3GPP TS 24.229 V11.6.0 (2012-12)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Core Network and Terminals;
IP multimedia call control protocol based on
Session Initiation Protocol (SIP)
and Session Description Protocol (SDP);
Stage 3
(Release 11)

Modified version for SIP (Gm) interfaces provided by Deutsche Telekom only !

Keywords
UMTS, Network, IP, SIP, SDP, multimedia, LTE

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

The present document is a modified version for the SIP (Gm) interfaces provided by Deutsche Telekom only and has been produced by the department TE3 of Deutsche Telekom Netzproduktion GmbH, Fixed Mobile Engineering Deutschland (in the following named as Deutsche Telekom) and defines the options, deviations and additional requirements for the NGN platform of Deutsche Telekom.

NOTE: Text modified due to Deutsche Telekom requirements that is added or deleted is shown as cursive and underlined (example for added text) or cursive and stricken (~~example for stricken text~~).

1 Scope

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

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);

~~- *the interface between the CSCF and any other CSCF;*~~

~~- *the interface between the CSCF and an Application Server (AS);*~~

~~- *the interface between the CSCF and an ISC gateway function;*~~

~~- *the interface between the ISC gateway function and an Application Server (AS);*~~

~~- *the interface between the CSCF and the Media Gateway Control Function (MGCF);*~~

~~- *the interface between the S-CSCF and the Multimedia Resource Function Controller (MRFC);*~~

~~- *the interface between the Application Server (AS) and the Multimedia Resource Function Controller (MRFC);*~~

~~- *the interface between the S-CSCF and the Media Resource Broker (MRB);*~~

~~- *the interface between the AS and the MRB;*~~

~~- *the interface between the MRB and the MRFC;*~~

~~- *the interface between the CSCF and the Breakout Gateway Control Function (BGCF);*~~

~~- *the interface between the BGCF and the MGCF;*~~

~~- *the interface between the CSCF and an IBCF;*~~

~~- *the interface between the IBCF and AS, MRFC or MRB;*~~

~~- *the interface between the E-CSCF and the Location Retrieval Function (LRF);*~~

~~- *the interface between the BGCF and any other BGCF;*~~

~~- *the interface between the CSCF and an external Multimedia IP network;*~~

~~- *the interface between the E-CSCF and the EATF;*~~

~~- *the interface between the P-CSCF and the ATCF;*~~

~~- *the interface between the ATCF and the I-CSCF;*~~

~~- *the interface between the ATCF and the IBCF; and*~~

~~- *the interface between the transit function and the AS.*~~

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

As the IM CN subsystem is designed to interwork with different IP-Connectivity Access Networks (IP-CANs), the IP-CAN independent aspects of the IM CN subsystem are described in the main body and annex A of this specification. Aspects for connecting a UE to the IM CN subsystem through specific types of IP-CANs are documented separately in the annexes or in separate documents.

The document also specificies HTTP for use by an AS and by an MRB in support of the provision of media resources.

The document also specifies media-related requirements for the NAT traversal mechanisms defined in this specification.

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

2 References

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

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

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

[1A] 3GPP TS 22.101: "Service aspects; Service principles".

[1B] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".

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

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

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

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

[4B] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".

[4C] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".

[4D] 3GPP TS 23.140 Release 6: "Multimedia Messaging Service (MMS); Functional description; Stage 2".

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

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

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

[7A] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[7B] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

[7C] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services; Stage 2".

[7D] 3GPP TS 23.380: "IMS Restoration Procedures".

[7E] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[7F] 3GPP TS 23.334: "IMS Application Level Gateway (IMS-ALG) – IMS Access Gateway (IMS-AGW) interface".

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

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

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

[8C] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3".

[8D] Void.

[8E] 3GPP TS 24.279: "Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services, stage 3, Release 7".

[8F] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[8G] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".

[8H] 3GPP TS 24.173: "IMS Multimedia telephony communication service and supplementary services; Stage 3".

[8I] 3GPP TS 24.606: "Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[8J] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[8K] 3GPP TS 24.323: "3GPP IMS service level tracing management object (MO)".

[8L] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3".

[8M] 3GPP TS 24.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".

[8N] 3GPP TS 24.647: "Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem".

[8O] 3GPP TS 24.292: "IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3".

[8P] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".

[8Q] 3GPP TS 24.182: "IP Multimedia Subsystem (IMS) Customized Alerting Tones (CAT); Protocol specification".

[8R] 3GPP TS 24.183: "IP Multimedia Subsystem (IMS) Customized Ringing Signal (CRS); Protocol specification".

[8S] 3GPP TS 24.616: "Malicious Communication Identification (MCID) using IP Multimedia (IM) Core Network (CN) subsystem".

[8T] 3GPP TS 24.305: "Selective Disabling of 3GPP User Equipment Capabilities (SDoUE) Management Object (MO)".

[8U] 3GPP TS 24.302: "Access to the Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".

[8V] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6".

[8W] 3GPP TS 24.390: "Unstructured Supplementary Service Data (USSD) using IP Multimedia (IM) Core Network (CN) subsystem IMS".

[8X] 3GPP TS 24.139: "3GPP System-Fixed Broadband Access Network Interworking; Stage 3".

[9] 3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

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

[10] Void.

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

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

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

[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".

[11C] 3GPP TS 29.161: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services with Wireless Local Access and Packet Data Networks (PDN)"

[11D] 3GPP TS 29.079: "Optimal Media Routeing within the IP Multimedia Subsystem".

[12] 3GPP TS 29.207 Release 6: "Policy control over Go interface".

[13] Void.

[13A] 3GPP TS 29.209 Release 6: "Policy control over Gq interface".

[13B] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".

[13C] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".

[13D] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

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

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

[15A] 3GPP TS 29.311: "Service Level Interworking for Messaging Services".

[15B] 3GPP TS 31.103: "Characteristics of the IP multimedia services identity module (ISIM) application".

[15C] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".

[15D] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)".

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

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

[17A] 3GPP TS 32.422: "Telecommunication management; Subscriber and equipment trace; Trace control and configuration management".

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

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

[19A] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[19B] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".

[19C] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol".

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

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

[20C] Void.

[20D] Void.

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

[20F] RFC 2132 (March 1997): "DHCP Options and BOOTP Vendor Extensions".

[20G] RFC 2234 (November 1997): "Augmented BNF for Syntax Specification: ABNF".

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

[22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".

[23] RFC 4733 (December 2006): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 6116 (March 2011): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[25] RFC 6086 (October 2009): "Session Initiation Protocol (SIP) INFO Method and Package Framework".

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

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

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

[27A] RFC 3263 (June 2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[27B] RFC 3264 (June 2002): "An Offer/Answer Model with Session Description Protocol (SDP)".

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

[28A] Void.

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

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

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

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

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

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

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

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

[35A] RFC 3361 (August 2002): "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

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

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

[37A] RFC 3605 (October 2003): "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)".

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

[39] RFC 4566 (June 2006): "SDP: Session Description Protocol".

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

[40A] RFC 2131 (March 1997): "Dynamic host configuration protocol".

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

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

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

[44] Void.

[45] Void.

[46] Void.

[47] Void.

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

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

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

[51] Void.

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

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

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

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

[55A] RFC 3551 (July 2003): "RTP Profile for Audio and Video Conferences with Minimal Control".

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

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

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

[56C] RFC 3646 (December 2003): "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

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

[58] RFC 4028 (April 2005): "Session Timers in the Session Initiation Protocol (SIP)".

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

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

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

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

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

[63A] RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".

[64] RFC 4032 (March 2005): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

[65] RFC 3842 (August 2004) "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)"

[65A] RFC 4077 (May 2005): "A Negative Acknowledgement Mechanism for Signaling Compression".

[66] RFC 4244 (November 2005): "An Extension to the Session Initiation Protocol (SIP) for Request History Information".

[67] RFC 5079 (December 2007): "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".

[68] RFC 4458 (January 2006): "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)".

[69] RFC 5031 (January 2008): "A Uniform Resource Name (URN) for Services".

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

[71] Void.

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

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

[74A] RFC 3603 (October 2003): "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture".

[74B] RFC 3959 (December 2004): "The Early Session Disposition Type for the Session Initiation Protocol (SIP)".

[75] RFC 4662 (August 2006): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".

[77] RFC 5875 (May 2010): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".

[78] RFC 4575 (August 2006): "A Session Initiation Protocol (SIP) Event Package for Conference State".

[79] RFC 5049 (December 2007): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

[80] Void.

[81] Void.

[82] RFC 4457 (April 2006): "The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-header)".

[83] RFC 4145 (September 2005): "TCP-Based Media Transport in the Session Description Protocol (SDP)".

[84] RFC 4320 (January 2006): "Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction".

[85] 3GPP2 C.S0005-D (March 2004): "Upper Layer (Layer 3) Signaling Standard for cdma2000 Standards for Spread Spectrum Systems".

[86] 3GPP2 C.S0024-B v3.0 (September 2009): "cdma2000 High Rate Packet Data Air Interface Standard".

[86A] 3GPP2 C.S0084-000 (April 2007): "Overview for Ultra Mobile Broadband (UMB) Air Interface Specification".

[86B] 3GPP2 X.S0060-0 v1.0: "HRPD Support for Emergency Services".

[86C] 3GPP2 X.P0057-C v1.0: "E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects".

Editor's note: The above document cannot be formally referenced until it is published by 3GPP2, at which time it will be designated as X.S0057-C rather than X.P0057-C.

[86D] 3GPP2 C.S0014-C v1.0: "Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems".

[86E] 3GPP2 X.P0059-200-A v1.0: "cdma2000 Femtocell Network: 1x and IMS Network Aspects".

Editor's note: The above document cannot be formally referenced until it is published by 3GPP2, at which time it will be designated as X.S0059-200-A rather than X.P0059-200-A.

[86F] 3GPP2 S.R0048-A v4.0: "3G Mobile Equipment Identifier (MEID) - Stage 1".

[87] ITU-T Recommendation J.112, "Transmission Systems for Interactive Cable Television Services"

[88] PacketCable Release 2 Technical Report, PacketCable™ Architecture Framework Technical Report, PKT-TR-ARCH-FRM.

[89] RFC 6442 (December 2011): "Location Conveyance for the Session Initiation Protocol".

[90] RFC 4119 (December 2005) "A Presence-based GEOPRIV Location Object Format".

[91] RFC 5012 (January 2008): "Requirements for Emergency Context Resolution with Internet Technologies".

[91A] Void.

[92] RFC 5626 (October 2009): "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

[93] RFC 5627 (October 2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".

[94] RFC 5628 (October 2009): "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUUs)".

[95] Void.

[96] RFC 4168 (October 2005): "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)".

[97] RFC 5002 (August 2007): "The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)".

[98] ETSI ES 283 035: "Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".

[99] RFC 5245 (April 2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[100] RFC 5389 (October 2008): "Session Traversal Utilities for NAT (STUN)".

[101] RFC 5766 (April 2010): "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[102] RFC 5768 (April 2010): "Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)".

[103] RFC 4967 (July 2007): "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier".

[104] RFC 5365 (October 2008): "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)".

[105] RFC 5368 (October 2008): "Referring to Multiple Resources in the Session Initiation Protocol (SIP)".

[106] RFC 5366 (October 2008): "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)".

[107] RFC 5367 (October 2008): "Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)".

[108] RFC 4583 (November 2006): "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams".

[109] RFC 5009 (September 2007): "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[110] RFC 4354 (January 2006): "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service".

[111] RFC 4964 (September 2007): "The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular".

[112] RFC 4694 (October 2006): "Number Portability Parameters for the 'tel' URI".

[113] Void.

[114] RFC 4769 (November 2006): "IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information".

[115] RFC 4411 (February 2006): "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events".

[116] RFC 4412 (February 2006): "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[117] RFC 5393 (December 2008): "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies".

[118] RFC 4896 (June 2007): "Signaling Compression (SigComp) Corrections and ClarificationsImplementer's Guide for SigComp".

[119] RFC 5112 (January 2008): "The Presence-Specific Static Dictionary for Signaling Compression (Sigcomp)".

[120] RFC 5688 (January 2010): "A Session Initiation Protocol (SIP) Media Feature Tag for MIME Application Subtype".

[121] RFC 6050 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[122] RFC 4346 (April 2006): "The TLS Protocol Version 1.1".

[123] Void.

[124] RFC 3986 (January 2005): "Uniform Resource Identifiers (URI): Generic Syntax".

[125] RFC 5360 (October 2008): "A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP)".

[126] draft-ietf-cuss-sip-uui-06 (May 2012): "A Mechanism for Transporting User to User Call Control Information in SIPTransporting User to User Information for Call Centers using SIP".

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

[126A] draft-ietf-cuss-sip-uui-isdn-04 (May 2012): "Interworking ISDN Call Control User Information with SIP".

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

[127] 3GPP2 X.S0011-E: "cdma2000 Wireless IP Network Standard ".

[130] RFC 6432 (November 2011): "Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses".

[131] RFC 6544 (March 2012): "TCP Candidates with Interactive Connectivity Establishment (ICE)".

[132] RFC 3023 (January 2001): "XML Media Types".

[133] RFC 5502 (April 2009): "The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem".

[134] draft-vanelburg-sipping-private-network-indication-02 (July 2008): "The Session Initiation Protocol (SIP) P-Private-Network-Indication Private-Header (P-Header)".

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

[135] RFC 4585 (July 2006): "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)".

[136] RFC 5104 (February 2008): "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)".

[137] RFC 5939 (September 2010): "Session Description Protocol (SDP) Capability Negotiation".

[138] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".

[139] Void.

[140] draft-dawes-sipping-debug-02 (February 2010): "Private Extension to the Session Initiation Protocol (SIP) for Debugging".

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

[141] Void.

[142] RFC 6228 (May 2011): "Response Code for Indication of Terminated Dialog".

[143] RFC 6223 (April 2011): "Indication of support for keep-alive".

[144] RFC 4240 (December 2005): "Basic Network Media Services with SIP".

[145] RFC 5552 (May 2009): "SIP Interface to VoiceXML Media Services".

[146] RFC 6230 (May 2011): "Media Control Channel Framework".

[147] RFC 6231 (May 2011): "An Interactive Voice Response (IVR) Control Package for the Media Control Channel Framework".

[148] RFC 6505 (March 2012): "A Mixer Control Package for the Media Control Channel Framework".

[149] RFC 2046 (November 1996): "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".

[150] RFC 5621 (September 2009): "Message Body Handling in the Session Initiation Protocol (SIP)".

[151] RFC 3862 (August 2004): "Common Presence and Instant Messaging (CPIM): Message Format".

[152] RFC 3890 (September 2004): "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)".

[153] draft-montemurro-gsma-imei-urn-11 (October 2012): "A Uniform Resource Name Namespace For The GSM Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".

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

[154] RFC 4122 (July 2005): "A Universally Unique IDentifier (UUID) URN Namespace".

[155] draft-ietf-mmusic-sdp-cs-00 (February 2009): "Session Description Protocol (SDP) Extension For Setting Up Audio Media Streams Over Circuit-Switched Bearers In The Public Switched Telephone Network (PSTN)".

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

[156] draft-garcia-mmusic-sdp-miscellaneous-caps-00 (August 2011): "Miscellaneous Capabilities Negotiation in the Session Description Protocol (SDP)".

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

[157] RFC 5438 (January 2009): "Instant Message Disposition Notification (IMDN)".

[158] RFC 5373 (November 2008): "Requesting Answering Modes for the Session Initiation Protocol (SIP)".

[160] Void.

[161] RFC 4288 (December 2005): "Media Type Specifications and Registration Procedures".

[162] draft-kaplan-dispatch-session-id-00 (December 2009): "A Session Identifier for the Session Initiation Protocol (SIP)".

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

[163] RFC 6026 (September 2010): "Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests".

[164] RFC 5658 (October 2009): "Addressing Record-Route issues in the Session Initiation Protocol (SIP)".

[165] RFC 5954 (August 2010): "Essential Correction for IPv6 ABNF and URI Comparison in RFC3261".

[166] RFC 4117 (June 2005): "Transcoding Services Invocation in the Session Initiation Protocol (SIP) using Third Party Call Control (3pcc)".

[167] RFC 4567 (July 2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".

[168] RFC 4568 (July 2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams".

[169] RFC 3711 (March 2004): "The Secure Real-time Transport Protocol (SRTP)".

[170] RFC 6043 (March 2011): "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)".

[171] RFC 4235 (November 2005): "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)".

[172] draft-ietf-mmusic-sdp-media-capabilities-08 (July 2009): "SDP media capabilities Negotiation".

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

[173] RFC 4488 (May 2006): "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription

[174] Void.

[175] draft-ietf-salud-alert-info-urns-06 (April 2012): "Alert-Info URNs for the Session Initiation Protocol (SIP) ".

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

[176] ANSI/J-STD-036-B: "Enhanced Wireless 9-1-1, Phase 2".

[177] Void.

[178] RFC 4975 (September 2007): "The Message Session Relay Protocol (MSRP)".

[179] RFC 3859 (August 2004): "Common Profile for Presence (CPP)".

[180] RFC 3860 (August 2004): "Common Profile for Instant Messaging (CPIM)".

[181] RFC 2368 (July 1998): "The mailto URL scheme".

[182] RFC 4745 (February 2007): "Common Policy: A Document Format for Expressing Privacy Preferences".

[183] RFC 5318 (December 2008): "The Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header)".

[184] RFC 4538 (June 2006): "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)".

[185] RFC 5547 (May 2009): "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer".

[186] RFC 4483 (May 2006): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages".

[187] draft-atarius-dispatch-meid-urn-01 (August 2011): "A Uniform Resource Name Namespace for the Device Identity and the Mobile Equipment Identity (MEID)".

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

[188] RFC 6679 (August 2012): "Explicit Congestion Notification (ECN) for RTP over UDP".

[189] RFC 3168 (September 2001): "The Addition of Explicit Congestion Notification (ECN) to IP".

[190] draft-ietf-sipcore-proxy-feature-12 (October 2012): "Mechanism to indicate support of features and capabilities in the Session Initiation Protocol (SIP)".

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

[191] RFC 6140 (March 2011): "Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)".

[192] draft-ietf-mediactrl-mrb-13 (July 2012): "Media Resource Brokering".

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

[193] ETSI TS 101 454-1 v1.1.1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 1: Overview and System Level specification".

[194] ETSI EN 301 545-2 v1.1.1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite standard".

[195] ETSI TS 101 545-3 v1.1.1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 3: Higher Layers Satellite ".

[196] RFC 2616 (June 1999): " Hypertext Transfer Protocol -- HTTP/1.1".

[197] draft-polk-local-emergency-rph-namespace-02 (July 2012): "IANA Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications".

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

[198] RFC 6357 (August 2011): "Design Considerations for Session Initiation Protocol (SIP) Overload Control".

[199] draft-ietf-soc-overload-control-09 (July 2012): "Session Initiation Protocol (SIP) Overload Control".

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

[200] draft-ietf-soc-overload-rate-control-02.txt (June 2012): " Session Initiation Protocol (SIP) Rate Control".

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

[201] draft-ietf-soc-load-control-event-package-03 (March 2012): "A Session Initiation Protocol (SIP) Load Control Event Package".

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

[202] ITU-T Recommendation T.38 (September 2010): "Procedures for real-time Group 3 facsimile communication over IP networks".

[203] ISO 8601 (December 2004): "Date elements and interchange formats – Information interchange – Representation of dates and times".

[Ref_dt1] void

[Ref_dt2] draft-ietf-bliss-call-completion: "Call Completion for Session Initiation Protocol (SIP) draft-ietf-bliss-call-completion".

[Ref_dt3] DT 1 TR 114: "Technical Specification of the SIP (Gm) interface between the User Equipment (UE) and the NGN platform of Deutsche Telekom".

[Ref_dt4] DT 1 TR 126: "Technical Specification for SIP User Equipments (UE) providing IMS simulation services via analogue (POTS) interfaces (POTS/SIP interworking) using the NGN platform of Deutsche Telekom".

3 Definitions and abbreviations

3.1 Definitions

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

Entry point:In the case that "border control concepts", as specified in 3GPP TS 23.228 [7], are to be applied in an IM CN subsystem, then these are to be provided by capabilities within the IBCF, and the IBCF acts as an entry point for this network (instead of the I-CSCF). In this case the IBCF and the I-CSCF can be co-located as a single physical node.

If "border control concepts" are not applied, then the I-CSCF is considered as an entry point of a network. If the P-CSCF is in the home network, then the I-CSCF is considered as an entry point for this document. Similary, in case that "border control concepts", as specified in 3GPP TS 23.218 [5], are to be applied in an ISC interface, then these are to be provided by capabilities within the ISC gateway function, and the ISC gateway function acts as an entry point for this network.

Exit point: If operator preference requires the application of "border control concepts" as specified in 3GPP TS 23.228 [7], then these are to be provided by capabilities within the IBCF, and requests sent towards another network are routed via a local network exit point (IBCF), which will then forward the request to the other network (discovering the entry point if necessary). Similary, in case that "border control concepts", as specified in 3GPP TS 23.218 [5], are to be applied in an ISC interface, then these are to be provided by capabilities within the ISC gateway function, and requests sent towards another network are routed via a local network exit point (ISC gateway function).

Geo-local number: Either a geo-local service number as specified in 3GPP TS 23.228 [7] or a number in non-international format according to an addressing plan used at the current physical location of the user.

Home-local number: Either a home local service number as specified in 3GPP TS 23.228 [7] or a number in non-international format according to an addressing plan used in the home network of the user.

Main URI: In the case that the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI is the URI which is used for the registration procedures in the To header of the REGISTER request as specified in RFC 6140 [191]; it represents the public user identities associated to that UE.

Newly established set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200 (OK) response to a REGISTER request was received.

Old set of security associations: Two pairs of IPsec security associations still in existence after another set of security associations has been established due to a successful authentication procedure.

Temporary set of security associations: Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

Integrity protected: See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity-protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirement exists to check that information was received "integrity-protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

Instance ID: An URN generated by the device that uniquely identifies a specific device amongst all other devices, and does not contain any information pertaining to the user (e.g., in GPRS instance ID applies to the Mobile Equipment rather than the UICC). The public user identity together with the instance ID uniquely identifies a specific UA instance. If the device has an IMEI available, it generates an instance ID based on its IMEI as defined in 3GPP TS 23.003 [3] clause 13. If the device has an MEID as defined in 3GPP2 S.R0048-A [86F] available, it generates an instance ID based on its MEID as defined in draft-atarius-device-id-meid-urn [187]. If the device does not have an IMEI available and does not have an MEID available, the instance ID is generated as a string representation of a UUID as a URN as defined in RFC 4122 [154].

Resource reservation: Mechanism for reserving bearer resources that is required for certain access technologies.

Local preconditions: The indication of segmented status preconditions for the local reservation of resources as specified in RFC 3312 [30].

Alias URI, Alias SIP URI: A URI is an alias of another URI if the treatment of both URIs is identical, i.e. both URIs belong to the same set of implicitly registered public user identities, and are linked to the same service profile, and are considered to have the exact same service configuration for each and every service.

NOTE 1: The S-CSCF recognizes that a given URI is an alias of another URI using the grouping sent from the HSS (see 3GPP TS 29.228 [14]).

Globally Routeable SIP URI: a SIP URI of which the hostname part can be resolved to the IP address of the entry entity of the network reponsible for the identity represented by the userpart.

