Call-ID: poiuytrewq101030@[2001:db8::1]
CSeq: 2001 MESSAGE
P-Asserted-Identity: "0322222223" <sip:0322222223@example1.ne.jp>,"0322222223" <tel:032
2222223;phone-context=example1.ne.jp>
Privacy: none
P-Called-Party-ID: <sip:0311111112@example1.ne.jp>
Content-Type: text/plain;charset=utf-8
Content-Length: 13

foo bar baz
```

F6: 200 OK (MESSAGE)

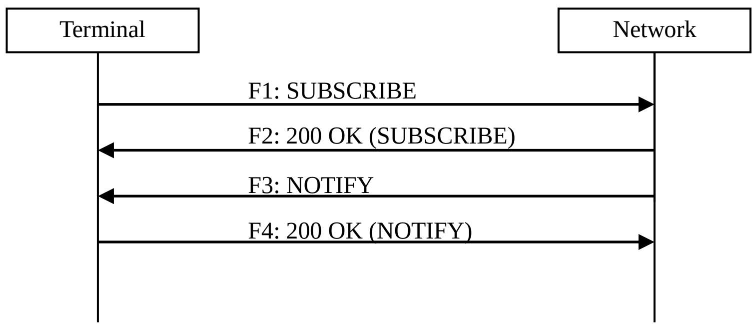
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP [2001:db8::1]:5060;branch=z9hG4bK87654321-10101030
To: <sip:0311111112@example1.ne.jp>;tag=1234abcd-11111131
From: <sip:0322222223@example1.ne.jp>;tag=9876zyxw-10101030
Call-ID: poiuytrewq101030@[2001:db8::1]
CSeq: 2001 MESSAGE
Content-Length: 0
```

vii.1.13. Subscription to registration event

This clause shows an example message flow in the case of subscribing (*SUBSCRIBE*) to registration (reg) event described in Annex c.6.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10
IP (RTP): 192.0.1.11



Appendix Figure 7-13/JT-Q3402: Subscription to registration event

F1: SUBSCRIBE

```
SUBSCRIBE sip:0311111111@example1.ne.jp SIP/2.0
Via: SIP/2.0/UDP 192.0.1.1:5060;branch=z9hG4bK12345678-11111141
Max-Forwards: 70
Route: <sip:192.0.1.10;lr>,<sip:s-cscf.example1.ne.jp>
To: <sip:0311111111@example1.ne.jp>
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 1 SUBSCRIBE
Contact: <sip:wertyuio@192.0.1.1>
P-Preferred-Identity: <sip:0311111111@example1.ne.jp>
Privacy: none
Event: reg
Expires: 3600
Accept: application/reginfo+xml
Content-Length: 0
```

F2: 200 OK (SUBSCRIBE)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.1:5060; branch=z9hG4bK12345678-11111141
Record-Route: <sip:192.0.1.10;lr>
To: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
From: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 1 SUBSCRIBE
Contact: <sip:oiuytrew@192.0.1.10>
Event: reg
Expires: 3600
Content-Length: 0
```

F3: NOTIFY

```
NOTIFY sip:wertyuio@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101040
Max-Forwards: 69
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Contact: <sip:oiuytrew@192.0.1.10>
Subscription-State: active;expires=3600
Event: reg
Expires: 3600
Content-Type: application/reginfo+xml
Content-Length: 741

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
            version="1" state="full">
  <registration aor="sip:0311111111@example1.ne.jp" id="a7" state="active">
    <contact id="76" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="sip:0311111112@example1.ne.jp" id="a8" state="active">
    <contact id="77" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="tel:+81311111111" id="a9" state="active">
    <contact id="78" state="active" event="registered">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
</reginfo>
```

F4: 200 OK (NOTIFY)

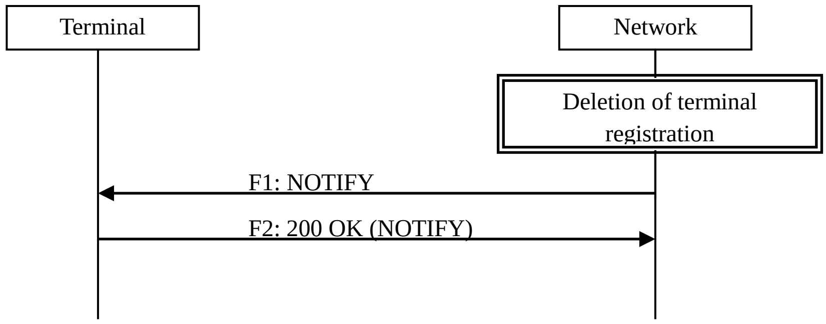
```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101040
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Content-Length: 0
```

vii.1.14. Notification of registration event (on deletion of terminal registration)

This clause shows an example message flow in the case that notification is given to the terminal by a *NOTIFY* request when the terminal registration is deleted by the network. The registration event was subscribed as described in clause vii.1.13 before this sequence.

SIP domain: example1.ne.jp
TEL: 03-1111-1111, 03-1111-1112
IP (SIP/RTP): 192.0.1.1

IP (SIP): 192.0.1.10



Appendix Figure 7-14/JT-Q3402: Notification of registration event

F1: NOTIFY

```
NOTIFY sip:wertyuio@192.0.1.1 SIP/2.0
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101041
Max-Forwards: 69
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Contact: <sip:oiuytrew@192.0.1.10>
Subscription-State: terminated
Event: reg
Expires: 3600
Content-Type: application/reginfo+xml
Content-Length: 758

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
            version="1" state="full">
  <registration aor="sip:0311111111@example1.ne.jp" id="a7" state="active">
    <contact id="76" state="terminated" event="deactivated">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="sip:0311111112@example1.ne.jp" id="a8" state="active">
    <contact id="77" state="terminated" event="deactivated ">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
  <registration aor="tel:+81311111111" id="a9" state="active">
    <contact id="78" state="terminated" event="deactivated ">
      <uri>sip:qwertyui@192.0.1.1</uri>
    </contact>
  </registration>
</reginfo>
```

F2: 200 OK (NOTIFY)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.0.1.10:5060;branch=z9hG4bK12345678-10101041
To: <sip:0311111111@example1.ne.jp>;tag=1234abcd-11111141
From: <sip:0311111111@example1.ne.jp>;tag=9876zyxw-10101040
Call-ID: qwertyuiop111114@192.0.1.1
CSeq: 101 NOTIFY
Content-Length: 0
```