Initial registration: The registration procedure for a public user identity initiated by the UE in the absence of any valid registration.

Registration expiration interval: An indication on how long a registration is valid, indicated using the Expires header field, or the "expires" header field parameter within the Contact header field, according to the procedures specified in RFC 3261 [26].

Re-registration: The registration procedure initiated by the UE to refresh or update an already existing registration for a public user identity.

Registration of an additional public user identity: The registration procedure initiated by the UE to explicitly register an additional public user identity during the life time of the registration of another registered public user identity, where both public user identities have the same contact address and P-CSCF.

Emergency registration: A special registration that relates to binding of a public user identity to a contact address used for emergency service.

Initial emergency registration: An emergency registration that is also an initial registration.

Emergency reregistration: An emergency registration that is also a reregistration.

Back-to-Back User Agent (B2BUA): As given in RFC 3261 [26]. In addition, for the usage in the IM CN subsystem, a SIP element being able to handle a collection of "n" User Agents (behaving each one as UAC and UAS, according to SIP rules), which are linked by some application logic that is fully independent of the SIP rules.

UE private IP address: It is assumed that the NAT device performs network address translation between a private and a public network with the UE located in the private network and the IM CN subsystem in the public network. The UE is assumed to be configured with a private IP address. This address will be denoted as UE private IP address.

UE public IP address: The NAT device is assumed to be configured with one (or perhaps more) public address(es). When the UE sends a request towards the public network, the NAT replaces the source address in the IP header of the packet, which contains the UE private IP address, with a public IP addressed assigned to the NAT. This address will be denoted as UE public IP address.

Encapsulating UDP header: For the purpose of performing UDP encapsulation according to RFC 3948 [63A] each IPsec ESP packet is wrapped into an additional UDP header. This header is denoted as Encapsulating UDP header.

Port_Uenc: In most residential scenarios, when the NAT device performs address translation, it also performs translation of the source port found in the transport layer (TCP/UDP) headers. Following RFC 3948 [63A], the UE will use port 4500 as source port in the encapsulating UDP header when sending a packet. This port is translated by the NAT into an arbitrarily chosen port number which is denoted as port_Uenc.

Multiple registrations: An additional capability of the UE, P-CSCF and S-CSCF, such that the UE (as identified by the private user identity and instance-id), can create multiple simultaneous registration bindings (flows), associated with one or more contact addresses, to any public user identity, Without this capability, a new registration from the UE for a public user identity replaces the existing registration binding, rather than merely creating an additional binding.

IMS flow set: An IMS flow set is a set of flows as defined in RFC 5626 [92]. The flows in an IMS flow set are determined by a combination of transport protocol, IP addresses, and ports. An IMS flow set is established by a successful IMS registration procedure.

NOTE 2: For IPsec, the ports associated with the flow set include protected client ports and protected server ports as defined in 3GPP TS 33.203 [19] and an IMS flow set is made up of the following four flows:

- Flow 1: (IP address UE, port_uc) <--> (IP address P-CSCF, port_ps) over TCP;
- Flow 2: (IP address UE, port_uc) <--> (IP address P-CSCF, port_ps) over UDP;
- Flow 3: (IP address UE, port_us) <--> (IP address P-CSCF, port_pc) over TCP; and
- Flow 4: (IP address UE, port_us) <--> (IP address P-CSCF, port_pc) over UDP.

NOTE 3: For IPsec, according to 3GPP TS 33.203 [19], the P-CSCF can only select among flows 1, 3, or 4 when forwarding requests towards the UE, where flow 1 is only possible in case of TCP connection re-use. According to 3GPP TS 33.203 [19], flow 2 is only used for UE originated requests and corresponding responses. The P-CSCF uses flow 2 to identify the correct IMS flow set.

NOTE 4: An IMS flow set can be considered as a realisation of a logical flow as used in RFC 5626 [92]. But this definition does not depend on any particular definition of a logical flow.

NOTE 5: For TLS, the ports associated with the flow set include a protected client port and a protected server port and an IMS flow set is made up of the following flow:

- (IP address UE, port) <--> (IP address P-CSCF, port) over TCP.

NOTE 6: For SIP digest without TLS, an IMS flow set is as defined in RFC 5626 [92].

IMS flow token: A IMS flow token is uniquely associated with a IMS flow set. When forwarding a request destined towards the UE, the P-CSCF selects the flow from the IMS flow set denoted by the IMS flow token as appropriate according to 3GPP TS 33.203 [19] and RFC 3261 [26].

IP Association: A mapping at the P-CSCF of a UE's packet source IP address, the "sent-by" parameter in the Via header field, and, conditionally, the port with the identities of the UE. This association corresponds to the IP address check table specified in 3GPP TS 33.203 [19].

Authorised Resource-Priority header field: a Resource-Priority header field that is either received from another entity in the trust domain relating to the Resource-Priority header field, or which has been identified as generated by a subscriber known to have such priority privileges for the resource priority namespace and level of priority used within that namespace.

Temporarily authorised Resource-Priority header field: a Resource Priority header field that has been temporarily approved by the P-CSCF, the S-CSCF, or an IBCF. Temporarily authorised Resource-Priority heaer field appears in an INVITE request only, and is applied only in the direction P-CSCF to S-CSCF to AS, S-CSCF to AS, or IBCF to S-CSCF to AS, for the request, and the reverse direction for 1xx responses to that request. Subsequent requests in the same dialog will require an authorised Resource-Priority header field in order to obtain priority privileges. It is only valid when all entities are in the same trust domain for the Resource-Priority header field.

Network-initiated resource reservation: A mechanism of resource reservation where the IP-CAN on the behalf of network initiates the resources to the UE.

Trace depth: When SIP signalling is logged for debugging purposes, trace depth is the level of detail of what is logged.

P-CSCF restoration procedures: the procedures for the IP-CAN and the UE to handle P-CSCF service interruption scenarios (see 3GPP TS 23.380 [7D]).

Public network traffic: traffic sent to the IM CN subsystem for processing according to normal rules of the NGN. This type of traffic is known as public network traffic.

Private network traffic: traffic sent to the IM CN subsystem for processing according to an agreed set of rules specific to an enterprise. This type of traffic is known as private network traffic. Private network traffic is normally within a single enterprise, but private network traffic can also exist between two different enterprises if not precluded for regulatory reasons.

NOTE 7: An IP-PBX or application functionality within the IM CN subsystem can change private network traffic to public network traffic and vice versa, by functionality known as "breakout" or "breakin" to the private network. As such a SIP transaction can be variously private network traffic and public network traffic on different hops across a SIP network.

Priviledged sender: A priviledged sender is allowed to send SIP messages where the identities in P-Asserted-Identity will be passed on in the P-CSCF and are not subject to further processing in the P-CSCF.

S-CSCF restoration procedures: the procedures for the IM CN subsystem and the UE to handle S-CSCF service interruption scenarios (see 3GPP TS 23.380 [7D]).

Loopback routeing: A method of routeing a SIP request back to the visited network for local breakout according to the roaming architecture for voice over IMS with local breakout as specified in 3GPP TS 23.228 [7].

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

Fully-Qualified Domain Name (FQDN)

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

Client
Dialog

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

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

3GPP AAA proxy
3GPP AAA server
Breakout Gateway Control Function (BGCF)
Call Session Control Function (CSCF)
Home Subscriber Server (HSS)
Location Retrieval Function (LRF)
Media Gateway Control Function (MGCF)
MSC Server enhanced for IMS centralized services
Multimedia Resource Function Processor (MRFP)
Packet Data Gateway (PDG)
Subscription Locator Function (SLF)
WLAN UE

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.122 [4C] apply:

Home PLMN (HPLMN)
Visited PLMN (VPLMN)

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclauses 3.1, 8 and 13 apply:

Filter criteria
Initial filter criteria
Initial request
ISC gateway function
Media Resource Broker (MRB)
Multimedia Resource Function Controller (MRFC)
Standalone transaction
Subsequent request

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6, 4.13, 4.15a, 5.2, 5.4.12.1 and 5.10 apply:

Border control concepts
Geo-local service number

Home local service number
Implicit registration set
Interconnection Border Control Function (IBCF)
Interrogating-CSCF (I-CSCF)
IMS Application Level Gateway (IMS-ALG)
IMS application reference
IMS Application Reference Identifier (IARI)
IMS communication service
IMS Communication Service Identifier (ICSI)
Local service number
IP-Connectivity Access Network (IP-CAN)
Policy and Charging Rule Function (PCRF)
Private user identity
Proxy-CSCF (P-CSCF)
Public Service Identity (PSI)
Public user identity
Roaming Architecture for Voice over IMS with Local Breakout
Serving-CSCF (S-CSCF)
Statically pre-configured PSI

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.292 [7C] apply:

ICS UE
SCC AS

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.167 [4B] apply:

Emergency-CSCF (E-CSCF)
Geographical location information
Location identifier
Location information

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

GPRS-IMS-Bundled Authentication (GIBA)
Port_pc
Port_ps
Port_uc
Port_us
Protected server port
Protected client port

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

IMS Credentials (IMC)
International Mobile Equipment Identity (IMEI)
IMS SIM (ISIM)
Serial NumbeR (SNR)
Type Approval Code (TAC)
Universal Integrated Circuit Card (UICC)
Universal Subscriber Identity Module (USIM)
User Equipment (UE)

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

Security association

A number of different security associations exist within the IM CN subsystem and within the underlying access transport. Within this document this term specifically applies to either:

i) the security association that exists between the UE and the P-CSCF. For this usage of the term, the term "security association" only applies to IPsec. This is the only security association that has direct impact on SIP; or

ii) the security association that exists between the WLAN UE and the PDG. This is the security association that is relevant to the discussion of Interworking WLAN as the underlying IP-CAN.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [7A] apply.

Interworking WLAN

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

International public telecommunication number

For the purposes of the present document, the following terms and definitions given in RFC 5012 [91] apply:

Emergency service identifier
Emergency service URN
Public Safety Answering Point (PSAP)
PSAP URI

For the purposes of the present document, the following terms and definitions given in RFC 5627 [93] apply:

Globally Routable User Agent URI (GRUU)

For the purposes of the present document, the following terms and definitions given in RFC 5626 [92] apply:

Flow

For the purposes of the present document, the following terms and definitions given in RFC 4346 [122] appendix B apply:

TLS session

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.292 [8O] apply:

CS media

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [8J] apply:

IMS Voice over PS Session (IMSVoPS) indicator

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.328 [19C] apply:

End-to-access edge security

For the purposes of the present document, the following terms and definitions given in 3GPP2 S.R0048-A v4.0 [86F] apply:

Mobile Equipment Identity (MEID)
Manufacturer code
Serial number

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AAA	Authentication, Authorization and Accounting
APN	Access Point Name
AS	Application Server
ATCF	Access Transfer Control Function
AUTN	Authentication TokeN
AVP	Attribute-Value Pair
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional

BRAS	Broadband Remote Access Server
CCF	Charging Collection Function
CDF	Charging Data Function
CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CPC	Calling Party's Category
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DT	*Deutsche Telekom*
DTD	Document Type Definition
DTMF	Dual Tone Multi Frequency
DVB	Digital Video Broadcast
DVB-RCS2	Second Generation DVB Interactive Satellite System
e2ae-security	End-to-access edge security
EATF	Emergency Access Transfer Function
EC	Emergency Centre
ECF	Event Charging Function
ECI	E-UTRAN Cell Identity
ECN	Explicit Congestion Notification
E-CSCF	Emergency CSCF
EF	Elementary File
EPS	Evolved Packet System
FAP	cdma2000® 1x Femtocell Access Point
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPON	Gigabit-capable Passive Optical Networks
GPRS	General Packet Radio Service
GRUU	Globally Routable User agent URI
GSTN	General Switched Telephone Network
HPLMN	Home PLMN
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
i	irrelevant
IARI	IMS Application Reference Identifier
IBCF	Interconnection Border Control Function
ICE	Interactive Connectivity Establishment
I-CSCF	Interrogating CSCF
ICS	Implementation Conformance Statement
ICID	IM CN subsystem Charging Identifier
ICSI	IMS Communication Service Identifier
ID	Identifier
IK	Integrity Key
IM	IP Multimedia
IMC	IMS Credentials
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia core network Subsystem
IMS-AGW	IMS Access Gateway
IMS-ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identity
IMSVoPS	IMS Voice over PS Session
IOI	Inter Operator Identifier
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP Multimedia Subsystem Service Control
ISIM	IM Subscriber Identity Module

I-WLAN	Interworking – WLAN
IWF	Interworking Function
KMS	Key Management Service
LRF	Location Retrieval Function
m	mandatory
MAC	Message Authentication Code
MCC	Mobile Country Code
MEID	Mobile Equipment IDentity
MGCF	Media Gateway Control Function
MGW	Media Gateway
MNC	Mobile Network Code
MRB	Media Resource Broker
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
MSC	Mobile-services Switching Centre
n/a	not applicable
NAI	Network Access Identifier
NA(P)T	Network Address (and Port) Translation
NASS	Network Attachment Subsystem
NAT	Network Address Translation
NCC	Network Control Center
NCC_ID	Network Control Center Identifier
NP	Number Portability
o	optional
OCF	Online Charging Function
OLI	Originating Line Information
OMR	Optimal Media Routeing
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PDG	Packet Data Gateway
PDN	Packet Data Network
PDP	Packet Data Protocol
PDU	Protocol Data Unit
P-GW	PDN Gateway
PICS	Protocol Implementation Conformance Statement
PIDF-LO	Presence Information Data Format Location Object
PLMN	Public Land Mobile Network
PSAP	Public Safety Answering Point
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
QCI	QoS Class Identifier
QoS	Quality of Service
RAND	RANDom challenge
RCS	Return Channel via Satellite
RCST	Return Channel via Satellite Terminal
RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SCTP	Stream Control Transmission Protocol
SDES	Session Description Protocol Security Descriptions for Media Streams
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SNR	Serial Number
SQN	SeQuence Number
STUN	Session Traversal Utilities for NAT
SVN	Satellite Virtual Network
SVN-MAC	SVN Medium Access Control label
TAC	Type Approval Code
TURN	Traversal Using Relay NAT
TLS	Transport Layer Security

TRF	Transit and Roaming Function
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDVM	Universal Decompressor Virtual Machine
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
USAT	Universal Subscriber Identity Module Application Toolkit
USIM	Universal Subscriber Identity Module
VPLMN	Visited PLMN
WLAN	Wireless Local Area Network
x	prohibited
xDSL	Digital Subscriber Line (all types)
XGPON1	10 Gigabit-capable Passive Optical Networks
XMAC	expected MAC
XML	eXtensible Markup Language

3A Interoperability with different IP-CAN

The IM CN subsystem can be accessed by UEs resident in different types of IP-CAN. The main body of this document, and annex A, are general to UEs and IM CN subsystems that are accessed using any type of IP-CAN. Requirements that are dependent on the type of IP-CAN are covered in annexes B, D, E, H, L, M, O, Q, R and S.

At any given time, for a given SIP transaction or dialog, the UE sees only one type of IP-CAN, as reported to it by the lower layers. The UE follows the procedures of the IP-CAN specific annex related to the last type of IP-CAN reported, even if it is different to one used previously. In particular, handover at the radio layers between two different access technologies can result in such a change while the dialog or transaction proceeds.

At any given time, for a given SIP transaction or dialog, the P-CSCF sees only one type of IP-CAN, as determined by interface to a particular resource architecture, e.g. policy and charging control, and by the access technology reported to it over that interface, or in the absence of this, by preconfiguration in the system. The P-CSCF follows the procedures of the IP-CAN specific annex related to the last type of IP-CAN determined, even if it is different to one used previously. In particular, handover at the radio layers between two different access technologies can result in such a change while the dialog or transaction proceeds.

It is the responsibility of the IP-CAN to ensure that usage of different bearer resources are synchronised on the handover from one IP-CAN to another, e.g. so that a signalling bearer provided by one IP-CAN is a signalling bearer (if provided by that IP-CAN) after handover, and that the appropriate QoS and resource reservation exists after handover. There is no SIP signalling associated with handover at the IP-CAN, and therefore no change in SIP state at one entity is signalled to the peer SIP entity when handover occurs.

In particular the following constraints exist that can have an impact on P-CSCF usage:

1) some IP-CANs can explicitly label a bearer as a signalling bearer, while others provide a bearer that has appropriate QoS, but no explicit labelling. Therefore if handover occurs from an IP-CAN with explicit labelling, to an IP-CAN with no explicit labelling, and then back to an IP-CAN with explicit labelling, the signalling will then be on a bearer that is not explicitly labelled; and

2) some IP-CANs support signalling of grouping of media within particular bearers, while others do not. Therefore if handover occurs from an IP-CAN with grouping, to an IP-CAN with no grouping, and then back to an IP-CAN with grouping, the signalled grouping can have been lost.

When a UE supports multiple IP-CANs, but does not support handover between those IP-CANs, the annex specific to that IP-CAN applies unmodified.

Where handover between IP-CANs occurs without a reregistration in the IM CN subsystem, the same identies and security credentials for access to the IM CN subsystem are used before and after the handover.

At the P-CSCF, the access technology can variously use the PCRF or NASS in support of both signalling and media bearer provision (or indeed use neither). How to determine which applies is up to network dependent rules, but can be specific to the access technology used by each different UE. Not all access technologies are defined for use with NASS, and not all access technologies are defined for use with the PCRF.

4 General

4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols

SIP defines a number of roles which entities can implement in order to support capabilities. These roles are defined in annex A.

Each IM CN subsystem functional entity using an interface at the Gm reference point, the Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Ml reference point, the Mm reference point, the Mr reference point, the Mr' reference point, the Cr reference point, the Mw reference point, the I2 reference point, the I4 reference point and the Ici reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP, as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

Deutsche Telekom Note: This document describes only the role for the Gm interface used by the End devices specified within the scope of 1TR114 [Ref_dt3]

Each IM CN subsystem entity using an interface at the Rc reference point shall implement HTTP as defined in RFC 2616 [196].

The Gm reference point, the Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Ml reference point, the Mm reference point, the Mr reference point, the Mw reference point, the Cr reference point, the I2 reference point, the I4 reference point and the ISC reference point are defined in 3GPP TS 23.002 [2]. The Ici reference point is defined in 3GPP TS 23.228 [7]. The Mr' reference point and the Rc reference point are defined in 3GPP TS 23.218 [5].

For SIP:

- The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access technology specific procedures described in the appropriate access technology specific annex (see subclause 3A and subclause 9.2.2). The UE may include one or several interconnected SIP elements registered as a single logical entity when the UE performs the functions of an external attached network (e.g. an enterprise network). This specification does not place any constraint on the SIP role played by each of the elements as long as the compound entity appears to the IM CM subsystem as a SIP UA with the aforementioned exceptions and additional capabilities except for the modifications defined by the UE performing the functions of an external attached network modifying role in annex A.

NOTE 1: When the UE performs the functions of an external attached network (e.g. an enterprise network), the internal structure of this UE is outside the scope of this specification. It is expected that in the most common case, several SIP elements will be connected to an additional element directly attached to the IM CN subsystem.

- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.2, with the exceptions and additional capabilities to SDP as described in subclause 6.2, and with the exceptions and additional capabilities to SigComp as described in subclause 8.2. Under certain circumstances, if the P-CSCF provides an application level gateway functionality (IMS-ALG), the P-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) when acting as a subscriber to or the recipient of event information (see subclause 5.2);

  b) when performing P-CSCF initiated dialog-release, even when acting as a proxy for the remainder of the dialog (see subclause 5.2);

c) when performing NAT traversal procedures (see annex F, annex G and annex K); and

d) when performing media plane security procedures (see subclause 5.2).

The P-CSCF shall also provide the access technology specific procedures described in the appropriate access technology specific annex (see subclause 3A and subclause 9.2.2).

- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.

- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4, and with the exceptions and additional capabilities to SDP as described in subclause 6.3. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;

  b) as the notifier of event information the S-CSCF shall provide the UA role;

  c) when providing a messaging mechanism by sending the MESSAGE method, the S-CSCF shall provide the UA role; and

  d) when performing S-CSCF initiated dialog release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.4.

- The BGCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.6.

- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.

- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.6. An AS performing media control of an MRFC shall also support the procedures and methods described in subclause 10.2.

NOTE 2: Subclause 5.7 and its subclauses define only the requirements on the AS that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

- The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.

- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8, and with the exceptions and additional capabilities to SDP as described in subclause 6.5. The MRFC shall also support the procedures and methods described in subclause 10.3 for media control.

- In inline aware mode, the MRB shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8A. In inline unaware mode, the MRB shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.8A. The MRB shall also support the procedures and methods described in subclause 10.4 for media control.

- The IBCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.10. If the IBCF provides an application level gateway functionality (IMS-ALG), then the IBCF shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.10, and

with the exceptions and additional capabilities to SDP as described in subclause 6.7. If the IBCF provides screening functionality, then the IBCF may provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.10.

- The E-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.11. Under certain circumstances as described in subclause 5.11, the E-CSCF shall provide the UA role in accordance with RFC 3323 [33], with the additional capabilities, as follows:

  a) when operator policy (e.g. determined by national regulatory requirements applicable to emergency services) allows user requests for suppression of public user identifiers and location information, then the E-CSCF shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.11;

  b) when performing E-CSCF initiated dialog release the E-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog, e.g. for any of the reasons specified in RFC 6442 [89] or RFC 3323 [33];

  c) when acting as a notifier for the dialog event package the E-CSCF shall provide the UA role; and

  d) if operator policy allows any LRF to provide a location by value using the mechanism defined in subclause 5.11.3. the E-CSCF shall provide the UA role.

- The LRF shall provide the UA role.

- The ISC gateway function shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.13. If the ISC gateway function provides an application level gateway functionality (IMS-ALG), then the ISC gateway function shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.13, and with the exceptions and additional capabilities to SDP as described in subclause 6.7.

- The MSC Server enhanced for ICS shall provide the UA role, with the exceptions and additional capabilities as described in 3GPP TS 24.292 [8O].

- The EATF shall provide the UA role, with the exceptions and additional capabilities as described in 3GPP TS 24.237 [8M].

- The ATCF shall:

  a) provide the proxy role, with the exceptions and additional capabilities as described in 3GPP TS 24.237 [8M]; and

  b) provide the UA role, with the exceptions and additional capabilities as described in 3GPP TS 24.237 [8M].

In addition to the roles specified above, the P-CSCF, the I-CSCF, the IBCF, the S-CSCF, the BGCF, the E-CSCF and the ISC gateway function can act as a UA when providing server functionality to return a final response for any of the reasons specified in RFC 3261 [26].

In addition to the roles specified above the S-CSCF, AS and an entity hosting the additional routeing capabilities as specified in subclause I.3 can act as a UA when providing either client or server functionality when the event package associated with overload control is deployed.

NOTE 3: Annex A can change the status of requirements in referenced specifications. Particular attention is drawn to table A.4 and table A.162 for capabilities within referenced SIP specifications, and to table A.317 and table A.328 for capabilities within referenced SDP specifications. The remaining tables build on these initial tables.

NOTE 4: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. In all other respects other than those more completely described in subclause 5.2 the P-CSCF implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

NOTE 5: Except as specified in clause 5 or otherwise permitted in RFC 3261, the functional entities providing the proxy role are intended to be transparent to data within received requests and responses. Therefore these entities do not modify message bodies. If local policy applies to restrict such data being passed on, the functional entity has to assume the UA role and reject a request, or if in a response and where such procedures apply, to pass the response on and then clear the session using the BYE method.

All the above entities are functional entities that could be implemented in a number of different physical platforms coexisting with a number of other functional entities. The implementation shall give priority to transactions at one functional entity, e.g. that of the E-CSCF, over non-emergency transactions at other entities on the same physical implementation. Such priority is similar to the priority within the functional entities themselves specified elsewhere in this document.

Additional routeing functionality can be provided to support the ability for the IM CN subsystem to provide transit functionality as specified in Annex I. The additional routeing functionality shall assume the proxy role.

4.2 URI and address assignments

In order for SIP and SDP to operate, the following prerequisite conditions apply:

1) I-CSCFs used in registration are allocated SIP URIs. Other IM CN subsystem entities may be allocated SIP URIs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URI may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URIs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IP addresses. Any IM CN subsystem entities can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. For systems providing access to IM CN subsystem using a GPRS IP-CAN or an EPS IP-CAN this is specified in 3GPP TS 23.221 [6] subclause 5.1. For systems providing access to IM CN subsystem using a cdma2000® packet data subsystem IP-CAN this is specified in subclause M.2.2.1.

3) The subscriber is allocated a private user identity by the home network operator. This private user identity is available to the SIP application within the UE. Depending on the network operator, various arrangements exist within the UE for retaining this information:

   a) where an ISIM is present, within the ISIM, see subclause 5.1.1.1A;

   b) where no ISIM is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A);

   c) neither ISIM nor USIM is present, but IMC is present, within IMC (see subclause 5.1.1.1B.1);

   d) when neither ISIM nor USIM nor IMC is present, the private user identity is available to the UE via other means (see subclause 5.1.1.1B.2).

NOTE 1: 3GPP TS 33.203 [19] specifies that a UE attached to a 3GPP network has an ISIM or a USIM.

NOTE 2: The SIP URIs can be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. The public user identity shall take the form of SIP URI as specified in RFC 3261 [26] or tel URI as specified in RFC 3966 [22]. At least one of the public user identities is a SIP URI . All registered public user identities are available to the SIP application within the UE, after registration. Depending on the network operator, various arrangements exist within the UE for retaining this information:

   a) where an ISIM is present, at least one public user identity, which is a SIP URI, within the ISIM, see subclause 5.1.1.1A;

   b) where no ISIM is present but USIM is present, a temporary public user identity is derived (see subclause 5.1.1.1A);

   c) neither ISIM nor USIM is present, but IMC is present, within IMC (see subclause 5.1.1.1B.1);

d) when neither ISIM nor USIM nor IMC is present, the public user identities are available to the UE via other means (see subclause 5.1.1.1B.2).

NOTE 3: 3GPP TS 33.203 [19] specifies that a UE attached to a 3GPP network has an ISIM or a USIM.

5) If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, then it shall have an Instance ID, in conformance with the mandatory requirements for Instance IDs specified in RFC 5627 [93] and RFC 5626 [92].

6) For each tel URI, there is at least one alias SIP URI in the set of implicitly registered public user identities that is used to implicitly register the associated tel URI.

NOTE 4: For each tel URI, there always exists a SIP URI that has identical user part as the tel URI and the "user" SIP URI parameter equals "phone" (see RFC 3261 [26] subclause 19.1.6), that represents the same public user identity. If a tel URI identifies a subscriber served by the IM CN subsystem, then the hostport parameter of the respective SIP URI contains the home domain name of the IM CN subsystem to which the subscriber belongs.

6A) Identification of the UE to a PSAP with point of presence in the CS domain is not possible if a tel URI is not included in the set of implicitly registered public user identities. If the included tel URI is associated either with the first entry in the list of public user identities provisioned in the UE or with the temporary public user identity, then a PSAP can uniquely identify the UE if emergency registration is performed.

NOTE 5: The tel URI uniquely identifies the UE by not sharing any of the implicit registered public user identities in the implicit registration set that contains this tel URI.

NOTE 6: Emergency registration is not always needed or supported.

7) The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities and different contact addresses. When reregistering and deregistering a given public user identity and associated contact address, the UE will use the same private user identity that it had used during the initial registration of the respective public user identity and associated contact address. If the tel URI is a shared public user identity, then the associated alias SIP URI is also a shared public user identity. Likewise, if the alias SIP URI is a shared public user identity, then the associated tel URI is also a shared public user identity.

8) For the purpose of access to the IM CN subsystem, UEs can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. For systems providing access to IM CN subsystem using a UMTS/GSM network this is specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures). For systems providing access to IM CN subsystem using a cdma2000® network this is specified in subclause M.2.2.1.

9) For the purpose of indicating an IMS communication service to the network, UEs are assigned ICSI values appropriate to the IMS communication services supported by the UE, coded as URNs as specified in subclause 7.2A.8.2.

NOTE 7: cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA).

10) E-CSCFs are allocated multiple SIP URIs. The SIP URI configured in the P-CSCF, AS or IBCF to reach the E-CSCF is distinct from the one given by the E-CSCF to the EATF such that EATF can reach the E-CSCF.

11) If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the subscriber is allocated one or usually more public user identities by the home network operator. The public user identity(s) shall be allocated as global numbers in the international format.

4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

NOTE: Support of SCTP as specified in RFC 4168 [96] is optional for IM CN subsystem entities implementing the role of a UA or proxy. SCTP transport between the UE and P-CSCF is not supported in the present document. Support of the SCTP transport is currently not described in 3GPP TS 33.203 [19].

For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.

The UE and the P-CSCF shall send and receive request and responses other than initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

In case of an emergency session if the UE does not have sufficient credentials to authenticate with the IM CN subsystem and regulations allow, the UE and P-CSCF shall send request and responses other than initial REGISTER requests on non protected ports.

4.2B Security mechanisms

4.2B.1 Signalling security (3GPP TS 24.229 Release 12)

3GPP TS 33.203 [19] defines the security features and mechanisms for secure access to the IM CN subsystem. This document defines a number of access security mechanisms, as summarised in table 4-1.

Table 4-1: Summary of access security mechanisms to the IM CN subsystem

Mechanism	Authentication	Integrity protection	Use of security agreement in accordance with RFC 3329 [48]	Support (as defined in 3GPP TS 33.203 [19])
~~IMS AKA plus IPsec ESP (see 3GPP TS 33.203 [19] clause 6)~~	~~IMS AKA~~	~~IPsec ESP~~	~~Yes~~	~~Mandatory for all UEs containing a UICC, else optional. Mandatory for all P-CSCF, I-CSCF, S-CSCF~~
SIP digest plus check of IP association (see 3GPP TS 33.203 [19] annex N) (note 2)	SIP digest	None (note 3)	No	Optional for UEs Optional for P-CSCF, I-CSCF, S-CSCF
SIP digest plus Proxy Authentication (see 3GPP TS 33.203 [19] annex N) (note 2)	SIP digest	None (note 3)	No	Optional for UEs Optional for P-CSCF, I-CSCF, S-CSCF
SIP digest with TLS (see 3GPP TS 33.203 [19] annex N and annex O)	SIP digest	TLS session	Yes	Optional for UEs Optional for P-CSCF, I-CSCF, S-CSCF
NASS-IMS bundled authentication (see 3GPP TS 33.203 [19] annex R) (notes 4, 5)	not applicable (note 1)	None (note 3)	No	No UE support required Optional for P-CSCF, I-CSCF, S-CSCF
~~GPRS-IMS-Bundled authentication (see 3GPP TS 33.203 [19] annex S) (note 5)~~	~~not applicable (note 1)~~	~~None (note 3)~~	~~No~~	~~Optional for UEs Optional for P-CSCF, I-CSCF, S-CSCF~~
~~Trusted node authentication (see 3GPP TS 33.203 [19] annex U)~~	~~not applicable (note 6)~~	~~None (note 3)~~	~~No~~	~~No UE support required Optional for I-CSCF, S-CSCF~~

NOTE 1: Authentication is not provided as part of the IM CN subsystem signalling.
NOTE 2: The term "SIP digest without TLS" is used in this specification to refer to both "SIP digest plus check of IP association" and "SIP digest plus Proxy Authentication".
NOTE 3: This security mechanism does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.
NOTE 4: A P-Access-Network-Info aware P-CSCF is required in order to provide NASS-IMS bundled authentication.
NOTE 5: The P-CSCF is restricted to the home network when performing this security mechanism.
NOTE 6: Trusted node authentication. For example the MSC server enhanced for IMS centralized services has authenticated the UE and as a consequence S-CSCF will skip authentication.

Specification of the mechanisms identified within table 4-1 within this document are provided in clause 5. Subclauses where security procedures are required consist of a general subclause applicable whichever security mechanisms are in use, and a separate subclause for each security mechanism identified by a row within table 4-1.

TLS is optional to implement and is used only in combination with SIP digest authentication. Authentication associated with registration to the IM CN subsystem is applicable to IMS AKA and SIP digest and is covered in subclause 5.1.1 for the UE, subclause 5.2.2 for the P-CSCF and subclause 5.4.1 for the S-CSCF. Additionally, SIP digest allows for authentication to also occur on an initial request for a dialog or a request for a standalone transaction, this additional capability is covered in subclause 5.1.2A and subclause 5.4.3.2.

If a UE that implements SIP digest is configured not to use TLS, then the UE does not establish a TLS session toward the P-CSCF. If a UE supports TLS, then the UE supports TLS as described in 3GPP TS 33.203 [19].

For SIP digest authentication, the P-CSCF can be configured to have TLS required or disabled:

- if TLS is required, the P-CSCF requires the establishment of a TLS session from all SIP digest UEs, in order to access IMS subsequent to registration; or

- if TLS is disabled, the P-CSCF does not allow the establishment of a TLS session from any UE.

NOTE: The mechanism to configure the P-CSCF to have TLS required or disabled is outside the scope of this specification.

SIP digest cannot be used in conjunction with the procedures of Annex F.

For emergency calls, 3GPP TS 33.203 [19] specifies some relaxations, which are further described in the subclauses of this document relating to emergency calls.

3GPP TS 33.210 [19A] defines the security architecture for network domain IP based control planes.
3GPP TS 33.210 [19A] applies for security mechanisms between entities in the IM CN subsystem.

4.2B.2 Media security (3GPP TS 24.229 Release 12)

MSRP using TLS, BFCP using TLS, UDPTL using DTLS are not part of this document. These features are marked as brown and NOT underlined text may be implemented as an option. Such features if implemented must be configurable and are deactivated per default. Such features (MSRP using TLS, BFCP using TLS, UDPTL using DTLS) are NOT supported by the Deutsche Telekom network.

3GPP TS 33.328 [19C] defines mechanisms for support of security on the media plane.

This document defines the required elements for signalling the support of media security.

The media security mechanisms are summarised as shown in table 4-2.

Table 4-2: Summary of media security mechanisms to the IM CN subsystem

Mechanism	Applicable to media	Support required by UE	Support required by IM CN subsystem entities	Network support outside IM CN subsystem entities
End-to-access-edge media security using SDES. ***Mandatory to be supported.***	RTP based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37. (NOTE)	Not applicable.
End-to-access-edge media security for MSRP using TLS and certificate fingerprints. ***not supported by the Deutsche Telekom network***	MSRP based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/40, A.317/40A, A.317/51 and A.317/37A.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/40, A.317/40A, A.317/51 and A.317/37A. (NOTE)	Not applicable.
End-to-access-edge media security for BFCP using TLS and certificate fingerprints. ***not supported by the Deutsche Telekom network***	BFCP based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/28, A.317/51 and A.317/37B.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/28, A.317/51 and A.317/37B. (NOTE)	Not applicable.
End-to-access-edge media security for UDPTL using DTLS and certificate fingerprints. ***not supported by the Deutsche Telekom network***	UDPTL based media only.	Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/52, A.317/51 and A.317/37C.	P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/52, A.317/51 and A.317/37C. (NOTE)	Not applicable.
End-to-end media security using SDES. ***not supported by the Deutsche Telekom network***	RTP based media only.	Support SDP extensions specified in table A.317, items A.317/34 and A.317/36.	Not applicable.	Not applicable.
End-to-end media security using KMS. ***not supported by the Deutsche Telekom network***	RTP based media only.	Support SDP extensions specified in table A.317, items A.317/34 and A.317/35.	Not applicable.	GBA and KMS support required.
End-to-end media security for MSRP using TLS and KMS.	MSRP based media only.	Support SDP extensions specified in table A.317, items	Not applicable.	GBA and KMS support required.

not supported by the Deutsche Telekom network		A.317/40, A.317/40A and A.317/35, and support RFC 4279 [218].		
NOTE: Support of end-to-access-edge media security is determined entirely by the network operator of the P-CSCF, which need not be the same network operator as that of the S-CSCF.				

For RTP media security, the UE supports the SDES key management protocol and optionally the KMS key management protocol as defined in 3GPP TS 33.328 [19C] and SRTP as defined in RFC 3711 [169] for secure transport of media.

For end-to-access-edge media security for MSRP using TLS and certificate fingerprints, the UE supports MSRP over TLS as defined in RFC 4975 [178] and RFC 6714 [214] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for BFCP using TLS and certificate fingerprints, the UE supports BFCP over TLS as defined in RFC 4583 [108] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, the UE supports UDPTL over DTLS as defined in RFC 7345 [217] with certificate fingerprints as defined in 3GPP TS 33.328 [19C].

For end-to-end media security for MSRP using TLS and KMS, the UE supports MSRP over TLS as defined in RFC 4975 [178] and RFC 6714 [214] with pre-shared key ciphersuites as defined in RFC 4279 [218] and the KMS key management protocol as defined in 3GPP TS 33.328 [19C]. The certificate fingerprints are not indicated.

There is no support for media security in the MGCF, because there would be no end-to-end media security support on calls interworked with the CS domain and the CS user. In this release of this document, there is no support for media security in the MRF. End-to-access-edge media security is not impacted by this absence of support.

For emergency calls, it is not expected that PSAPs would support end-to-end media security and therefore the procedures of this document do not allow the UE to establish such sessions with end-to-end media security. End-to-access-edge media security is not impacted and can be used on emergency calls.

When the UE performs the functions of an external attached network (e.g. an enterprise network):

- where end-to-access-edge media security is used, the UE functionality is expected to be in the gateway of the external attached network, and support for further media security is outside the scope of this document; and

- where end-to-end media security is used, the UE functionality is expected to be supported by the endpoints in the attached network.

4.3 Routeing principles of IM CN subsystem entities

Each IM CN subsystem functional entity shall apply loose routeing policy as described in RFC 3261 [26], when processing a SIP request. In cases where the I-CSCF, IBCF, S-CSCF and the E-CSCF may interact with strict routers in non IM CN subsystem networks, the I-CSCF, IBCF, S-CSCF and E-CSCF shall use the routeing procedures defined in RFC 3261 [26] to ensure interoperability with strict routers.

4.4 Trust domain

4.4.1 General

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the functional entities that belong to the same operator's network (P-CSCF, the E-CSCF, the I-CSCF, the IBCF, the S-CSCF, the BGCF. the MGCF, the MRFC, the MRB, the EATF, the ATCF, the ISC gateway function, and all ASs that are included in the trust domain). Additionally, other nodes within the IM CN subsystem that are not part of the same operator's domain may or may not be part of the trust domain, depending on whether an interconnect agreement exists with the remote network. SIP functional entities that belong to a network for which there is an interconnect agreement are part of the trust domain. ASs outside the operator's network can also belong to the trust domain if they have a trusted relationship with the home network.

NOTE 1: Whether any peer functional entity is regarded as part of the same operator's domain, and therefore part of the same trust domain, is dependent on operator policy which is preconfigured into each functional entity.

NOTE 2: For the purpose of this document, the PSAP is typically regarded as being within the trust domain, except where indicated. National regulator policy applicable to emergency services determines the trust domain applicable to certain header fields. This means that e.g. the handling of the P-Access-Network-Info header field, P-Asserted-Identity header field and the History-Info header field can be as if the PSAP is within the trust domain, and trust domain issues will be resolved accordingly.

Within the IM CN subsystem trust domains will be applied to a number of header fields. These trust domains do not necessarily contain the same functional entities or cover the same operator domains. The procedures in this subclause apply to the functional entities in clause 5 in the case where a trust domain boundary exists at that functional entity.

Where the IM CN subsystem supports business communication, different trust domains can apply to public network traffic, and to private network traffic belonging to each supported corporate network.

NOTE 3: Where an external attached network (e.g. an enterprise network) is in use, the edges of the trust domains need not necessarily lie at the P-CSCF. In this release of the specification, the means by which the P-CSCF learns of such attached devices, and therefore different trust domain requirements to apply, is not provided in the specification and is assumed to be by configuration or by a mechanism outside the scope of this release of the specification.

A trust domain applies for the purpose of the following header fields: P-Asserted-Identity, P-Access-Network-Info, History-Info, Resource-Priority, P-Asserted-Service, Reason (only in a response), P-Profile-Key, P-Private-Network-Indication, P-Served-User, P-Early-Media and Feature-Caps. A trust domain applies for the purpose of the CPC and OLI tel URI parameters. The trust domains of these header fields and parameters need not have the same boundaries. Clause 5 defines additional procedures concerning these header fields.

4.4.2 P-Asserted-Identity

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Asserted-Identity header field according to RFC 3325 [34] when SIP signalling crosses the boundary of the trust domain. The priv-value "id" shall not be removed from the Privacy header field when SIP signalling crosses the boundary of the trust domain. Subclause 5.4 identifies additional cases for the removal of the P-Asserted-Identity header field.

4.4.3 P-Access-Network-Info

A functional entity at the boundary of the trust domain shall remove any P-Access-Network-Info header field.

4.4.4 History-Info

A functional entity at the boundary of the trust domain will need to determine whether to remove the History-Info header field according to RFC 4244 [66] subclause 3.3 when SIP signalling crosses the boundary of the trust domain. Subclause 5.4 identifies additional cases for the removal of the History-Info header field.

4.4.5 P-Asserted-Service

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Asserted-Service header field according to RFC 6050 [121] when SIP signalling crosses the boundary of the trust domain.

4.4.6 Resource-Priority

A functional entity shall only include a Resource-Priority header field in a request or response forwarded to another entity within the trust domain. If a request or response is forwarded to an entity outside the trust domain, the functional entity shall remove the Resource-Priority header field from the forwarded request or response. If a request or response is received from an untrusted entity (with the exception requests or responses received by the P-CSCF from the UE for which procedures are defined in subclause 5.2) that contains the Resource-Priority header field, the functional entity shall remove the Resource-Priority header field before forwarding the request or response within the trust domain.

NOTE: Alternate treatments can be applied when a non-trusted Resource-Priority header field is received over the boundary of trust domain. The exact treatment (e.g. removal, modification, or passing of the Resource-Priority header field) is left to national regulation and network configuration.

4.4.7 Reason (in a response)

A functional entity shall only include a Reason header field in a response forwarded to another entity within the trust domain (as specified in RFC 6432 [130]). If a response is forwarded to an entity outside the trust domain, the functional entity shall remove the Reason header field from the forwarded response.

NOTE: A Reason header field can be received in a response from outside the trust domain and will not be removed.

4.4.8 P-Profile-Key

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Profile-Key header field as defined in RFC 5002 [97] when SIP signalling crosses the boundary of the trust domain.

4.4.9 P-Served-User

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Served-User header field according to RFC 5502 [133] when SIP signalling crosses the boundary of the trust domain.

4.4.10 P-Private-Network-Indication

A functional entity shall only include a P-Private-Network-Indication header field in a request or response forwarded to another entity within the trust domain. If a request or response is forwarded to an entity outside the trust domain, the functional entity shall remove the P-Private-Network-Indication header field from the forwarded request or response. If a request or response is received from an untrusted entity that contains the P-Private-Network-Indication header field, the functional entity shall remove the P-Private-Network-Indication header field before forwarding the request or response within the trust domain.

NOTE 1: Other entities within the enterprise will frequently be part of this trust domain.

NOTE 2: The presence of the P-Private-Network-Indication header field is an indication that the request constitutes private network traffic. This can modify the trust domain behaviour for other header fields.

NOTE 3: If a trust domain boundary is encountered for this header field without appropriate business communication processing, then this can be an indication that misconfiguration has occurred in the IM CN subsystem. Removal of this header field changes the request from private network traffic to public network traffic.

4.4.11 P-Early-Media

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Early-Media header field as defined in RFC 5009 [109] when SIP signalling crosses the boundary of the trust domain.

Deutsche Telekom: The P-Early-Media Header is forwarded to the UE and will be forwarded to the P-CSCF when sent by the UE.

4.4.12 CPC and OLI

Entities in the IM CN subsystem shall restrict "cpc" and "oli" URI parameters to specific domains that are trusted and support the "cpc" and "oli" URI parameters. Therefore for the purpose of the "cpc" and "oli" URI parameters within this specification, a trust domain also applies.

SIP functional entities within the trust domain shall remove the "cpc" and "oli" URI parameters when the SIP signalling crosses the boundary of the trust domain.

4.4.13 Feature-Caps

A functional entity at the boundary of the trust domain shall remove all Feature-Caps header fields received from UEs and external networks outside the trust domain.

NOTE: A UE that is a priviledged sender is considered as part of the trust domain.

4.5 Charging correlation principles for IM CN subsystems

4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in clause 5. See 3GPP TS 32.240 [16] and 3GPP TS 32.260 [17] for further information on charging.

The IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IM CN subsystem Charging Identifier (ICID);
2. Access network charging information;
3. Inter Operator Identifier (IOI);
4. Charging function addresses:
   a. Charging Data Function (CDF);
   b. Online Charging Function (OCF).

How to use and where to generate the parameters in IM CN subsystems are described further in the subclauses that follow. The charging correlation information is encoded in the P-Charging-Vector header field as defined in subclause 7.2A.5. The P-Charging-Vector header field contains the following header field parameters: "icid-value", "related-icid", "access-network-charging-info", "orig-ioi" "term-ioi" and "transit-ioi".

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in RFC 3455 [52]. The P-Charging-Function-Addresses header field contains the following header field parameters: "ccf" for CDF and "ecf" for OCF.

NOTE: P-Charging-Function-Addresses parameters were defined using previous terminology.

4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems. The ICID is used also for session unrelated messages (e.g. SUBSCRIBE request, NOTIFY request, MESSAGE request) for the correlation with CDRs generated among the IM CN subsystem entities.

The first IM CN subsystem entity involved in a SIP transaction will generate the ICID and include it in the "icid-value" header field parameter of the P-Charging-Vector header field in the SIP request. For a dialog relating to a session, this will be performed only on the INVITE request, for all other transactions, it will occur on each SIP request. See 3GPP TS 32.260 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for UE-originated calls. The I-CSCF will generate an ICID for UE-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. The MSC server will generate an ICID for ICS and SRVCC originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for UE-terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header field. The valid duration of the ICID is specified in 3GPP TS 32.260 [17].

The "icid-value" header field parameter is included in any request that includes the P-Charging-Vector header field. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF to the IP-CAN via PCRF. The interface supporting this operation is outside the scope of this document.

4.5.2A Related ICID

During the process of SRVCC access transfer the MSC server or the P-CSCF generates an ICID for the target access leg. For the purpose of charging correlation between the source access leg and the target access leg when the user is roaming the SCC AS and the ATCF includes the ICID used on the source access leg in the "related-icid" header field parameter of the P-Charging-Vector header field returned in 1xx and 2xx responses to the initial INVITE request.

Delete Section 4.5.3 Access network charging information (not relevant for a 1TR114 UE therefore deleted)

Delete Section 4.5.4 Inter operator identifier (IOI) (not relevant for a 1TR114 UE therefore deleted)

Delete Section 4.5.4A Transit inter operator identifier (Transit IOI) (not relevant for a 1TR114 UE therefore deleted)

Delete Section 4.5.5 Charging function addresses (not relevant for a 1TR114 UE therefore deleted)

4.6 Support of local service numbers

For the IM CN subsystem, the support of local service numbers is provided by an AS in the subscriber's home network as described in subclause 5.7.1.7.

4.7 Emergency service

Delete Sectione 4.7.1 Introduction (not relevant for a 1TR114 UE therefore deleted)

4.7.2 Emergency calls generated by a UE

All phone numbers beginning with "11" (short codes, e.g. 112 or 110 or 11833; see also national number plan of Germany) shall not be manipulated by any UE; these numbers shall be sent out without neither any Country Code (CC) nor any National Destination Code (NDC).

All further requirements and procedures with regard to emergency services are describe within the main document 1TR114.

~~*If the UE cannot detect the emergency call attempt, the UE initiates the request as per normal procedures as described in subclause 5.1.2A. Depending on network policies, for a non-roaming UE or for a roaming UE where the P-CSCF is in the same network where the UE is roaming an emergency call attempt can succeed even if the UE did not detect that an emergency session is being requested, otherwise the network rejects the request indicating to the UE that the attempt was for an emergency service.*~~

~~*The UE procedures for UE detectable emergency calls are defined in subclause 5.1.6.*~~

~~*The P-CSCF, S-CSCF, and E-CSCF procedures for emergency service are described in subclause 5.2.10, 5.4.8 and 5.11, respectively.*~~

~~*Access dependent aspects of emergency service (e.g. emergency registration support and location provision) are defined in the access technology specific annexes for each access technology.*~~

~~*There are a number of variants within these procedures and which variant gets used depends on a number of issues. These conditions are defined more specifically in 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex, but are summarised as follows:*~~

~~*a) if the UE knows that it is in its own home network, then an existing registration is permitted to be used for signalling the emergency call, except where item c) applies. The access technology specific annexes define the mechanism by which home network determination is made;*~~

~~*b) if emergency calls are permitted without security credentials (or additionally where the authentication is not possible or has failed), then the emergency call is made directly without use of any security association created by a registration, and therefore without the registration; and*~~

~~*c) where the access technology defines emergency bearers for the support of emergency calls, a new emergency registration is required so that these emergency bearers can be used for both signalling and media, unless an existing emergency registration exists on those emergency bearers.*~~

Delete Sectione 4.7.3 Emergency calls generated by an AS (not relevant for a 1TR114 UE therefore deleted)

Delete Sectione 4.7.4 Emergency calls received from an enterprise network (not relevant for a 1TR114 UE therefore deleted)

Delete Sectione 4.7.5 Location in emergency calls (not relevant for a 1TR114 UE therefore deleted)

4.8 Tracing of signalling

4.8.1 General

IM CN subsystem entities can log SIP signalling, for debugging or tracing purposes, as described in 3GPP TS 32.422 [17A]. Debugging of SIP signalling is configured from the debug-event package, specified in draft-dawes-sipping-debug [140], hosted on the S-CSCF. This event package provides a source of configuration data available to any SIP entity, including entities that are not in the Service-Route: header field, and entities in a visited network.

4.8.2 Trace depth

The depth parameter in trace control and configuration indicates which SIP requests and responses are logged. If the trace depth is "maximum" then all requests and responses within a dialog or standalone transaction are logged. If the trace depth is "minimum" then all requests and responses except for non-reliable 1xx responses (including 100 (Trying) responses) and the ACK request are logged.

Delete Sectione 4.9 Overlap signalling (not relevant for a 1TR114 UE therefore deleted)

4.10 Dialog correlation for IM CN subsystems

4.10.1 General

The Call-ID header field in combination with the tags in the From header field and in the To header field is the standard mechanism to identify SIP messages which belong to the same dialog. However the Call-ID header field is often changed by B2BUAs and other SIP intermediaries in the end-to-end message path.

To solve this problem, a Session-ID header field containing a globally unique session identifier, as defined in draft-kaplan-dispatch-session-id [162], can be used to correlate SIP messages belonging to the same session. In the case of a concatenation of dialogs, the dialog correlation mechanism indicates that these dialogs belong to the same session.

The usage of the Session-ID header field is specified in annex A.

Deutsche Telekom Extension: The setup of a Session-Id by a UE is mandatory.

4.10.2 CONF usage

In case of the activation of a 3PTY conference, in the INVITE request to the CONF AS the Session-ID header field is added to the URIs in the URI list, in order to indicate the dialogs which are to be included to the 3PTY conference at the CONF AS, as described in 3GPP TS 24.147 [8B].

Delete Section 4.11 Priority mechanisms (not relevant for a 1TR114 UE therefore deleted)

Delete Section 4.12 Overload control (not relevant for a 1TR114 UE therefore deleted)

5 Application usage of SIP

5.1 Procedures at the UE

5.1.0 General

The UE procedures for UE detectable emergency calls are defined in subclause 5.1.6. Exceptions to UE procedures for SIP that do not relate to emergency, are documented in subclause 5.1.6 and shall apply. These exceptions include handling of a response to a request not detected by the UE as relating to an emergency.

5.1.1 Registration and authentication

5.1.1.1 General

The UE shall register public user identities (see table A.4/1 and dependencies on that major capability).

NOTE 1: The UE can use multiple Contact header field values simultaneously containing the same IP address and port number in the contact address.

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

The UE can register any one of its public user identities with any IP address acquired by the UE. The same public user identity can be bound to more than one IP address of the UE. While having valid registrations of previously registered public user identities, the UE can register any additional public user identity with any of its IP addresses. When binding

any one of its public user identities to an additional contact address, the UE shall follow the procedures described in RFC 5626 [92].

If SIP digest without TLS is used, the UE shall not include signalling plane security mechanisms in the header fields defined in RFC 3329 [48] in any SIP messages.

NOTE 2: The UE determines if SIP digest is used with or without TLS based on device configuration. If SIP digest with TLS is used, then the UE includes the TLS signalling plane security mechanism in the header fields defined in RFC 3329 [48] as described in subclause 5.1.1.2.4.

SIP requests that indicate security mechanisms for both the signalling plane and the media plane can contain multiple instances or a single instance of the Security-Client, Security-Verify, or Security-Server header fields defined in RFC 3329 [48].

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT, the UE may need to modify the SIP contents according to the procedures described in either annex F or annex K.

NOTE 3: If UE populates the display-name of the Contact header field included in the REGISTER request with UE name, other UEs of the user can discover the UE name of the UE in the reg event package notification. The UE name is a text string chosen by the user allowing the user to distinguish individual UEs of the same user.

Delete Section 5.1.1.1A Parameters contained in the ISIM (not relevant for a 1TR114 UE therefore deleted)

5.1.1.1B Parameters provisioned to a UE without ISIM or USIM

5.1.1.1B.1 Parameters provisioned in the IMC

In case the UE contains neither an ISIM nor a USIM, but IMC is present the UE shall use preconfigured parameters in the IMC to initiate the registration to the IM CN subsystem and for authentication.

The following IMS parameters are assumed to be available to the UE:

- a private user identity;
- a public user identity; and
- a home network domain name to address the SIP REGISTER request to.

These parameters may not necessarily reside in a UICC.

The first public user identity in the list stored in the IMC is used in emergency registration requests.

5.1.1.1B.2 Parameters when UE does not contain ISIM, USIM or IMC

If the UE contains neither ISIM, nor USIM nor IMC, the UE shall generate a temporary public user identity, a private user identity and a home network domain name to address the SIP REGISTER request to, according 3GPP TS 23.003 [3].

5.1.1.2 Initial registration

5.1.1.2.1 General

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626 [92]. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626 [92], then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and

- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261 [26].

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require to use negotiated ports for exchanging protected messages.

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

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be registered;

b) a To header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:

   1) supports GRUU (see table A.4, item A.4/53);

   2) supports multiple registrations;

   3) has an IMEI available; or

   4) has an MEID available;

   the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 6: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 7: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 8: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 9: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration, find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and

- if the UE used the procedures specified in RFC 6140 [191] for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie"header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 10: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquenly identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 11: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about thederegistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626 [92];

g) store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a session level, or on a media level when it initiates new media in an existing session; and

NOTE 12: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223 [143].

On receiving a 305 (Use Proxy) response to the unprotected REGISTER request, unless otherwise specified in access specific annexes (as described in Annex B or Annex L), the UE shall:

a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 13: The 305 response is not expected to contain a Contact header field.

b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;

d) select a P-CSCF address, which is different from the previously used address, from the address list; and

e) perform the procedures for initial registration as described in subclause 5.1.1.2.

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

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

~~*On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) or 600 (Busy Everywhere) response for an initial registration, the UE may attempt to perform initial registration again.*~~

~~*When the timer F expires at the UE, the UE may:*~~

~~*a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;*~~

~~*b) if no response has been received when attempting to contact all P-CSCFs known by the UE, get a new set of P-CSCF addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in Annex B or Annex L); and*~~

~~*c) perform the procedures for initial registration as described in subclause 5.1.1.2.*~~

~~*NOTE 14: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.*~~

~~*After a first unsuccessful initial registration attempt, if the Retry-After header field was not present and the initial registration was not performed as a consequence of a failed reregistration, the UE shall not wait more than 5 minutes before attempting a new registration.*~~

After a maximum of 2 consecutive unsuccessful initial registration attempts, the UE shall implement the mechanism defined in subclause 4.5 of RFC 5626 [92] for new registration attemps. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in in subclause 4.5 of RFC 5626 [92] shall be used.

The values of max-time and base-time may be provided by the network to the UE using OMA-DM with the management objects specified in 3GPP TS 24.167 [8G]. Other mechanisms may be used as well and are outside the scope of the present specification.

Delete Section 5.1.1.2.2 Initial registration using IMS AKA (not relevant for a 1TR114 UE therefore deleted)

5.1.1.2.3 Initial registration using SIP digest without TLS

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 [21] unless otherwise specified in the access specific annexes, with:

- the "username" header field parameter, set to the value of the private user identity;
- the "realm" header field parameter, set to the domain name of the home network;
- the "uri" header field directive, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to an empty value; and
- the "response" header field parameter, set to an empty value;

Note: For Re-Register and all other requests the NONCE value, if valid, shall be set to avoid challenge of each request.

b) the hostport parameter in the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and

c) the sent-by field in the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

The UE shall use the locally available public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration. The method whereby the public user identity and private user identity are made available to the UE is outside the scope of this document (e.g. a public user identity could be input by the end user).

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.4.

5.1.1.2.4 Initial registration using SIP digest with TLS *(only optional; currently not used within the NGN platform of Deutsche Telekom)*

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field set in accordance with subclause 5.1.1.2.3 unless otherwise specified in the access specific annexes; and

b) a Security-Client header field set to specify the signalling plane security mechanism the UE supports. The UE shall support the setup of a TLS session as defined in 3GPP TS 33.203 [19]. The UE shall support the "tls" security mechanism, as specified in RFC 3329 [48]. The UE shall support TLS for integrity and confidentiality protection as defined in RFC 3261 [26], and shall announce support for them according to the procedures defined in RFC 3329 [48].

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

a) set the TLS session lifetime to the longest of either the previously existing TLS session lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

If a UE supports TLS, then the UE shall support TLS ciphersuites as described in 3GPP TS 33.203 [19]. TLS session lifetime is determined by local configuration of the UE.

For SIP digest with TLS, the UE associates a protected server port with the TLS session port on the UE.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.6.

5.1.1.2.5 Initial registration using NASS-IMS bundled authentication

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) optionally, an Authorization header field, with the "username" header field parameter, set to the value of the private user identity;

NOTE 1: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When NASS-IMS bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

Delete Section 5.1.1.2.6 Initial registration using GPRS-IMS-Bundled authentication (not relevant for a 1TR114 UE therefore deleted)

5.1.1.3 Subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

NOTE 1: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the subscription will be directed to the main URI, as described in RFC 6140 [191].

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package.

NOTE 2: The subscription information stored in the HSS ensures that the default public user identity is a SIP URI.

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

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to the SIP URI that is the default public user identity used for subscription;

b) a From header field set to the SIP URI that is the default public user identity used for subscription;

c) a To header field set to the SIP URI that is the default public user identity used for subscription;

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

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void.

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

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the UE shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to RFC 3265 [28].

Otherwise, the UE shall consider the subscription invalid and start a new initial subscription according to RFC 3265 [28].

5.1.1.3A Subscription to the debug event package

Upon receipt of a 2xx response to a registration that contains an empty P-Debug-ID header field, the UE shall subscribe to the debug event package for the public user identity registered at the user's registrar (S-CSCF) as described in draft-dawes-sipping-debug [140].

The UE shall use the default public user identity for subscription to the debug event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the debug event package, if the public user identity that was used for initial registration is not barred.

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

a) an Event header set to the "debug" event package.

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

5.1.1.4 User-initiated reregistration and registration of an additional public user identity

5.1.1.4.1 General

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used).

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities either:

- over the existing set of security associations or TLS sessions, if appropriate to the security mechanism in use, that is associated with the related contact address; or

- via an initial registration as specified in subclause 5.1.1.2.

The UE can fetch bindings as defined in RFC 3261 [26] at any time after the initial registration has been completed. The procedure for fetching bindings is the same as for a reregistration except that the REGISTER request does not contain a Contact header field.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62] or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated either with the contact address or to the registration flow and the associated contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

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

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be registered;

b) a To header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE:

   1) supports GRUU (see table A.4, item A.4/53);

   2) supports multiple registrations;

   3) has an IMEI available; or

   4) has an MEID available.

   Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 1: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

   If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

   if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in RFC 6223 [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and:

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 3: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value either to the contact address or to the registration flow and the associated contact address used in this registration;

NOTE 4: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

b) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 5: The stored list of service route values will be used to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used).

NOTE 6: If the list of Service-Route headers saved from a previous registration and bound either to this contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 7: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and

- if the UE used the procedures specified in RFC 6140 [191]for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie"header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 8: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquenly identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field and labelled with the "mediasec" header field parameter specified in subclause 7.2A.7, if any. Once the UE chooses a media security mechanism from the list received in the

Security-Server header field from the server, it may initiate that mechanism on a session level, or on a media level when it initiates new media in an existing session; and

NOTE 9: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in RFC 6223 [143], towards the P-CSCF.

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

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

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

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) response for a reregistration, the UE shall perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 305 (Use Proxy) response to the REGISTER request, unless otherwise specified in the access specific annexes (as described in Annex B or Annex L), the UE shall:

a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 4: The 305 response is not expected to contain a Contact header field.

b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if theUE was pre-configured with more than one P-CSCF's IP addresses or domain names;

d) select a P-CSCF address, which is different from the previously used address, from the address list; and

e) perform the procedures for initial registration as described in subclause 5.1.1.2.

When the timer F expires at the UE:

1) the UE shall stop processing of all ongoing dialogs and transactions associated with that flow, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs); and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2:

   a) the UE may select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in Annex B or Annex L);

   c) the UE may perform the procedures for initial registration as described in subclause 5.1.1.2; and

   d) the UE shall perform the procedures in RFC 5626 [92] to form a new flow to replace the failed one if it supports multiple registrations. If failed registration attempts occur in the process of creating a new flow, the flow recovery procedures defined in RFC 5626 [92] shall apply. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in in subclause 4.5 of RFC 5626 [92] shall be used.

NOTE 10: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

Delete Section 5.1.1.4.2 IMS AKA as a security mechanism (not relevant for a 1TR114 UE therefore deleted)

5.1.1.4.3 SIP digest without TLS as a security mechanism

On sending a REGISTER request that does not contain a challenge response, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 [21], including:

- the "username" header field parameter, set to the value of the private user identity;
- the "realm" header field parameter, set to the domain name of the home network;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to an empty value; and
- the "response" header field parameter, set to an empty value;

b) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and

c) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

5.1.1.4.4 SIP digest with TLS as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field set in accordance with subclause 5.1.1.2.3;

b) the Security-Client header field set to specify the signalling plane security mechanism the UE supports. The UE shall support the setup of a TLS session as defined in 3GPP TS 33.203 [19]. The UE shall support the "tls" security mechanism, as specified in RFC 3329 [48]. The UE shall support TLS for integrity and confidentiality protection as defined in RFC 3261 [26], and shall announce support for them according to the procedures defined in RFC 3329 [48]; and

c) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

a) set the lifetime of the respective TLS session to the value configured.

5.1.1.4.5 NASS-IMS bundled authentication as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) optionally, an Authorization header field, with the "username" header field parameter, set to the value of the private user identity;

NOTE 1: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When NASS-IMS bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

Delete Section 5.1.1.4.6 GPRS-IMS-Bundled authentication as a security mechanism (not relevant for a 1TR114 UE therefore deleted)

5.1.1.5 Authentication

Delete Section 5.1.1.5.1 IMS AKA - general (not relevant for 1TR114 UE therefore deleted)

~~*5.1.1.5.2 Void*~~

Delete Section 5.1.1.5.3 IMS AKA abnormal cases (not relevant for 1TR114 UE therefore deleted)

5.1.1.5.4 SIP digest without TLS – general

On receiving a 401 (Unauthorized) response to the REGISTER request, and where the "algorithm" Authorization header field parameter is "MD5", the UE shall extract the digest-challenge parameters as indicated in RFC 2617 [21] from the WWW-Authenticate header field. The UE shall calculate digest-response parameters as indicated in RFC 2617 [21]. The UE shall send another REGISTER request containing an Authorization header field. The header fields are populated as defined in subclause 5.1.1.2.3, with the addition that the UE shall include an Authorization header field containing a challenge response, i.e. "cnonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [21]. The UE shall set the Call-ID of the REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge. If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header fields with this REGISTER.

On receiving the 200 (OK) response for the REGISTER request, if the "algorithm" Authentication-Info header field parameter is "MD5", the UE shall authenticate the S-CSCF using the "rspauth" Authentication-Info header field parameter as described in RFC 2617 [21]. If the nextnonce field is present in the Authentication-Info header field the UE ~~*should*~~ *shall* use it when constructing the Authorization (***Authorization header for REGISTER and Proxy-Authorization for INVITE***) header for its next request as specified in RFC 2617 [21].

The nexnonce shall be stored by the IAD as long as the nonce value is valid. i.e. a new nonce will be provided either by sending the nonce in a Authentication-Info with the "nextnonce" or via nonce value received within a challenge response (401 or 407) as described in RFC 2617 [21]

The procedure for the use of nonce, nonce counter and next-nonce described within this document is valid for NASS bundled and Digest authentication.

The latest received "next-nonce" within a 200 OK for a request shall be used for the Re-Register.

5.1.1.5.5 SIP digest without TLS – abnormal procedures

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed.

5.1.1.5.6 SIP digest with TLS – general (Release 12)

On receiving a 401 (Unauthorized) response to the REGISTER request, the procedures in subclause 5.1.1.5.4 ***(see 4.2.7 in 1TR114)*** apply with the following differences:

- The UE shall check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or the list of supported security mechanisms does not include "tls", the UE shall abandon the authentication procedure and send a new REGISTER request.

In the case that the 401 (Unauthorized) response to the REGISTER is deemed to be valid the UE shall:

- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any; and

NOTE 1: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- send another REGISTER request using the TLS session to protect the message.

When TLS is used, the UE (IAD) shall register all IMPUs (Contacts) via one shared TLS connection. Connection reuse for 'SIP over TLS over TCP' shall apply according RFC 5923 [90] and RFC 5630 [91]

Implementation of RFC 5923 as follows:

Benefits of TLS Connection Reuse:

Opening an extra connection where an existing one is sufficient can result in potential scaling and performance problems. Each new connection using TLS requires a TCP three-way handshake, a handful of round trips to establish TLS, typically expensive asymmetric authentication and key generation algorithms, and certificate verification.

Either the UE or the server may terminate a TLS session by sending a TLS closure alert. Before closing a TLS connection, the initiator of the closure MUST either wait for any outstanding SIP transactions to complete, or explicitly abandon them.

After the initiator of the close has sent a closure alert, it MUST discard any TLS messages until it has received a similar alert from its peer. The receiver of the closure alert MUST NOT start any new SIP transactions after the receipt of the closure alert.

Implementation of RFC5630 as follows:

Since SIP allows for requests in both directions (e.g., an incoming call), the UE is expected to keep the TLS connection alive, and that connection is expected to be reused for both incoming and outgoing requests.

This solution of having the UA always initiate and keep alive the connection also solves the Network Address Translation (NAT) and firewall problem as it ensures that responses and further requests will always be deliverable on the existing connection.

The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header field containing a challenge response, "cnonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [21]. The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

When SIP digest with TLS is used, and for the case where the 401 (Unauthorized) response to the REGISTER request is deemed to be valid, the UE shall establish the TLS session as described in 3GPP TS 33.203 [19]. The UE shall use this TLS session to send all further messages towards the P-CSCF towards the protected server port.

5.1.1.5.7 SIP digest with TLS – abnormal procedures

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed. If performing SIP digest with TLS, the UE should send an initial REGISTER according to the procedure specified in subclause 5.1.1.2 if the UE considers the TLS session to be no longer active at the P-CSCF.

5.1.1.5.8 NASS-IMS bundled authentication – general

NASS-IMS bundled authentication is only applicable to UEs that contain neither USIM nor ISIM. Authentication is achieved via the registration and re-registration procedures as defined in subclause 5.1.1.2 and subclause 5.1.1.4. NASS-bundled authentication is granted by the network upon receipt by the UE of a 200 (OK) response to the initial REGISTER request.

There is no separate authentication procedure.

5.1.1.5.9 NASS-IMS bundled authentication – abnormal procedures

There is no separate authentication procedure, and therefore no abnormal procedures.

Delete Section 5.1.1.5.10 GPRS-IMS-Bundled authentication – general (not relevant for 1TR114 UE therefore deleted)

Delete Section 5.1.1.5.11 GPRS-IMS-Bundled authentication – abnormal procedures (not relevant for 1TR114 UE therefore deleted)

5.1.1.5.12 Abnormal procedures for all security mechanisms

A UE shall only respond to two consecutive invalid challenges and shall not automatically attempt authentication after two consecutive failed attempts to authenticate. The UE may attempt to register with the network again after an implementation specific time.

5.1.1.5A Network-initiated re-authentication

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and
- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expiry attribute within the <contact> sub-element that the UE registered to adjust the expiration time for that public user identity; and
2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, if required.

NOTE: When authenticating a given private user identity, the S-CSCF will only shorten the expiry time within the <contact> sub-element that the UE registered using its private user identity. The <contact> elements for the same public user identity, if registered by another UE using different private user identities remain unchanged. The UE will not initiate a reregistration procedure, if none of its <contact> sub-elements was modified.

5.1.1.5B Change of IPv6 address due to privacy

Stateless address autoconfiguration as described in RFC 2462 [20E] defines how an IPv6 prefix and an interface identifier is used by the UE to construct a complete IPv6 address.

If the UE receives an IPv6 prefix, the UE may change the interface identity of the IPv6 address as described in RFC 3041 [25A] due to privacy but this can result in service discontinuity for services provided by the IM CN subsystem.

NOTE: When the UE constructs new IPv6 address by changing the interface identity, the UE can either transfer all established dialogs to new IPv6 address as specified in 3GPP TS 24.237 [8M] and subsequently relinquish the old IPv6 address, or terminate all established dialogs and transactions. While transferring the established dialogs to new IPv6 address, the UE will have double registration, i.e. one registration for the old IPv6 address and another for the new IPv6 address.

The procedure described below assumes that the UE will terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem until the new registration is performed. If the UE decides to change the IPv6 address due to privacy and terminate all established dialogs and transaction, associated with old IPv6 address, the UE shall:

1) terminate all ongoing dialogs (e.g., sessions) and transactions (e.g., subscription to the reg event) that were using the old IPv6 address;
2) deregister all registered public user identities that were using the old IPv6 address as described in subsclause 5.1.1.4;

3) construct a new IPv6 address according to the procedures specified in RFC 3041 [25A];

4) register the public user identities that were deregistered in step 2 above with a new IPv6 address, as follows:

   a) by performing an initial registration as described in subsclause 5.1.1.2; and

   b) by performing a subscription to the reg event package as described in subsclause 5.1.1.3; and

5) subscribe to other event packages it was subscribed to before the change of IPv6 address procedure started.

To ensure a maximum degree of continuous service to the end user, the UE should transfer all established dialogs to the new IPv6 address as specified in 3GPP TS 24.237 [8M] rather than terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem as described above.

5.1.1.6 User-initiated deregistration

5.1.1.6.1 General

For any public user identity that the UE has previously registered, the UE can deregister via a single registration procedure:

- all contact addresses bound to the indicated public user identity;

- some contact addresses bound to the indicated public user identity;

- a particular contact address bound to the indicated public user identity; or

- when the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field) one or more flows bound to the indicated public user identity.

The UE can deregister a public user identity that it has previously registered with its contact address at any time. The UE shall protect the REGISTER request using a security association or TLS session that is associated with contact address, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

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

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs that were using the contact addresses or the flow that is going to be deregistered and related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities. However:

- if the dialog that was established by the UE subscribing to the reg event package used the public user identity that is going to be deregistered; and

- this dialog is the only remaining dialog used for subscription to reg event package of the user, i.e. there are no other contact addresses registered with associated subscription to the reg event package of the user;

then the UE shall not release this dialog.

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses or one of its flows, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be deregistered;

c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and:

1) if the UE is removing the binding between the public user identity indicated in the To header field, (together with the associated implicitly registered public user identities), and the contact address indicated in the Contact header field; and

- if the UE supports GRUU, or multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), or has an IMEI available, or has an MEID available, the Contact header field also contains the "+sip.instance" header field parameter. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks;

- if the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), the Contact header field does not contain the "reg-id" header field parameter;

- if the UE does not supports GRUU and does not support multiple registrations (i.e. the "outbound" option tag is not included in the Supported header field), and does not have an IMEI available, and does not have an MEID available, the Contact header field does not contain either the "+sip.instance" header field parameter or the "reg-id" header field parameter;

NOTE 1: Since the contact address is deregistered, if there are any flows that were previously registered with the respective contact address, all flows terminating at the respective contact address are removed.

2) if the UE is removing the binding between the public user identity indicated in the To header field, (together with the associated implicitly registered public user identities) and one of its flows, the Contact header field contains the "+sip.instance" header field parameter and the "reg-id" header field parameter that identifies the flow; and

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

3) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;

e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, ;

NOTE 3: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

i) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

For a public user identity that the UE has registered with multiple contact addresses or multiple flows (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses or multiple flows, bound to its public user identity, via single deregistration proceduere as specified in RFC 3261 [26]. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header field is populated as specifed above in bullets a) through i).

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "*" and the Expires header field with a value of "0". The UE shall not include the "instance-id" feature tag and the "reg-id" header field parameter in the Contact header field in the REGISTER request.

NOTE 4: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

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

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- remove all registration details relating to this public user identity and the associated contact address.
- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

If there are no more public user identities registered with this contact address, the UE shall delete any stored media plane security mechanisms and related keys and any security associations or TLS sessions and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and all security association or TLS session is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

Delete Section 5.1.1.6.2 IMS AKA as a security mechanism (not relevant for 1TR114 UE therefore deleted)

5.1.1.6.3 SIP digest without TLS as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 [21], including:
   - the "username" header field parameter, set to the value of the private user identity;
   - the "realm" header field parameter, set to the domain name of the home network;
   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
   - the "nonce" header field parameter, set to an empty value; and
   - the "response" header field parameter, set to an empty value;

b) for each Contact header field and associated contact address include the associated unprotected port value (where the UE was expecting to receive mid-dialog requests); and

c) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

5.1.1.6.4 SIP digest with TLS as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field set in accordance with subclause 5.1.1.6.3; and

b) a Security-Client header field, set to specify the signalling plane security mechanism it supports. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

c) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

5.1.1.6.5 NASS-IMS bundled authentication as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) optionally, an Authorization header field, with the "username" header field parameter, set to the value of the private user identity;

NOTE 1: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.6.1, there are no additional requirements for the UE.

NOTE 2: When NASS-IMS bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request ~~is not~~ *has to be* expected to be received.

In Deutsche Telekom IMS the challenge mechanism is also used for NAS-IMS bundled authentication is used. Further procedures apply according to section 5.1.1.5.4

Delete Section 5.1.1.6.6 GPRS-IMS-Bundled authentication as a security mechanism (not relevant for 1TR114 UE therefore deleted)

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request, on any dialog which was generated during the subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE, with:

1) the state attribute within the <registration> element set to "terminated", and within each <contact> element belonging to this UE, the state attribute set to "terminated" and the event attribute set either to "unregistered", or "rejected", or "deactivated", the UE shall remove all registration details relating to the respective public user identity (i.e. consider the public user identity indicated in the aor attribute of the <registration> element as deregistered); or

2) the state attribute within the <registration> element set to "active", and within a given <contact> element belonging to this UE, the state attribute set to "terminated", and the associated event attribute set either to "unregistered", or "rejected" or "deactivated", the UE shall consider the binding between the public user identity and either the contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used) indicated in the respective <contact> element as removed. The UE shall consider its public user identity as deregistered when all bindings between the respective public user identity and all contact addresses and all registration flow and the associated contact address (if the multiple registration mechanism is used) belonging to this UE are removed.

NOTE 1: When multiple registration mechanism is used to register a public user identity and bind it to a registration flow and the associated contact address, there will be one <contact> element for each registration flow and the associated contact address.

NOTE 2: If the state attribute within the <registration> element is set to "active" and the <contact> element belonging to this UE is set to "active", the UE will consider that the binding between the public user identity and either the respective contact address or the registration flow and the associated contact address as left unchanged.

In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request, the UE shall delete all security associations or TLS sessions towards the P-CSCF either:

- if all <registration> element(s) have their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header field contains the value of "terminated"; or

- if each <registration> element that was registered by this UE has either the state attribute set to "terminated", or the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated".

When all UE's public user identities are registered via a single P-CSCF and the subscription dialog to the reg event package of the UE is set via the respective P-CSCF, the UE shall delete these security associations or TLS sessions towards the respective P-CSCF when all public user identities have been deregistered and after the server transaction (as defined in RFC 3261 [26]) pertaining to the received NOTIFY request terminates.

NOTE 3: Deleting a security association or TLS session is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 4: If all the public user identities (i.e. <contact> elements) registered by this UE are deregistered and the security associations or TLS sessions have been removed, the UE considers the subscription to the reg event package terminated since the NOTIFY request was received with Subscription-State header field containing the value of "terminated".

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID header field, and the values of tags in To and From header fields).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package the UE shall perform the following actions:

- if a state attribute "active", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a state attribute "active" is received, and the UE supports GRUU (see table A.4, item A.4/53), then for each public user identity indicated in the notification that contains a <pub-gruu> element or a <temp-gruu> element or both (as defined in RFC 5628 [94]) then the UE shall store the value of those elements in association with the public user identity;

- if a state attribute "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered and shall remove any associated GRUUs.

NOTE 1: There can be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity or when S-CSCF receives a Push-Profile-Request (PPR) from the HSS (as described in 3GPP TS 29.228 [14]) changing the status of a public user identity associated with a registered implicit set from barred to non-barred. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities can also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

NOTE 2: RFC 5628 [94] provides guidance on the management of temporary GRUUs, utilizing information provided in the reg event notification.

5.1.2.2 General SUBSCRIBE requirements

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

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

5.1.2A.1 UE-originating case

5.1.2A.1.1 General

The UE may also use Service Code Commands (SCC). The procedures are described in Annex A of 1TR126 [Ref_dt2]. The SCC are provided in Annex D of the main document 1TR114 [Ref_dt1].

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

When the UE sends any request using either a given contact address or to the registration flow and the associated contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

- if SIP digest without TLS is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the port value of an unprotected port and the contact address where the UE expects to receive subsequent mid-dialog requests; and

  b) populate the Via header field of the request with the port value of an unprotected port and the respective contact address where the UE expects to receive responses to the request;

- if SIP digest with TLS is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port; and

  b) include the protected server port in the Via header field entry relating to the UE;

- if NASS-IMS bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2;

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

RELEASE 12 ???

When SIP digest *or NASS bundled authentication is* in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;

- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication *(next INVITE Requests) as well as for authentication (next REGISTER request)* associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;

- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication *(which is the same as for authentication)* associated to the same registration or registration flow (if the multiple registration mechanism is used); and

- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

Where a security association or TLS session exists, the UE shall discard any SIP response that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

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

The P-Preferred-ID is applicable.
The privacy header shall be used to request OIR.

NOTE 1: Since the S-CSCF uses the P-Asserted-Identity header field when checking whether the UE originating request matches the initial filter criteria, the P-Preferred-Identity header field inserted by the UE determines which services and applications are invoked.

When sending any initial request for a dialog or request for a standalone transaction using either a given contact address or to the registration flow and the associated contact address, the UE may include any of the following in the P-Preferred-Identity header field:

- a public user identity which has been registered by the user with the respective contact address;
- an implicitly registered public user identity returned in a registration-state event package of a NOTIFY request whose <uri> sub-element inside the <contact> sub-element of the <registration> element is the same as the contact address being used for this request and was not subsequently deregistered or that has not expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 2: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header field.

NOTE 3: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header field.

NOTE 4: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header field to "Anonymous" as specified in RFC 3261 [26].

NOTE 5: The contents of the From header field are not necessarily modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user can well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header field from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header field other than Anonymous.

The UE shall determine the public user identity to be used for this request as follows:

1) if a P-Preferred-Identity was included, then use that as the public user identity for this request; or
2) if no P-Preferred-Identity was included, then use the default public user identity for the security association or TLS session and the associated contact address as the public user identity for this request;

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 6: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g first contacted via a registration or configuration procedure). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate draft-montemurro-gsma-imei-urn [153] even when the UE requests privacy using RFC 3323 [33].

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627 [93]; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627 [93]; or

   - otherwise, a SIP URI containing the contact address of the UE;

   NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626 [92];

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841 [56B], the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841 [56B], the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

If this is a request within an existing dialog, and the request includes a Contact header field, then the UE should insert the previously used Contact header field.

If the UE support multiple registrations as specified in RFC 5626 [92], the UE should include option-tag "outbound" in the Supported header field.

If this is a request for a new dialog or standalone transaction and the request is related to an IMS communication service that requires the use of an ICSI then the UE:

1) shall include the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service that is related to the request in a P-Preferred-Service header field according to RFC 6050 [121]. If a list of network supported ICSI values was received as specified in 3GPP TS 24.167 [8G], the UE shall only include an ICSI value that is in the received list;

NOTE 8: The UE only receives those ICSI values corresponding to the IMS communication services that the network provides to the user.

2) may include an Accept-Contact header field containing an ICSI value (coded as specified in subclause 7.2A.8.2) that is related to the request in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 if the ICSI for the IMS communication service is known.

NOTE 9: If the UE includes the same ICSI values into the Accept-Contact header field and the P-Preferred-Service header field, there is a possibility that one of the involved S-CSCFs or an AS changes the ICSI value in the P-Asserted-Service header field, which results in the message including two different ICSI values (one in the P-Asserted-Service header field, changed in the network and one in the Accept-Contact header field).

If an IMS application indicates that an IARI is to be included in a request for a new dialog or standalone transaction, the UE shall include an Accept-Contact header field containing an IARI value (coded as specified in subclause 7.2A.9.2) that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B].

NOTE 10: RFC 3841 [56B] allows multiple Accept-Contact header fields along with multiple Reject-Contact header fields in a SIP request, and within those header fields, expressions that include one or more logical operations based on combinations of media feature tags. Which registered UE will be contacted depends on the Accept-Contact header field and Reject-Contact header field combinations included that evaluate to a logical expression and the relative qvalues of the registered contacts for the targeted registered public user identity. There is therefore no guarantee that when multiple Accept-Contact header fields or additional Reject-Contact header field(s) along with the Accept-Contact header field containing the ICSI value or IARI value are included in a request that the request will be routed to a contact that registered the same ICSI value or IARI value. Charging and accounting is based upon the contents of the P-Asserted-Service header field and the actual media related contents of the SIP request and not the Accept-Contact header field contents or the contact reached.

NOTE 11: The UE only includes the header field parameters "require" and "explicit" in the Accept-Contact header field containing the ICSI value or IARI value if the IMS communication service absolutely requires that the terminating UE understand the IMS communication service in order to be able to accept the session. Including the header field parameters "require" and "explicit" in Accept-Contact header fields in requests which don't absolutely require that the terminating UE understand the IMS communication service in order to accept the session creates an interoperability problem for sessions which otherwise would interoperate and violates the interoperability requirements for the ICSI in 3GPP TS 23.228 [7].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

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

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 12: The case where the UE is unaware of the requirement for resource priority because the user requested the capability as part of the dialstring falls outside the scope of this requirement. Such cases can exist and will need to be dealt with by an appropriate functional entity (e.g. P-CSCF) to process the dialstring. For certain national implementations, signalling of a Resource-Priority header field to or from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and

b) the P-CSCF port based on the security mechanism in use:

- if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;

c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

NOTE 14: When the UE registers multiple contact addresses, there will be a list of Service-Route headers for each contact address. When sending a request using a given contact address and the associated security associations or TLS session, the UE will use the corresponding list of Service-Route headers to construct a list of Route headers.

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

If a request is for a new dialog or standalone transaction, and the request matches a trigger for starting logging of SIP signalling, as described in draft-dawes-sipping-debug [140] and contained in the trace management object defined in 3GPP TS 24.323 [8K], the UE shall:

- start to log SIP signalling for this dialog; and
- in any requests or responses sent on this dialog, insert a P-Debug-ID header field containing the value contained in the trace management object.

If a request or response is sent on a dialog for which logging of signalling is in progress, the UE shall check whether a trigger for stopping logging of SIP signalling has occurred, as described in draft-dawes-sipping-debug [140] and contained in the trace management object defined in 3GPP TS 24.323 [8K].

a) If a stop trigger event has occurred, the UE shall stop logging of signalling; or

b) if a stop trigger event has not occurred, the UE shall:

   - in any requests or responses sent on this dialog, insert a P-Debug-ID header field containing the value for this session contained in the trace management object; and
   - log the request.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 15: It is an implementation option whether these actions are also triggered by other means.

If the UE receives a 1xx or 200 (OK) response to an initial request for a dialog, the response containing a P-Asserted-Identity header field set to an emergency number as specified in 3GPP TS 22.101 [1A], the UE procedures in subclause 5.1.6.10 apply.

If the UE receives a 3xx response containing a Contact header field:

1) if the 3xx response is a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry of the Path header field value received during registration and the response contains a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) then the UE shall not recurse on the Contact header field, the UE shall apply the procedures in subclause 5.1;

NOTE 16: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

2) otherwise, the UE should not automatically recurse on the Contact header field without first indicating the identity of the user to which a request will be sent and obtaining authorisation of the served user.

NOTE 17: A UE can still automatically recurse on 3xx responses as part of a service if the nature of the service enables the UE to identify 3xx responses as having originated from the home network and networks trusted by the home network and the nature of the service ensures that the charging for the requests sent as a result of the 3xx response is correlated with the original request.

NOTE 18: Automatically recursing on untrusted 3xx responses opens up the UE to being redirected to premium rate URIs without the user's consent.

5.1.2A.1.2 Structure of Request-URI

The UE may include a SIP URI complying with RFC 3261 [26], a tel URI complying with RFC 3966 [22], a pres URI complying with RFC 3859 [179], an im URI complying with RFC 3860 [180] or a mailto URI complying with RFC 2368 [181].

The UE may use non-international formats of E.164 numbers or non-E.164 numbers, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966 [22], with a local number followed by a "phone-context" tel URI parameter value.

2) a SIP URI, complying with RFC 3261 [26], with the "user" SIP URI parameter set to "phone"

3) a SIP URI, complying with RFC 3261 [26] and RFC 4967 [103], with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

5.1.2A.1.3 UE without dial string processing capabilities

In this case the UE does not perform any analysis of the dial string. This requires that the dialling plan is designed so it enables the network to differentiate local numbers from other numbers.

The dial string is sent to the network, in the Request-URI of a initial request or a stand alone transaction, using one of the following formats:

1) a tel-URI, syntactically complying with RFC 3966 [22], with the dial string encoded as a local number followed by a "phone-context" tel URI parameter value;

EXAMPLE: tel:<input dial string>;phone-context=operator.com

2) a SIP URI, syntactically complying with RFC 3261 [26], with the user =phone parameter, embedding a tel-URI with a "phone-context" tel URI parameter value;

EXAMPLE: sip:<input dial string>;
phone-context=operator.com@operator.com;user=phone

3) a SIP URI, complying with RFC 3261 [26] and RFC 4967 [103], with the user=dialstring parameter and a with a "phone-context" tel-URI parameter value in the user part; or

EXAMPLE: sip:<input dial string>;
phone-context=operator.com@operator.com;user=dialstring

phone-context=unprocesseddialstringexample.com@operator.com;user=dialstring

4) a SIP URI syntactically complying with RFC 3261 [26], where the user part contains the dial string and the domain name is specific enough to enable to network to understand that the user part contains a dial string.

EXAMPLE: sip:<input dial string>@dialstrings.entreprise.com

For cases 1), 2), and 3) the UE shall set the "phone-context" tel URI parameter in accordance with subclause 5.1.2A.1.5.

5.1.2A.1.4 UE with dial string processing capabilities

In this case the UE performs sufficient dial string analysis (or receives an explicit indication from the user) to identify the type of numbering that is used and processes the dial string accordingly before building the Request-URI

If the UE detects that a local dialling plan is being used, where the terminal is able to identify a global telephone number, the normal procedures apply after removing all dial string elements used for local numbering detection purposes (e.g. escape codes).

If the UE detects that a local (private or public) dialling plan is being used, it may decide to send the dial string unchanged to the network as described in subclause 5.1.2A.3.2 or the UE may decide to alter it to comply with the local numbering plan (e.g. remove all dial string elements used for local numbering detection).

In the latter case the local numbering information is sent using one of the following formats:

1) a tel-URI, complying with RFC 3966 [22], with a local number followed by a "phone-context" tel-URI parameter value;

2) a SIP URI, complying with RFC 3261 [26], with the "user" SIP URI parameter set to "phone" and a user part embedding a local number with a phone-context parameter; and

3) if the UE intends to send information related to supplementary services, a SIP URI, complying with RFC 3261 [26] and RFC 4967 [103], with the "user" SIP URI parameter set to "dialstring" and a with a "phone-context" tel URI parameter value in the user part.

The UE shall set the "phone-context" tel URI parameter in accordance with subclause 5.1.2A.1.5.

NOTE: The way how the UE process the dial-string and handles special characters (e.g. pause) in order to produce a conformant SIP URI or tel-URI according to RFC 3966 [22] is implementation specific.

As a general rule, recognition of special service numbers shall take priority over other dialling plan issues. If the dial string equates to a pre-configured service URN as specified in RFC 5031 [69]) then the service-urn should be sent.

5.1.2A.1.5 Setting the "phone-context" tel URI parameter

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966 [22].

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 [22] as defined in subclause 7.2A.10; and

- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 [22] as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number or the UE is unable to determine the type of the dialled number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966 [22], e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value (e.g. using OMA-DM with the management object specified in 3GPP TS 24.167 [8G]) inserted by the UE.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

5.1.2A.1.6 Abnormal cases

In the event the UE receives a *504 (Server Time-out)* response containing:

1) a P-Asserted-Identity header field set to a value equal to a URI:

   a) from the Service-Route header field value received during registration; or

   b) from the Path header field value received during registration; and

NOTE 1: If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field and Service-Route header field values. The Path header field value and Service-Route header field value corresponding to the flow on which the 504 (Server Time-out) response was received are checked.

2) a *Content-Type header field set according to subclause* 7.6 *(i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the* following treatment*default content disposition, identified as "3gpp-alternative-service", is applied as follows:*

a) *if the 504 (Server Time-out) response includes an IM CN subsystem XML body as described in subclause 7.6 with* the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element:

A*a*) with *the* <*type*> child *element set to "restoration"* (see table 7.6.2*7AA*); *and*

B*b*) with *the* <*action*> child *element set to "initial-registration"* (see table 7.6.3*7AB*);

then the UE:

- *shall initiate* S-CSCF *restoration procedures by performing an initial registration as specified in subclause 5.1.1.2; and*

- *may provide an indication to the user based on the text string contained in the* <*reason*> child *element* of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 2: If the UE has discovered multiple P-CSCF addresses and has *got back the* information that the P-CSCF was unable to forward the *a* request resulting in sending back the *by receiving a* 504 (Server Time-out) response, when starting the*the UE shall start a new* initial registration it is appropriate for the UE to select*via* a P-CSCF address different from the one used for the registration binding on which the 504 (Server Time-out) response was received.

When the UE is unable to forward an initial request to the P-CSCF, i.e. there is no response to ~~*the*~~ service request ~~*and*~~ its retransmissions received by the UE (i.e. the SIP transaction timer B or F expires), the UE shall initiate an initial registration as specified in subclause 5.1.1.2.

5.1.2A.2 UE-terminating case

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

Where a security association or TLS session exists, the UE shall discard any SIP request that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

If an initial request contains an Accept-Contact header field containing the g.3gpp.icsi-ref media feature tag with an ICSI value, the UE should invoke the IMS application that is the best match for the ICSI value.

If an initial request contains an Accept-Contact header field containing the g.3gpp.iari-ref media feature tag with an IARI value the UE should invoke the IMS application that is the best match for the IARI value.

The UE can receive multiple ICSI values, IARI values or both in an Accept-Contact header field. In this case it is up to the implementation which of the multiple ICSI values or IARI values the UE takes action on.

NOTE 1: The application verifies that the contents of the request (e.g. SDP media capabilities, Content-Type header field) are consistent with the the ICSI value in the g.3gpp.icsi-ref media feature tag and IARI value contained in the g.3gpp.iari-ref media feature tag.

If an initial request does not contain an Accept-Contact header field containing a g.3gpp.icsi-ref media feature tag or a g.3gpp.iari-ref media feature tag the UE shall invoke the application that is the best match based on the contents of the request (e.g. SDP media capabilities, Content-Type header field, media feature tag).

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

NOTE 2: In the UE-terminating case, this version of the document makes no provision for the UE to provide a P-Preferred-Identity in the form of a hint.

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

~~*The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses.*~~

*T*he UE shall not inc*lu*de its *"*+sip.instance*"* header field parameter in the Contact header field in its non-register requests *and* responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 4: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g first contacted via a registration or configuration procedure). Including

~~*Editor's Note: Whether the inclusion of*~~ the "+sip.instance" header field parameter containing an IMEI URN does not violate draft-montemurro-gsma-imei-urn [153] even when the UE requests privacy using RFC 3323 [33].

If the response includes a Contact header field, and the response is sent within an existing dialog, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

If the response includes a Contact header field, and the response is not sent within an existing dialog, the Contact header field is populated as follows:

1) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does not indicate privacy of the contents of the P-Asserted-Identity header field, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627 [93];

2) if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does indicate privacy of the P-Asserted-Identity, then should insert the temporary GRUU ("temp-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93];

NOTE 5: The above items 1 and 2 are mutually exclusive.

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3841 [56B] the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service and then the UE may include the IARI value for any IMS application that applies for the dialog, (coded as specified in subclause 7.2A.9.2), that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B]. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the originating UE(s) and other IARI values for the IMS application that is related to the IMS communication service; and

4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then the UE may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to any IMS application and that applies for the dialog, in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

If the UE did not insert a GRUU in the Contact header field then the UE shall include a port in the address in the Contact header field as follows:

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; or

- if SIP digest without TLS is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial registration.

If the UE receives a Resource-Priority header field in accordance with RFC 4412 [16] in an initial request for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 6: For certain national implementations, signalling of a Resource-Priority header field to and from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method (see subclause 7.2A.4).

If a request is for a new dialog or standalone transaction, and the request matches a trigger for starting logging of SIP signalling, as described in draft-dawes-sipping-debug [140] and contained in the trace management object defined in 3GPP TS 24.323 [8K], the UE shall:

- start to log SIP signalling for this dialog; and
- in any requests or responses sent on this dialog, insert a P-Debug-ID header field containing the value contained in the trace management object.

If a request or response is sent on a dialog for which logging of signalling is in progress, the UE shall check whether a trigger for stopping logging of SIP signalling has occurred, as described in draft-dawes-sipping-debug [140] and contained in the trace management object defined in 3GPP TS 24.323 [8K].

a) If a stop trigger event has occurred, the UE shall stop logging of signalling; or

b) if a stop trigger event has not occurred, the UE shall:

   - in any requests or responses sent on this dialog, insert a P-Debug-ID header field containing the value for this session contained in the trace management object; and
   - log the request or response.

5.1.3 Call initiation - UE-originating case

5.1.3.1 Initial INVITE request

If a UE for non mobile access supports the precondition mechanism then the UE shall set neither the supported nor the required header for preconditions when sending a initial INVITE.
The support of preconditions (if implemented) is "passive" and if initial INVITE received by the UE and indicates the precondition mechanism as supported or required the UE shall reserve the local resources and indicate the preconditions as required within the response to the initial INVITE. Further detail is described within the following section.

Upon generating an initial INVITE request, the UE shall include the Accept header field with "application/sdp", the MIME type associated with the 3GPP IM CN subsystem XML body (see subclause 7.6.1) and any other MIME type the UE is willing and capable to accept.

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

The UE ~~*may*~~ *shall* initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

~~*NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.*~~

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism *shall not indicate the support* ~~*should make use*~~ of the precondition mechanism, ~~*even if*~~ *when* it does not require local resource reservation.

~~*Upon generating an initial INVITE request using the precondition mechanism, the UE shall:*~~

- ~~*indicate the support for reliable provisional responses and specify it using the Supported header field mechanism;and*~~
- ~~*indicate the support for the preconditions mechanism and specify it using the Supported header field mechanism.*~~

~~*Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header field mechanism.*~~

~~*NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header field, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.*~~

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE *shall* ~~*can*~~ accept ~~*or reject*~~ any of the forked responses *(minimum 10 provisional responses from a forked INVITE)*, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

When supporting reliability of provisional responses (100rel) as defined in RFC 3262 [27] then the procedures in receiving multiples provisional responses for each UE or group of UE has to apply with answering PRACK for each provisional response received.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation after a 200 (OK) response has been received for the initial INVITE request, in case the terminating UE does not support the PRACK request (as described in RFC 3262 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

NOTE 5: If the UE supports the P-Early-Media header field, upon receiving a 18x provisional response with a P-Early-Media header field indicating authorized early media, as described in RFC 5009 [109], if the preconditions are met, the UE should, based on local configuration, present received early media to the user.

NOTE 6: If the UE supports the P-Early-Media header field, upon receiving a 180 (Ringing) provisional response with a P-Early-Media header field indicating authorized early media, as described in RFC 5009 [109], if the preconditions are met, and the UE presents the received early media to the user based on local configuration, the UE will not provide an indication that the invited user is being alerted.

NOTE 7: If the UE supports the P-Early-Media header field and if the most recently received P-Early-Media header field within the dialog includes a parameter applicable to media stream with value "inactive", then based on local configuration, the UE will provide an indication that the invited user is being alerted and stop presenting received early media to the user if requested by any previous receipt of P-Early-Media header field within the dialog.

If the UE wishes to receive early media authorization indications, as described in RFC 5009 [109], the UE shall add the P-Early-Media header field with the "supported" parameter to the INVITE request.

To request end to access edge media security either on a session or media level, the UE shall send an SDP Offer for an SRTP stream containing one or more SDES crypto attributes, each with a key and other security context parameters required according to RFC 4568 [168], together with the attribute "a=3ge2ae".

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

1) acknowledge the response with an ACK request; and

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

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

NOTE 8: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements.

Upon receiving a 421 (Extension Required) response to an initial INVITE request in which the precondition mechanism was not used, including the "precondition" option-tag in the Require header field, the originating UE shall:

- send a new INVITE request using the precondition mechanism, if the originating UE supports the precondition mechanism; and
- send an UPDATE request as soon as the necessary resources are available and a 200 (OK) response for the first PRACK request has been received.

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

The UE may include a "cic" tel-URI parameter in a tel-URI, or in the userinfo part of a SIP URI with user=phone, in the Request-URI of an initial INVITE request if the UE wants to identify a user-dialed carrier, as described in RFC 4694 [112].

NOTE 9: The method whereby the UE determines when to include a "cic" tel-URI parameter and what value it should contain is outside the scope of this document (e.g. the UE could use a locally configured digit map to look for special prefix digits that indicate the user has dialled a carrier).

NOTE 10: The value of the "cic" tel-URI parameter reported by the UE is not dependent on UE location (e.g. the reported value is not affected by roaming scenarios).

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry of the Path header field value received during registration and the the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), the UE shall attempt an emergency call as described in subclause 5.1.6.

NOTE 11: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

Upon receiving a 199 (Early Dialog Terminated) provisional response to an established early dialog the UE shall release resources specifically related to that early dialog.

5.1.4 Call initiation - UE-terminating case

5.1.4.1 Initial INVITE request

In cases when the UE supports preconditions then the support of preconditions shall be "passive". I.e. when a initial INVITE is received by the UE and indicates the precondition mechanism as supported or required the UE shall reserve the local resources and indicate the preconditions as required within the response to the initial INVITE. Further detail is described within the following section.

The preconditions mechanism should be supported by the terminating UE.

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

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and

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

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header field and:

   - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

   - the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism; or

c) the received INVITE request includes the "precondition" option-tag in the Require header field, the terminating UE shall use the precondition mechanism.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the terminating UE requires a reliable alerting indication at the originating side, the UE shall send the 180 (Ringing) response reliably.

In case more than one UE or groups of UE's are connected to the IAD (See Figure) multiples provisional responses will be sent back from the IAD supporting the profile of the end device which are connected. e.G if analogue and DECT phones are connected each port (or group of ports) reflects an own UA which has to answer properly due to TS 24.229/RFC3261 procedures. This different provisional responses has to be sent with the popper SDP.

When supporting reliability of provisional responses (100rel) then the procedures in sending multiples provisional responses for each UE or group of UE has to apply. Each PRACK has to be answered properly with a 200 OK (PRACK).

If the received INVITE request indicated support for reliable provisionable responses, but did not require their use, the terminating UE shall send provisional responses reliably only if the provisional response carries SDP or for other application related purposes that requires its reliable transport.

NOTE 4: Certain applications, *(i.e. DT IMS applications),* services and operator policies might mandate the terminating UE to send a 199 (Early Dialog Terminated) provisional response (see RFC 6228 [142]) prior to sending a non-2xx final response to the INVITE request.

If the terminating UE uses the precondition mechanism and if the originating side requested confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE then upon successful reservation of local resources, the terminating UE shall confirm the successful resource reservation (see subclause 6.1.3) within an SIP UPDATE request.

NOTE 5: Originating side requests confirmation for the result of the resource reservation at the terminating UE e.g. when an application server performs 3rd party call control. The request for confirmation for the result of the resource reservation at the terminating UE can be included e.g. in the SDP answer in the PRACK request.

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sends an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

5.1.5 Call release

Void.

Delete Section 5.1.6 Emergency service mechanism (not relevant for 1TR114 UE therefore deleted)

NOTE: The implementation of the emergency service is Deutsche Telekom specific.

5.1.7 Void

5.1.8 Void

Delete Section 5.2 Procedures at the P-CSCF mechanism (not relevant for 1TR114 UE therefore deleted)

Delete Section 5.3 Procedures at the I-CSCF (not relevant for 1TR114 UE therefore deleted)

Delete Section 5.4 Procedures at the S-CSCF (not relevant for 1TR114 therefore deleted)

Delete Section 5.5 Procedures at the MGCF (not relevant for 1TR114 therefore deleted)

Delete Section 5.6 Procedures at the BGCF (not relevant for 1TR114 therefore deleted)

Delete Section 5.7 Procedures at the Application Server (AS) (not relevant for 1TR114 therefore deleted)

Delete Section 5.8 Procedures at the MRFC (not relevant for 1TR114 therefore deleted)

Delete Section 5.8AProcedures at the MRB (not relevant for 1TR114 therefore deleted)

5.9 Void

5.9.1 Void

Delete Section 5.10 Procedures at the IBCF (not relevant for 1TR114 therefore deleted)

Delete Section 5.11 Procedures at the E-CSCF (not relevant for 1TR114 therefore deleted)

Delete Section 5.12 Location Retrieval Function (LRF) (not relevant for 1TR114 therefore deleted)

Delete Section 5.13 ISC gateway function (not relevant for 1TR114 therefore deleted)

6 Application usage of SDP

6.1 Procedures at the UE

6.1.1 General

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect SDP message bodies. Hence, the UE shall not encrypt SDP message bodies.

During the session establishment procedure, and during session modification procedures, SIP messages shall only contain an SDP message body if that is intended to modify the session description, or when the SDP message body is included in the message because of SIP rules described in RFC 3261 [26].

NOTE 1: A codec can have multiple payload type numbers associated with it.

In order to support accurate bandwidth calculations, the UE may include the "a=ptime" attribute for all "audio" media lines as described in RFC 4566 [39]. If a UE receives an "audio" media line with "a=ptime" specified, the UE should transmit at the specified packetization rate. If a UE receives an "audio" media line which does not have "a=ptime" specified or the UE does not support the "a=ptime" attribute, the UE should transmit at the default codec packetization rate as defined in RFC 3551 [55A]. The UE will transmit consistent with the resources available from the network.

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

For "video" and "audio" media types that utilize the RTP/RTCP, in addition to the "b=AS" parameter, the UE may specify the "b=TIAS", and "a=maxprate" parameters in accordance with RFC 3890 [152]. The value of the parameter shall be determined as described in RFC 3890 [152]. The value or absence of the "b=" parameter(s) may affect the assigned QoS which is defined in 3GPP TS 29.213 [13C].

If a UE receives a media line which contains both a=ptime and a=maxprate, the UE should use the a=maxprate value, if this attribute is supported.

If multiple codecs are specified on the media line, "a=maxprate" (or "a=ptime" if "a=maxprate" is not available or not supported) should be used to derive the packetization time used for all codecs specified on the media line. Given that not all codecs support identical ranges of packetization, the UE should ensure that the packetization derived by "a=maxprate" (or "a=ptime" if "a=maxprate" is not available or not supported) is a valid packetization time for each codec specified in the list.

If the media line in the SDP message body indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890 [152].

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213 [13C].

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

If an in-band DTMF codec is supported by the application associated with an audio media stream, then the UE shall include, in addition to the payload type numbers associated with the audio codecs for the media stream, a payload type number associated with the MIME subtype "telephone-event", to indicate support of in-band DTMF as described in RFC 4733 [23].

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

In case of UE initiated resource reservation and if the UE determines resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 3: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

In order to fulfil the QoS requirements of one or more media streams, the UE may re-use previously reserved resources. In this case the UE shall indicate as met the local preconditions related to the media stream, for which resources are re-used.

If the SDP is affected due to a rejected IP-CAN bearer, a modified IP-CAN bearer or a released IP-CAN bearer then the UE shall:

1) update the session according to RFC 3261 [26] and RFC 3311 [29] and set the ports of the media stream(s) for which IP-CAN resource was rejected, modified or released to zero in the new SDP offer;

2) release the session according to RFC 3261 [26];

3) cancel the session setup or the session modification according to RFC 3261 [26]; or

4) reject the session setup or the session modification according to RFC 3261 [26].

NOTE 4: The UE can use one IP address for signalling (and specify it in the Contact header field) and different IP address(es) for media (and specify it in the "c=" parameter of the SDP).

If the UE wants to transport media streams with TCP and there are no specific alternative negotiation mechanisms defined for that particular application, then the UE shall support the procedures and the SDP rules specified in RFC 4145 [83].

6.1.2 Handling of SDP at the originating UE (Release 12)

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566 [39], unless the UE knows that the precondition mechanism is supported by the remote UE.

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

If the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in the SDP message body.

~~If t~~The UE *shall* indicate~~d~~ support for end-to-access-edge media security using SDES during registration, and the P-CSCF indicated support for end-to-access-edge media security using SDES during registration, then upon generating an SDP offer with an RTP based media, for each RTP based media except those for which the UE requests an end-to-end media security mechanism, the UE shall:

- offer SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C] *(See ANNEX A of this document);*
- include the SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C] *(The used cipher Suits are shown in Section 3.2 within this document.)* ; and
- include an SDP "a=3ge2ae:requested" attribute.

If the UE indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an MSRP based media, for each MSRP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP "a=3ge2ae:requested" attribute.

NOTE 3: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an BFCP based media, for each BFCP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP "a=3ge2ae:requested" attribute.

If the UE indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, then upon generating an SDP offer with an UDPTL based media, for each UDPTL based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer UDPTL over DTLS transport protocol according to draft-ietf-mmusic-udptl-dtls [217] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP "a=3ge2ae:requested" attribute.

If the P-CSCF did not indicate support for end-to-access-edge media security using SDES during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any RTP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any MSRP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any BFCP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any UDPTL based media in any SDP offer.

The UE shall not include an SDP "a=3ge2ae:requested" attribute in any media other than RTP based, MSRP based, BFCP based and UDPTL based in any SDP offer.

Deutsche Telekom Note: End-to-end media security for MSRP is currently not used in the Deutsche Telekom network.

Upon generating an SDP offer with an MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

NOTE 3: SDP fingerprint attribute is not included.

Upon receiving an SDP answer to the SDP offer with the MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, and if the MSRP based media is accepted and associated with the SDP key-mgmt attribute as described in RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C] in the SDP answer, then the UE indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

When the UE detects that an emergency call is being made, the UE shall not include end-to-end media security on any media in the SDP offer.

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the SDP offer shall contain a subset of the allowed media types, codecs and other parameters from the SDP message bodies of all 488 (Not Acceptable Here) responses so far received for the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). For each media line, the UE shall order the codecs in the SDP offer according to the order of the codecs in the SDP message bodies of the 488 (Not Acceptable Here) responses.

NOTE 4: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP message bodies of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create an SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64]; and
- *if* the media streams *were* previously set to inactive mode *then they* are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec per media stream, excluding the in-band DTMF codec, as described in subclause 6.1.1, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

If the UE sends an initial INVITE request that includes only an IPv6 address in the SDP offer, and receives an error response (e.g., 488 (Not Acceptable Here) with 301 Warning header field) indicating "incompatible network address format", the UE shall send an ACK as per standard SIP procedures. Subsequently, the UE may acquire an IPv4 address or use an existing IPv4 address, and send a new initial INVITE request to the same destination containing only the IPv4 address in the SDP offer.

For the terminating UE (Section 6.1.3 1 TR 114 ANNEX B) shall be replaced with the following text out of 3GPP TS 24.229 Release 12:

General: end-to-end media security is NOT required, thus the related procedures are not valid to be implemented.

MSRP using TLS, BFCP using TLS, UDPTL using DTLS are not part of this Amendment. These features are marked as brown ***and NOT underlined text may be implemented as an option. Such features if implemented must be configurable and are deactivated per default. Such features (MSRP using TLS, BFCP using TLS, UDPTL using DTLS) are NOT supported by the Deutsche Telekom network.***

Preconditions are not used within the Deutsche Telekom network. For further information please see 1TR114 Amendment 3. This text is also marked as blue text

6.1.3 Handling of SDP at the terminating UE

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to:
  - active mode, if the offered media streams were not listed as inactive; or
  - inactive mode, if the offered media streams were listed as inactive.

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, the UE shall set the media streams to active mode by applying the procedures described in RFC 4566 [39] with respect to setting the direction of media streams.

Upon sending a SDP answer to an SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per media line and indicate only the selected codec for the related media stream. In addition, the UE may indicate support of the in-band DTMF codec, as described in subclause 6.1.1.

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 1: If the terminating UE does not support the precondition mechanism it will ignore any precondition information received from the originating UE.

Upon receiving an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, the UE shall respond with the 488 (Not Acceptable Here) response with 301 Warning header field indicating "incompatible network address format".

NOTE 2: Upon receiving an initial INVITE request that does not include an SDP offer, the UE can accept the request and include an SDP offer in the first reliable response. The SDP offer will reflect the called user's terminal capabilities and user preferences for the session.

If the UE receives an SDP offer that specifies different IP address type for media (i.e. specify it in the "c=" parameter of the SDP offer) that the UE is using for signalling, and if the UE supports both IPv4 and IPv6 addresses simultaneously, the UE shall accept the received SDP offer. Subsequently, the UE shall either acquire an IP address type or use an existing IP address type as specified in the SDP offer, and include it in the "c=" parameter in the SDP answer.

NOTE 3: Upon receiving an initial INVITE request, that includes an SDP offer containing connection addresses (in the "c=" parameter) equal to zero, the UE will select the media streams that is willing to accept for the session, reserve the QoS resources for accepted media streams, and include its valid connection address in the SDP answer.

~~If t~~The UE ***shall*** support~~s~~ the end-to-access-edge media security using SDES, upon receiving an SDP offer containing an RTP based media:

- transported using the SRTP transport protocol as defined in RFC 3711 [169];
- with an SDP crypto attribute as defined in RFC 4568 [168]; and
- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the RTP based media, then the UE shall generate the SDP answer with the related RTP based media:

- transported using the SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C]; *(See ANNEX A of this document);* and
- including an SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C] *(See ANNEX C of this document)*.

If the UE supports the end-to-access-edge media security for MSRP using TLS and certificate fingerprints, upon receiving an SDP offer containing an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214];
- with the SDP fingerprint attribute as defined in RFC 4572 [216]; and
- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the MSRP based media, then the UE shall generate the SDP answer with the related MSRP based media:

- transported using the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and
- including the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C].

NOTE 4: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE supports the end-to-access-edge media security for BFCP using TLS and certificate fingerprints, upon receiving an SDP offer containing an BFCP based media:

- transported using the BFCP over TLS transport protocol as defined in RFC 4583 [108];
- with the SDP fingerprint attribute as defined in RFC 4572 [216]; and
- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the BFCP based media, then the UE shall generate the SDP answer with the related BFCP based media:

- transported using the BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C]; and
- including the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C].

If the UE supports the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints, upon receiving an SDP offer containing an UDPTL based media:

- transported using the UDPTL over DTLS transport protocol as defined in draft-ietf-mmusic-udptl-dtls [217];
- with the SDP fingerprint attribute as defined in RFC 4572 [216]; and
- with the SDP "a=3ge2ae:applied" attribute;

and if the UE accepts the UDPTL based media, then the UE shall generate the SDP answer with the related UDPTL based media:

- transported using the UDPTL over DTLS transport protocol according to draft-ietf-mmusic-udptl-dtls [217] and the profile defined in 3GPP TS 33.328 [19C]; and
- including the SDP fingerprint attribute according to RFC 4572 [216] and the profile defined in 3GPP TS 33.328 [19C].

Upon receiving an SDP offer containing an MSRP based media:

- transported using the MSRP over TLS transport protocol as defined in RFC 4975 [178] and RFC 6714 [214]; and
- with the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

and if the UE accepts the MSRP based media, the UE shall:

1) generate the SDP answer with the related MSRP based media:
   a) transported using the MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and
   b) include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C]; and

   NOTE 5: SDP fingerprint attribute is not included.

2) indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1), if the desired QoS resources for one or more media streams have not been reserved at the terminating UE when constructing the SDP offer, the terminating UE shall indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment.

NOTE 6: It is out of scope of this specification which media streams are to be included in the SDP offer.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1) and if the desired QoS resources for one or more media streams are available at the terminating UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment.

If the terminating UE sends an UPDATE request to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sets the ports of the media streams to be removed from the session to zero in the new SDP offer.

Delete Section 6.2 Procedures at the P-CSCF (not relevant for 1TR114 therefore deleted)

Deletes Section 6.3 Procedures at the S-CSCF (not relevant for 1TR114 therefore deleted)

Delete Section 6.4 Procedures at the MGCF (not relevant for 1TR114 therefore deleted)

Delete Section 6.5 Procedures at the MRFC (not relevant for 1TR114 therefore deleted)

Delete Section 6.6 Procedures at the AS (not relevant for 1TR114 therefore deleted)

Delete Section 6.7 Procedures at the IMS-ALG functionality- (not relevant for 1TR114 therefore deleted)

7 Extensions within the present document

7.1 SIP methods defined within the present document

There are no SIP methods defined within the present document over and above those defined in the referenced IETF specifications.

7.2 SIP header fields defined within the present document

7.2.0 General

There are no SIP header fields defined within the present document over and above those defined in the referenced IETF specifications.

7.2.1 Void

7.2.2 Void

7.2.3 Void

7.2.4 Void

7.2.5 Void

7.2.6 Void

7.2.7 Void

7.2.8 Void

7.2.9 Void

7.2.10 Void

7.2A Extensions to SIP header fields defined within the present document

7.2A.1 Extension to WWW-Authenticate header field

7.2A.1.1 Introduction

This extension defines a new authentication parameter (auth-param) for the WWW-Authenticate header field used in a 401 (Unauthorized) response to the REGISTER request. For more information, see RFC 2617 [21] subclause 3.2.1.

7.2A.1.2 Syntax

The syntax for for auth-param is specified in table 7.2A.1.

Table 7.2A.1: Syntax of auth-param

```
auth-param      = 1#( integrity-key / cipher-key )
integrity-key   = "ik" EQUAL ik-value
cipher-key      = "ck" EQUAL ck-value
ik-value        = LDQUOT *(HEXDIG) RDQUOT
ck-value        = LDQUOT *(HEXDIG) RDQUOT
```

7.2A.1.3 Operation

This authentication parameter will be used in a 401 (Unauthorized) response in the WWW-Authenticate header field during UE authentication procedure as specified in subclause 5.4.1.

The S-CSCF appends the integrity-key parameter (directive) to the WWW.-Authenticate header field in a 401 (Unauthorized) response. The P-CSCF stores the integrity-key value and removes the integrity-key parameter from the header field prior to forwarding the response to the UE.

The S-CSCF appends the cipher-key parameter (directive) to the WWW-Authenticate header field in a 401 (Unauthorized) response. The P-CSCF removes the cipher-key parameter from the header field prior to forwarding the response to the UE. In the case ciphering is used, the P-CSCF stores the cipher-key value.

7.2A.2 Extension to Authorization header field

7.2A.2.1 Introduction

This extension defines a new auth-param for the Authorization header field used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

7.2A.2.2 Syntax

The syntax of auth-param for the Authorization header field is specified in table 7.2A.2.

Table 7.2A.2: Syntax of auth-param for Authorization header field

```
auth-param = "integrity-protected" EQUAL ("yes" / "no" / "tls-pending" / "tls-yes" / "ip-assoc-
pending" / "ip-assoc-yes") / "auth-done"
```

7.2A.2.3 Operation

This authentication parameter is inserted in the Authorization header field of all the REGISTER requests. The value of the "integrity-protected" header field parameter in the auth-param parameter is set as specified in subclause 5.2.2. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

The values in the "integrity-protected" header field field are defined as follows:

"yes": indicates that a REGISTER request received in the P-CSCF is protected using an IPsec security association and IMS AKA is used as authentication scheme.

"no": indicates that a REGISTER request received in the P-CSCF is not protected using an IPsec security association and IMS AKA is used as authentication scheme, i.e. this is an initial REGISTER request with the Authorization header field not containing a challenge response.

"tls-yes": indicates that a REGISTER request is received in the P-CSCF protected over a TLS connection and the Session ID, IP address and port for the TLS connection are already bound to a private user identity. The S-CSCF will decide whether or not to challenge such a REGISTER request based on its policy. This is used in case of SIP digest with TLS.

"tls-pending": indicates that a REGISTER request is received in the P-CSCF protected over a TLS connection and the Session ID, IP address and port for the TLS connection are not yet bound to a private user identity. The S-CSCF shall challenge such a REGISTER request if it does not contain an Authorization header field with a challenge response or if the verification of the challenge response fails. This is used in case of SIP digest with TLS.

"ip-assoc-yes": indicates that a REGISTER request received in the P-CSCF does map to an existing IP association in case SIP digest without TLS is used.

"ip-assoc-pending": indicates that a REGISTER request received in the P-CSCF does not map to an existing IP association, and does contain a challenge response in case SIP digest without TLS is used.

"auth-done": indicates that a REGISTER request is sent from an entity that is trusted and has authenticated the identities used in the REGISTER request. An example for such an entity is the MSC server enhanced for IMS centralized services. The S-CSCF shall skip authentication.

NOTE 1: In case of SIP digest with TLS is used, but the REGISTER request was not received over TLS, the P-CSCF does not include an "integrity-protected" header field parameter in the auth-param to indicate that an initial REGISTER request was not received over an existing TLS session. The S-CSCF will always challenge such a REGISTER request.

NOTE 2: In case of SIP digest without TLS is used, but the REGISTER request was not received over TLS, the P-CSCF does not include an "integrity-protected" header field parameter in the auth-param to indicate that the REGISTER request does not map to an existing IP association, and does not contain a challenge response. The S-CSCF will always challenge such a REGISTER request.

NOTE 3: The value "yes" is also used when an initial REGISTER request contains an Authorization header field with a challenge response as in this case the IPsec association is already in use, and its use by the UE implicitly authenticates the UE. This is a difference to TLS case where the use of TLS alone does not yet implicitly authenticates the UE. Hence in the TLS case, for an initial REGISTER request containing an Authorization header field with a challenge response the value "tls-pending" and not "tls-yes" is used.

7.2A.3 Tokenized-by header field parameter definition (various header fields)

7.2A.3.1 Introduction

The "tokenized-by" header field parameter is an extension parameter appended to encrypted entries in various SIP header fields as defined in subclause 5.10.4.

7.2A.3.2 Syntax

The syntax for the "tokenized-by" header field parameter is specified in table 7.2A.3:

Table 7.2A.3: Syntax of tokenized-by-param

```
rr-param =  tokenized-by-param / generic-param
via-params =  via-ttl / via-maddr
     / via-received / via-branch
     / tokenized-by-param / via-extension
tokenized-by-param = "tokenized-by" EQUAL hostname
```

The BNF for rr-param and via-params is taken from RFC 3261 [26] and modified accordingly.

7.2A.3.3 Operation

The "tokenized-by" header field parameter is appended by IBCF (THIG) after all encrypted strings within SIP header fields when network configuration hiding is active. The value of the header field parameter is the domain name of the network which encrypts the information.

7.2A.4 P-Access-Network-Info header field

7.2A.4.1 Introduction

The P-Access-Network-Info header field is extended to include specific information relating to particular access technologies.

7.2A.4.2 Syntax

The syntax of the P-Access-Network-Info header field is described in RFC 3455 [52]. There are additional coding rules for this header field depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.2A.4 describes the 3GPP-specific extended syntax of the P-Access-Network-Info header field defined in RFC 3455 [52].

Table 7.2A.4: Syntax of extended P-Access-Network-Info header field

```
P-Access-Network-Info  = "P-Access-Network-Info" HCOLON
         access-net-spec *(COMMA access-net-spec)
access-net-spec    = (access-type / access-class) *(SEMI access-info)
access-type    = "IEEE-802.11" / "IEEE-802.11a" / "IEEE-802.11b" / "IEEE-802.11g" / "IEEE-802.11n"
                           / "3GPP-GERAN" / "3GPP-UTRAN-FDD" / "3GPP-UTRAN-TDD" / "3GPP-E-UTRAN-
                           FDD" / "3GPP-E-UTRAN-TDD" / "ADSL" / "ADSL2" / "ADSL2+" / "RADSL" /
                           "SDSL" / "HDSL" / "HDSL2" / "G.SHDSL" / "VDSL" / "IDSL" / "3GPP2-1X" /
                           "3GPP2-1X-Femto" / "3GPP2-1X-HRPD" / "3GPP2-UMB" / "DOCSIS" / "IEEE-
                           802.3" / "IEEE-802.3a" / "IEEE-802.3e" / "IEEE-802.3i" / "IEEE-802.3j" /
                           "IEEE-802.3u" / "IEEE-802.3ab"/ "IEEE-802.3ae" / "IEEE-802.3ah" / "IEEE-
                           802.3ak" / "IEEE-802.3aq" / "IEEE-802.3an" / "IEEE-802.3y" / "IEEE-
                           802.3z" / GPON/ XGPON1 / "GSTN"/ "DVB-RCS2"/ token
...access-class     = "3GPP-GERAN" / "3GPP-UTRAN" / "3GPP-E-UTRAN" / "3GPP-WLAN" / "3GPP-GAN" /
                           "3GPP-HSPA" / "3GPP2" / token
np       = "network-provided"
access-info    = cgi-3gpp / utran-cell-id-3gpp / dsl-location / i-wlan-node-id / ci-3gpp2 / ci-
                           3gpp2-femto / eth-location / fiber-location / np/ gstn-location / local-
                           time-zone / dvb-rcs2-node-id / extension-access-info
extension-access-info  = generic-param
cgi-3gpp     = "cgi-3gpp" EQUAL (token / quoted-string)
utran-cell-id-3gpp   = "utran-cell-id-3gpp" EQUAL (token / quoted-string)
i-wlan-node-id   = "i-wlan-node-id" EQUAL (token / quoted-string)
dsl-location     = "dsl-location" EQUAL (token / quoted-string)
eth-location     = "eth-location" EQUAL (token / quoted-string)
fiber-location   = "fiber-location" EQUAL (token / quoted-string)
ci-3gpp2     = "ci-3gpp2" EQUAL (token / quoted-string)
ci-3gpp2-femto   = "ci-3gpp2-femto" EQUAL (token / quoted-string)
gstn-location    = "gstn-location" EQUAL (token / quoted-string)
dvb-rcs2-node-id   = "dvb-rcs2-node-id" EQUAL quoted-string
local-time-zone    = "local-time-zone" EQUAL (token / quoted-string)
```

The presence of the "np" parameter indicates a P-Access-Network-Info header field is provided by the P-CSCF, S-CSCF, the AS, the MSC server enhanced for ICS or by the MGCF. The content can differ from a P-Access-Network-Info header field without this parameter which is provided by the UE.

The "np" parameter can be used with both "access-type" and "access-class" constructs. The "access-type" construct is provided for use where the value is not known to be specific to a particular "access-class" value, e.g. in the case of some values delivered from the PCRF. The "access-class" field can be set only by the P-CSCF. The "np" parameter can be set only by the P-CSCF, S-CSCF, the AS, the MSC server enhanced for ICS or by the MGCF. The "local-time-zone" parameter, the "gstn-location" parameter and the "GSTN" value of access-type field shall not be inserted by the UE.

The "local-time-zone" parameter indicates the time difference between local time and UTC of day. For 3GPP accesses, the "local-time-zone" parameter represents the time zone allocated to the routing area or traffic area which the UE is currently using. As the edge of such areas may overlap, there can be some discrepancy with the actual time zone of the UE where the UE is in the near proximity to a time zone boundary.

7.2A.4.3 Additional coding rules for P-Access-Network-Info header field

The P-Access-Network-Info header field is populated with the following contents:

1) the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "3GPP2-1X-Femto", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", or "DOCSIS", "IEEE-802.3", "IEEE-802.3a", "IEEE-802.3e", "IEEE-802.3i", "IEEE-802.3j", "IEEE-802.3u", or "IEEE-802.3ab", "IEEE-802.3ae", "IEEE-802.3ah", "IEEE-802.3ak", "IEEE-802.3aq", "IEEE-802.3an", "IEEE-802.3y", "IEEE-802.3z" or "DVB-RCS2" as appropriate to the access technology in use.

2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);

3) if the access type field is equal to "3GPP-UTRAN-FDD", or "3GPP-UTRAN-TDD", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits using a full hexadecimal representation);

4) void

5) if the access type field is set to "3GPP2-1X", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of SID (16 bits), NID (16 bits), PZID (8 bits) and BASE_ID (16 bits) (see 3GPP2 C.S0005-D [85]) in the specified order. The length of the ci-3gpp2 parameter shall be 14 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters. If the UE does not know the values for any of the above parameters, the UE shall use the value of 0 for that parameter. For example, if the SID is unknown, the UE shall represent the SID as 0x0000;

NOTE 1: The SID value is represented using 16 bits as supposed to 15 bits as specified in 3GPP2 C.S0005-D [85].

EXAMPLE: If SID = 0x1234, NID = 0x5678, PZID = 0x12, BASE_ID = 0xFFFF, the ci-3gpp2 value is set to the string "1234567812FFFF".

6) if the access type field is set to "3GPP2-1X-HRPD", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of Sector ID (128 bits) and Subnet length (8 bits) (see 3GPP2 C.S0024-B [86]) and Carrier-ID, if available, (see 3GPP2 X.S0060 [86B])in the specified order. The length of the ci-3gpp2 parameter shall be 34 or 40 hexadecimal characters depending on whether the Carrier-ID is included. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters;

EXAMPLE: If the Sector ID = 0x12341234123412341234123412341234, Subnet length = 0x11, and the Carrier-ID=0x555444, the ci-3gpp2 value is set to the string "12341234123412341234123412341234123411555444".

7) if the access type field is set to "3GPP2-UMB" 3GPP2 C.S0084-000 [86A], a ci-3gpp2 parameter is set to the ASCII representation of the hexadecimal value of the Sector ID (128 bits) defined in 3GPP2 C.S0084-000 [86A]. The length of the ci-3gpp2 parameter shall be 32 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters;

EXAMPLE: If the Sector ID = 0x12341234123412341234123412341234, the ci-3gpp2 value is set to the string "12341234123412341234123412341234".

8) if the access-type field set to one of "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" or "IEEE-802.11g", or "IEEE-802.11n", an "i-wlan-node-id" parameter is set to the ASCII representation of the hexadecimal value of the AP's MAC address without any delimiting characters;

EXAMPLE: If the AP's MAC address = 00-0C-F1-12-60-28, then i-wlan-node-id is set to the string "000cf1126028".

9) if the access type field is set to "3GPP2-1X-Femto", a ci-3gpp2-femto parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of femto MSCID (24 bit), femto CellID (16 bit), FEID (64bit), macro MSCID (24 bits) and macro CellID (16 bits) (3GPP2 X.P0059-200 [86E]) in the specified order. The length of the ci-3gpp2-femto parameter is 36 hexadecimal characters. The hexadecimal characters (A through F) are coded using the uppercase ASCII characters.

10) if the access-type field is set to one of "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", the access-info field shall contain a dsl-location parameter obtained from the CLF (see NASS functional architecture);

11) if the access-type field set to "DOCSIS", the access info parameter is not inserted. This release of this specification does not define values for use in this parameter;

12) if the access type field is equal to "3GPP-E-UTRAN-FDD" or "3GPP-E-UTRAN-TDD", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, Tracking Area Code as described in 3GPP TS 23.003 [3] and the E-UTRAN Cell Identity (ECI) as described in 3GPP TS 23.003 [3], obtained from lower layers of the UE, and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), Tracking Area Code (fixed length code of 16 bits using full hexadecimal representation) and ECI (fixed length code of 28 bits using a full hexadecimal representation);

13) if the access-type field is set to one of "IEEE-802.3", "IEEE-802.3a", "IEEE-802.3e", "IEEE-802.3i", "IEEE-802.3j", "IEEE-802.3u", "IEEE-802.3ab", "IEEE-802.3ae", IEEE-802.3ak", IEEE-802.3aq", IEEE-802.3an", "IEEE-802.3y" or "IEEE-802.3z" and NASS subsystem is used, the access-info field shall contain an eth-location parameter obtained from the CLF (see NASS functional architecture);

14) if the access-type field is set to one of "GPON", "XGPON1" or "IEEE-802.3ah" and NASS is used, the access-info field shall contain an fiber-location parameter obtained from the CLF (see NASS functional architecture);

15) if the access-type field is set to "GSTN", the access-info field may contain a gstn-location parameter if received from the GSTN; and

NOTE 2: The "cgi-3gpp", the "utran-cell-id-3gpp", the "ci-3gpp2", the "ci-3gpp2-femto", the "i-wlan-node-id", eth-location, and the "dsl-location" parameters described above among other usage also constitute the location identifiers that are used for emergency services.

16) if the access-type field is set to "DVB-RCS2", the access-info field shall contain a "dvb-rcs2-node-id" parameter which consists of comma-separated list consisting of NCC_ID, satellite_ID, beam_ID, and SVN-MAC as specified in ETSI TS 101 545-2 [194], ETSI TS 101 545-3 [195]; the NCC_ID shall be represented as two digit hexadecimal value, the satellite_ID shall be represented as a two digit hexadecimal value, the beam_ID shall be respresented as a four digit hexadecimal value, and the SVN-MAC shall be represented as six digit hexadecimal value.

EXAMPLE: If the (8 bit) NCC_ID = 0x3A, the (8 bit) satellite_ID = 0xF5, the (16 bit) beam_ID = 0xEA23, and the (24 bit) SVN-MAC = 0xE40AB9, then the "dvb-rcs2-node-id" is set to the string "3A,F5,EA23,E40AB9".

17) the local-time-zone-parameter in access-info field is coded as a text string as follows:

UTC±[hh]:[mm]. [hh] is two digits from 00 to 13, and [mm] is two digits from four values : "00", "15", "30" or "45", see ISO 8601 [203].

EXAMPLE: "UTC+1:00" indicates that the time difference between local time and UTC of day is one hour.

Delete Section 7.2A.5 P-Charging-Vector header field

Delete Section 7.2A.5.2.2 GPRS as IP-CAN

Delete Section 7.2A.5.2.3 I-WLAN as IP-CAN

7.2A.5.2.4 xDSL as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. The access-network-charging-info parameter includes alternative definitions for different types of access networks. This subclause defines the components of the xDSL instance of the access-network-charging-info.

For xDSL, there are the following components to track: BRAS address (bras parameter), media authorization token (auth-token parameter), and a set of dsl-bearer-info parameters that contains the information for one or more xDSL bearers.

The dsl-bearer-info contains one or more dsl-bearer-item values followed by a collection of parameters (dsl-bearer-sig, dslcid, and flow-id). The value of the dsl-bearer-item is a unique number that identifies each of the dsl-bearer-related charging information within the P-Charging-Vector header field. Each dsl-bearer-info has an indicator if it is an IM CN subsystem signalling dsl-bearer (dsl-bearer-sig parameter), an associated DSL Charging Identifier (dslcid parameter),

and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the dsl-bearer charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.214 [13D].

The format of the dslcid parameter is identical to that of ggsn parameter. On receipt of this header field, a node receiving a dslcid shall decode from hexadecimal into binary format.

For a dedicated dsl-bearer for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Rx and Gx interfaces. Since there are no dslcid, media authorization token or flow identifiers in this case, the dslcid and media authorization token are set to zero and no flow identifier parameters are constructed by the PCRF.

Delete Section 7.2A.5.2.5 DOCSIS as IP-CAN-

Delete Section 7.2A.5.2.6 cdma2000® packet data subsystem as IP-CAN

Delete Section 7.2A.5.2.7 EPS as IP-CAN

7.2A.5.2.8 Ethernet as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. For Ethernet accesses, the IP Edge Node address (ip-edge parameter) is tracked. The IP Edge Node is defined in ETSI ES 282 001 [138].

7.2A.5.2.9 Fiber as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. For Fiber accesses, the IP Edge Node address (ip-edge parameter) is tracked. The IP Edge Node is defined in ETSI ES 282 001 [138].

7.2A.5.3 Operation

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

7.2A.6 Orig parameter definition

7.2A.6.1 Introduction

The "orig" parameter is a uri-parameter intended to:

- tell the S-CSCF that it has to perform the originating services instead of terminating services;
- tell the I-CSCF that it has to perform originating procedures.

7.2A.6.2 Syntax

The syntax for the orig parameter is specified in table 7.2A.6:

Table 7.2A.6: Syntax of orig parameter

```
uri-parameter = transport-param / user-param / method-param / ttl-param / maddr-param / lr-param /
    orig / other-param
orig = "orig"
```

The BNF for uri-parameter is taken from RFC 3261 [26] and modified accordingly.

7.2A.6.3 Operation

The orig parameter is appended to the address of the S-CSCF, I-CSCF or IBCF by the ASs, when those initiate requests on behalf of the user, or to the address of the S-CSCF or I-CSCF by an IBCF acting as entry point, if the network is performing originating service to another network. The S-CSCF will run originating services whenever the orig parameter is present next to its address. The I-CSCF will run originating procedures whenever the orig parameter is present next to its address. The IBCF will preserve the "orig" parameter in the topmost Route header field if received, or it may append the "orig" parameter to the URI in the topmost Route header field (see subclause 5.10.2.3).

7.2A.7 Extension to Security-Client, Security-Server and Security-Verify header fields

7.2A.7.1 Introduction

This extension defines new paramerts for the Security-Client, Security-Server and Security-Verify header fields.

This subclause defines the "mediasec" header field parameter that labels any of the Security-Client:, Security-Server, or Security-Verify: header fields as applicable to the media plane and not the signalling plane.

7.2A.7.2 Syntax

7.2A.7.2.1 General

The syntax for the Security-Client, Security-Server and Security-Verify header fields is defined in RFC 3329 [48]. The additional syntax is defined in Annex H of 3GPP TS 33.203 [19].

This specification reuses Security-Client, Security-Server and Security-Verify defined in RFC 3329 [48] and defines the mechanism-name "sdes-srtp" and the header field parameter "mediasec".

Security mechanisms that apply to the media plane only shall not have the same name as any signalling plane mechanism. If a signalling plane security mechanism name is re-used for the media plane and distinguished only by the "mediasec" parameter, then implementations that do not recognize the "mediasec" parameter may incorrectly use that security mechanism for the signalling plane.

7.2A.7.2.2 "mediasec" header field parameter

The "mediasec" header field parameter may be used in the Security- Client, Security-Server, or Security-Verify header fields defined in RFC 3329 [48] to indicate that a header field applies to the media plane. Any one of the media plane security mechanisms supported by both client and server, if any, may be applied when a media stream is started. Or, a media stream may be set up without security.

Values in the Security-Client, Security-Server, or Security-Verfiy header fields labelled with the "mediasec" header field parameter are specfic to the media plane and specific to the secure media transport protocol used on the media plane.

Syntax of mediasec header field parameter is:

```
mediasec = mechanism-name

mechanism-name = ( "sdes-srtp" / token )
```

The parameters described by the BNF above have the following semantics:

sdes-srtp: SDES security mechanism for SRTP applied end to access edge.

7.2A.7.3 Operation

The operation of the additional parameters for the Security-Client, Security-Server and Security-Verify header fields is defined in Annex H of 3GPP TS 33.203 [19].

Any one of the mechanisms labelled with the "mediasec" header field parameter can be applied on-the-fly as a media stream is started, unlike mechanisms for signalling one of which is chosen and then applied throughout a session.

Media plane security can be supported independently of any signalling plane security defined in RFC 3329 [4], but in order to protect any cryptographic key carried in SDP signalling plane security as defined in RFC 3329 [4] SHOULD be used.

The message flow is identical to the flow in RFC 3329 [48], but it is not mandatory for the user agent to apply media plane security immediately after it receives the list of supported media plane mechanisms from the server, or any timer after that, nor will the lack of a mutually supported media plane security mechanism prevent SIP session setup.

7.2A.7.4 IANA registration

7.2A.7.4.1 "mediasec" header field parameter

Editor's note: [MEDIASEC_CORE, CR 4156] This subclause forms the basis for IANA registration of the mediasec header field parameter. Registration is intended to be created by an RFC that describes the mediasec header field parameter and creates an IANA registry for its values.

NOTE: This subclause contains information to be provided to IANA for the registration of the media plane security indicator header field parameter.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Header field parameter name (as it will appear in SIP)

mediasec

Long-form Attribute Name in English:

3GPP_media plane security mechanism indicator

Type of Attribute

Header field parameter applicable to Security-Client, Security-Server, and Security-Verify header field parameters defined in RFC 3329 [48].

Purpose of the header field parameter:

This attribute specifies the end-to-access-edge security-indicator as used for IMS media plane security

Appropriate Attribute Values for this header field parameter:

The value "mediasec" is defined.

7.2A.7.4.2 "sdes-srtp" security mechanism

Editor's note: [MEDIASEC_CORE, CR 4156] This subclause forms the basis for IANA registration of the value for the mediasec header field parameter. The registration should be performed by MCC when the registry for mediasec parameter values has been created by IANA.

NOTE: This subclause contains information to be provided to IANA for the registration of the media plane security indicator header field parameter.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Mechanism name (as it will appear in SIP)

sdes-srtp

Long-form Attribute Name in English:

3GPP media plane security mechanism name sdes-srtp for using SDES with SRTP

Type of Attribute

Mechanism name applicable to Security-Client, Security-Server, and Security-Verify header fields defined in RFC 3329 [48].

Purpose of the mechanism name:

This specification adds one value to the list of security mechanism names in RFC 3329 [48].This mechanism name specifies that SDES with SRTP (see RFC 4568 [168]) is supported for IMS media plane security.

Appropriate values for this mechanism name:

The value " sdes-srtp " is defined.

7.2A.8 IMS Communication Service Identifier (ICSI)

7.2A.8.1 Introduction

The ICSI is defined to fulfil the requirements as stated in 3GPP TS 23.228 [7]. An ICSI may have specialisations which refine it by adding subclass identifiers separated by dots. Any specialisations of an ICSI shall have an "is a" relationship if the subclasses are removed. For example, a check for ICSI urn:urn-7:3gpp-service.ims.icsi.mmtel will return true when evaluating ICSI urn:urn-7:3gpp-service.ims.icsi.mmtel.hd-video.

7.2A.8.2 Coding of the ICSI

This parameter is coded as a URN. The ICSI URN may be included as:

- a tag-value within the g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62], in which case those characters of the URN that are not part of the tag-value definition in RFC 3840 [62] shall be represented in the percent encoding as defined in RFC 3986 [124];
- a feature cap value within the "g.3gpp.icsi-ref" feature cap, as defined in subclause 7.9A.1 and draft-ietf-sipcore-proxy-feature [190], in which case those characters of the URN that are not part of the feature cap value definition syntax shall be represented in the percent encoding, as defined in RFC 3986 [124]; or
- as a value of the P-Preferred-Service or P-Asserted-Service header fields as defined RFC 6050 [121].

A list of the URNs containing ICSI values registered by 3GPP can be found at http://www.3gpp.com/Uniform-Resource-Name-URN-list.html

An example of an ICSI for a 3GPP defined IMS communication service is:

```
urn:urn-7:3gpp-service.ims.icsi.mmtel
```

An example of a g.3gpp.icsi-ref media feature tag containing an ICSI for a 3GPP defined IMS communication service is:

```
g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
```

An example of a g.3gpp.icsi-ref feature cap containing an ICSI for a 3GPP defined IMS communication service is:

```
g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
```

An example of an ICSI for a 3GPP defined IMS communication service in a P-Preferred-Service header field is

```
P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
```

An example of an ICSI for a 3GPP defined IMS communication service in a P-Asserted-Service header field is

```
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
```

An example of an ICSI for a defined IMS communication service with a specialisation is:

```
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel.game-v1
```

An example of an ICSI for a 3GPP defined IMS communication service with an organisation-y defined specialisation is:

```
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel.organisation-y.game-v2
```

Editor's note: [TEI11] [CR# 3855] The consequences of the use of ICSI sub-classes within the Contact and Accept-Contact header fields are FFS.

7.2A.9 IMS Application Reference Identifier (IARI)

7.2A.9.1 Introduction

The IARI is defined to fulfil the requirements as stated in 3GPP TS 23.228 [7].

7.2A.9.2 Coding of the IARI

This parameter is coded as a URN. The IARI URN may be included as a tag-value within the g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62], in which case those characters of the URN that are not part of the tag-value definition in RFC 3840 [62] shall be represented in the percent encoding as defined in RFC 3986 [124].

A list of the URNs containing IARI values registered by 3GPP can be found at http://www.3gpp.com/Uniform-Resource-Name-URN-list.html

An example of a g.3gpp.iari-ref media feature tag containing an IARI is:

```
g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.game-v1"
```

7.2A.10 "phone-context" tel URI parameter

7.2A.10.1 Introduction

The "phone-context" tel URI parameter indicates that the UE uses local service number or that the UE has included information according to a local dialling plan in the Request-URI.

In the former case, the "phone-context" tel URI parameter is included in a Tel-URI or a corresponding SIP URI with a "user" SIP URI parameter set to "phone".

In the latter case, the "phone-context" tel URI parameter is included in the user part of a SIP URI with the "user" SIP URI parameter set to "dialstring" (see RFC 4967 [103]).

7.2A.10.2 Syntax

The syntax of the "phone-context" tel URI parameter is described in RFC 3966 [22]. There are additional coding rules for this parameter depending on the type of IP-CAN, according to access technology specific descriptions.

7.2A.10.3 Additional coding rules for "phone-context" tel URI parameter

In case the current IP-CAN is indicated in the "phone-context" tel URI parameter, the entities inserting the "phone-context" tel URI parameter shall populate the "phone-context" tel URI parameter with the following contents:

~~*1) if the IP-CAN is GPRS, then the "phone-context" tel URI parameter is a domain name. It is constructed from the MCC, the MNC and the home network domain name by concatenating the MCC, MNC, and the string "gprs" as domain labels before the home network domain name;*~~

~~*EXAMPLE: If MCC = 216, MNC = 01, then the "phone-context" tel URI parameter is set to '216.01.gprs.home1.net'.*~~

~~*2) if the IP-CAN is I-WLAN, then the "phone-context" tel URI parameter is a domain name. It is constructed from the SSID, AP's MAC address, and the home network domain name by concatenating the SSID, AP's MAC address, and the string "i-wlan" as domain labels before the home network domain name;*~~

~~*EXAMPLE: If SSID = BU-Airport, AP's MAC = 00-0C-F1-12-60-28, and home network domain name is "home1.net", then the "phone-context" tel URI parameter is set to the string "bu-airport.000cf1126028.i-wlan.home1.net".*~~

3) if the IP-CAN is xDSL, then the "phone-context" tel URI parameter is a domain name. It is constructed from the dsl-location (see subclause 7.2A.4) and the home network domain name by concatenating the dsl-location and the string "xdsl" as domain labels before the home network domain name;

~~*4) if the IP-CAN is DOCSIS, then the "phone-context" tel URI parameter is based on data configured locally in the UE;*~~

~~*5) if the IP-CAN is EPS, then the "phone-context" tel URI parameter is a domain name. It is constructed from the MCC, the MNC and the home network domain name by concatenating the MCC, MNC, and the string "eps" as domain labels before the home network domain name;*~~

~~*6) if the IP-CAN is Ethernet, then the "phone-context" parameter is a domain name. It is constructed from the eth-location (see subclause 7.2A.4) and the home network domain name by concatenating the eth-location and the string "ethernet" as domain labels before the home network domain name;*~~

~~*7) if the IP-CAN is Fiber, then the "phone-context" parameter is a domain name. It is constructed from the fiber-location (see subclause 7.2A.4) and the home network domain name by concatenating the fiber-location and the string "fiber" as domain labels before the home network domain name;*~~

~~*8) if the IP-CAN is cdma2000®, then the "phone-context" parameter is a domain name. It is constructed from the subnet id and the home network domain name by concatenating the subnet id as the domain label before the home network domain name;*~~

~~*9) if the IP-CAN is DVB-RCS2, then the "phone-context" tel URI parameter is based on data configured locally in the UE; and*~~

10) if the access network information is not available in the UE, then the "phone-context" tel URI parameter is set to the home network domain name preceded by the string "geo-local.".

In case the home domain is indicated in the "phone-context" tel URI parameter, the "phone-context" tel URI parameter is set to the home network domain name (as it is used to address the SIP REGISTER request, see subclause 5.1.1.1A or subclause 5.1.1.1B).

In case the "phone-context" tel URI parameter indicates a network other than the home network or the visited access network, the "phone-context" tel URI parameter is set according to RFC 3966 [22].

7.2A.11 Void

7.2A.11.1 Void

7.2A.11.2 Void

7.2A.11.3 Void

7.2A.12 CPC and OLI tel URI parameter definition

7.2A.12.1 Introduction

The use of the "cpc" and "oli" URI parameters for use in the P-Asserted-Identity in SIP requests is defined.

7.2A.12.2 Syntax

The Calling Party's Category and Originating Line Information are represented as URI parameters for the tel URI scheme and SIP URI representation of telephone numbers. The ABNF syntax is as follows and extends the formal syntax for the tel URI as specified in RFC 3966 [22]:

Table 7.2A.7

```
par =/ cpc / oli
cpc = cpc-tag "=" cpc-value
oli = oli-tag "=" oli-value
cpc-tag = "cpc"
oli-tag = "oli"
cpc-value
= "ordinary" / "test" / "operator" /
"payphone" / "unknown" / "mobile-hplmn" / "mobile-vplmn" / "emergency" /
genvalue
oli-value = 2*(DIGIT)
genvalue = 1*(alphanum / "-" / "." )
```

The Accept-Language header field shall be used to express the language of the operator.

The semantics of these Calling Party's Category values are described below:

ordinary: The caller has been identified, and has no special features.

test: This is a test call that has been originated as part of a maintenance procedure.

operator: The call was generated by an operator position.

payphone: The calling station is a payphone.

unknown: The CPC could not be ascertained.

mobile-hplmn: The call was generated by a mobile device in its home PLMN.

mobile-vplmn: The call was generated by a mobile device in a vistited PLMN.

emergency: The call is an emergency service call.

NOTE 1: The choice of CPC and OLI values and their use are up to the Service Provider. CPC and OLI values can be exchanged across networks if specified in a bilateral agreement between the service providers.

NOTE 2: Additional national/regional CPC values can exist.

The two digit OLI values are decimal codes assigned and administered by North American Numbering Plan Administration.

7.2A.12.3 Operation

The "cpc" and "oli" URI parameters may be supported by IM CN subsystem entities that provide the UA role and by IM CN subsystem entities that provide the proxy role.

The "cpc" and "oli" URI parameters shall not be populated at the originating UE.

Unless otherwise specified in this document, "cpc" and "oli" URI parameters are only passed on by IM CN subsystem entities (subject to trust domain considerations as specified in subclause 4.4.12).

7.2A.13 "sos" SIP URI parameter

7.2A.13.1 Introduction

The "sos" SIP URI parameter is intended to:

- indicate to the S-CSCF that a REGISTER request that includes the "sos" SIP URI parameter is for emergency registration purposes;

- tell the S-CSCF to not apply barring of the public user identity being registered; and
- tell the S-CSCF to not apply initial filter criteria to requests destined for an emergency registered contact.

7.2A.13.2 Syntax

The syntax for the "sos" SIP URI parameter is specified in table 7.8

Table 7.2A.8: Syntax of sos SIP URI parameter

```
uri-parameter =/ sos-param
sos-param = "sos"
```

The BNF for uri-parameter is taken from RFC 3261 [26] and modified accordingly.

7.2A.13.3 Operation

When a UE includes the "sos" SIP URI parameter in the URI included in the Contact header field of REGISTER request, the REGISTER request is intended for emergency registration.

When a S-CSCF receives a REGISTER request for emergency registration that includes the "sos" SIP URI parameter, the S-CSCF is required to preserve the previously registered contact address. This differs to the registrar operation as defined in RFC 3261 [26] in that the rules for URI comparison for the Contact header field shall not apply and thus, if the URI in the Contact header field matches a previously received URI, then the old contact address shall not be overwritten.

7.2A.14 P-Associated-URI header field

Procedures of RFC 3455 [52] are modified to allow a SIP proxy to remove URIs from the P-Associated-URI header field.

NOTE: Table 1 RFC 3455 [52] needs to be modified to allow a proxy to modify and read the P-Associated-URI header field.

7.2A.15 Extension to P-Served-User

7.2A.15.1 Introduction

The P-Served-User header field is extended to include the ORIG_CDIV session case.

Editor's note: [WI: IMSProtoc5, CR#3904] as per RFC 5727 an IETF expert review is needed in order to obtain the IANA registration of this extention.

7.2A.15.2 Syntax

The syntax of the P-Served-User header field is described in RFC 5502 [133].

Table 7.2A.15 describes 3GPP-specific extension to the P-Served-User header field defined in RFC 5502 [133].

Table 7.2A.15: Syntax of extension to P-Served-User header field

```
orig-cdiv-param = "orig-cdiv"
```

The orig-cdiv-param parameter is an instance of generic-param from the current served-user-param component of P-Served-User header field.

The orig-cdiv-param header field parameter may be included in the P-Served-User header field by a SIP proxy (e.g. S-CSCF) to indicate that the SIP request was initially destined to the served user and has been retargeted to another

destination. This indication can be used by the receiving Application Server of the served user to determine the appropriate services to be applied to this served user.

7.2A.15.3 IANA registration

NOTE: This subclause contains information to be provided to IANA for the registration of the orig-cdiv-param header field parameter of the P-Served-User header field.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Header field parameter name (as it will appear in SIP)

orig-cdiv

Header field name (as it will appear in SIP)

P-Served-User.

Purpose of the header field parameter:

This header field parameter indicates that the SIP request was initially destined to the served user and has been retargeted to another destination. This indication can be used by the receiving Application Server of the served user to determine the appropriate services to be applied to this served user..

Appropriate Attribute Values for this header field parameter:

None

7.3 Option-tags defined within the present document

There are no option-tags defined within the present document over and above those defined in the referenced IETF specifications.

7.4 Status-codes defined within the present document

There are no status-codes defined within the present document over and above those defined in the referenced IETF specifications.

7.5 Session description types defined within the present document

7.5.1 General

This subclause contains definitions for SDP parameters that are specific to SDP usage in the 3GPP IM CN Subsystem and therefore are not described in an RFC.

7.5.2 End-to-access-edge media plane security

Editor's note: This subclause forms the basis for IANA registration of the new SDP attribute. The registration should be performed by MCC when the MEDIASEC_CORE work item is declared 100% complete.

7.5.2.1 General

The end-to-access-edge security-indicator is used to indicate that a UE requests a P-CSCF to apply media plane security or to indicate that a P-CSCF has applied end-to-access-edge security as defined in 3GPP TS 33.328 [19C].

7.5.2.2 Syntax

3GPP end-to-access-edge media security indicator is a value attribute which is encoded as a media-level SDP attribute with the ABNF syntax defined in table 7.5.1. ABNF is defined in RFC 2234 [20G].

Table 7.5.1: ABNF syntax of 3ge2ae attribute

```
3ge2ae-attribute = "a=3ge2ae:" indicator
indicator = "requested" / "applied" / token
```

"requested": the sender indicates its wish that end-to-access-edge media security is applied.

"applied": the sender indicates that it has applied end-to-access-edge media security.

This version of the specification only defines usage of the "requested" and "applied" attribute values. Other values shall be ignored.

The "3ge2ae" attribute is charset-independent.

7.5.2.3 IANA registration (Release 12)

NOTE: This subclause contains information to be provided to IANA for the registration of the end-to-access-edge security indicator SDP attribute.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Attribute Name (as it will appear in SDP)

3ge2ae

Long-form Attribute Name in English:

3GPP_e2ae-security-indicator

Type of Attribute

Media level

Is Attribute Value subject to the Charset Attribute?

This Attribute is not dependent on charset.

Purpose of the attribute:

This attribute specifies the end-to-access-edge security-indicator as used for IMS media plane security

Appropriate Attribute Values for this Attribute:

The attribute is a value attribute. The values "requested" and "applied" are defined.

Delete Section 7.5.3 Optimal Media Routeing (OMR) attributes

7.6 3GPP IM CN subsystem XML body

7.6.1 General

This subclause contains the 3GPP IM CN Subsystem XML body in XML format. The 3GPP IM CN Subsystem XML shall be valid against the 3GPP IM CN Subsystem XML schema defined in table 7.6.1.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

See subclause 7.6.4 and subclause 7.6.5 for the associated MIME type definition.

7.6.2 Document Type Definition

The XML Schema, is defined in table 7.6.1.

Table 7.7.6.1: IM CN subsystem XML body, XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
           attributeFormDefault="unqualified" version="1">
 <xs:complexType name="tIMS3GPP">
  <xs:sequence>
   <xs:choice>
    <xs:element name="alternative-service" type="tAlternativeService"/>
    <xs:element name="service-info" type="xs:string"/>
   </xs:choice>
   <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:attribute name="version" type="xs:decimal" use="required"/>
  <xs:anyAttribute/>
 </xs:complexType>
 <xs:complexType name="tAlternativeService">
  <xs:sequence>
   <xs:element ref="type"/>
   <xs:element name="reason" type="xs:string"/>
   <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
  </xs:sequence>
  <xs:anyAttribute/>
 </xs:complexType>

 <!-- root element -->
 <xs:element name="ims-3gpp" type="tIMS3GPP"/>

 <xs:element name="type" type="xs:string"/>

 <!-- action element for //ims-3gpp//alternative-service -->
 <xs:element name="action" type="xs:string"/>

</xs:schema>
```

7.6.3 XML Schema description

This subclause describes the elements of the IM CN subsystem XML Schema as defined in table 7.6.1.

<ims-3gpp>: The <ims-3gpp> element is the root element of the IM CN subsystem XML body. It is always present. XML instance documents of future versions of the XML Schema in table 7.6.1 is valid against the XML Schema in table 7.6.1 in this document. XML instance documents of the XML Schema in table 7.6.1 in the present document have a version attribute value, part of the <ims-3gpp> element, that is equal to the value of the XML Schema version described in the present document.

<service-info>: the transparent element received from the HSS for a particular trigger point are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem or as a response to initiate S-CSCF restoration procedures. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

In the present document, the <alternative-service> element contains a <type> element, a <reason> element, and an optional <action> element.

The <type> element indicates the type of alternative service. The <type> element contains only the values specified in table 7.6.2 in the present document.

Table 7.6.2: ABNF syntax of values of the <type> element

```
emergency-value = %x65.6D.65.72.67.65.6E.63.79 ; "emergency"
restoration-value = %x72.65.73.74.6F.72.61.74.69.6F.6E ; "restoration"
```

The <action> element contains only the values specified in table 7.6.3 in the present document.

Table 7.6.3: ABNF syntax of values of the <action> element

```
emergency-registration-value = %x65.6D.65.72.67.65.6E.63.79.2D.72.65.67.69.73.74.72.61.74.69.6F.6E ;
    "emergency-registration"
initial-registration-value = %x69.6E.69.74.69.61.6C.2D.72.65.67.69.73.74.72.61.74.69.6F.6E ;
    "initial-registration"
```

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

If included in the IM CN subsystem XML body:

1. the <type> element with the value "emergency" is included as the first child element of the <alternative-service> element;

2. the <type> element with the value "restoration" is included as one of the following:

   a) the first child element of the <alternative-service> element; or

   b) the third or later child element of the <alternative-service> element;

3. the <action> element with the value "emergency-registration" is includes as the third child element of the <alternative-service> element; and

4. the <action> element with value "initial-registration" is included as the third or later child element of the <alternative-service> element.

NOTE: When included, the <action> and the second occurence of the <type> elements are validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of their parent elements.

7.6.4 MIME type definition

7.6.4.1 Introduction

This subclause defines the MIME type for "application/3gpp-ims+xml". A 3GPP IM CN subsystem XML Document can be identified with this media type.

7.6.4.2 Syntax

The following optional parameters are defined:

- "charset": the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in RFC 3023 [132].
- "sv" or "schemaversion": the syntax for the "sv" or "schemaversion" parameter is specified in table 7.6.4:

Table 7.6.4: Syntax of the "sv" or "schemaversion" parameter

```
m-parameter  =/ ("sv" / "schemaversion") EQUAL LDQUOT [ sv-value-list ] RDQUOT
sv-value-list  =  sv-value-range *( "," sv-value )
sv-value-range =  sv-value [ "-" sv-value ]
sv-value   =  number / token
number   =  1*DIGIT [ "." 1*DIGIT ]
```

The BNF for m-parameter is taken from RFC 3261 [26] and modified accordingly.

7.6.4.3 Operation

The encoding considerations for "application/3gpp-ims+xml" are identical to those of "application/xml" as described in RFC 3023 [132].

The "sv" or "schemaversion" parameter's value is used to indicate:

- the versions of the 3GPP IM CN Subsystem XML schema that can be used to validate the 3GPP IM CN subsystem XML body (if the MIME type and parameter are present in the Content-Type header field); or
- the accepted versions of the 3GPP IM CN Subsystem XML body (if the MIME type and parameter are present in the Accept header field).

If the "sv" and "schemaversion" parameter are absent, it shall be assumed that version 1 of the XML Schema for the IM CN subsystem XML body is supported.

7.6.5 IANA Registration

NOTE: RFC 4288 [xy], subclause 9, states the process that applies in case of changes to the registry of media types. Any future changes to the format or to subclause 7.6.5 would invoke this procedure.

MIME media type name:

application

MIME subtype name:

3gpp-ims+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in RFC 3023 [132].

"sv" or "schemaversion" the parameter's value is used to indicate:

- the versions of the 3GPP IP Multimedia (IM) Core Network (CN) subsystem XML schema that can be used to validate the 3GPP IM CN subsystem XML body (if the MIME type and parameter are present in the Content-Type header field); or

- the accepted versions of the 3GPP IM CN Subsystem XML body (if the MIME type and parameter are present in the Accept header field).

If the "sv" and "schemaversion" parameter are absent, it shall be assumed that version 1 of the XML Schema for the IM CN subsystem XML body is supported.

Encoding considerations:

Same as encoding considerations of application/xml as specified in RFC 3023 [132]

Security considerations:

Same as general security considerations for application/xml as specified in subclause 10 of RFC 3023 [132].

In addition, this content type provides a format for exchanging information in SIP, so the security considerations from RFC 3261 [26] apply.

Interoperability considerations:

Same as Interoperability considerations as specified in subclause 3.1 of RFC 3023 [132].

If both "sv" and "schemaversion" are specified, then the value of "schemaversion" is ignored

Published specification:

3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3", as published in subclause 7.6.5, version 8.9.0.

Available via <http://www.3gpp.org/specs/numbering.htm>.

Applications which use this media:

Applications that use the 3GPP IM CN Subsystem as defined by 3GPP.

Intended usage:

COMMON

Additional information:

1. Magic number(s): none
2. File extension(s): none
3. Macintosh file type code: none
4. Object Identifiers: none

7.7 SIP timers

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays. Table 7.7.1 shows recommended values for IM CN subsystem.

Table 7.7.1 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "value to be applied between IM CN subsystem elements" lists the values recommended for network elements e.g. P-CSCF, S-CSCF, MGCF, when communicating with each other i.e. when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "value to be applied at the UE" lists the values recommended for the UE, when in normal operation the UE generates requests or responses containing a P-Access-Network-Info header field which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2". These are modified when compared to RFC 3261 [26] to accommodate the air interface delays. In all other cases, the UE should use the values specified in RFC 3261 [26] as indicated in the second column of table 7.7.1.

The fourth column, titled "value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed, and which are used on all SIP transactions on a specific security association where the security association was established using a REGISTER request containing a P-Access-Network-Info header field provided by the UE which included a value of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2". These are modified when compared to RFC 3261 [26]. In all other cases, the P-CSCF should use the values specified in RFC 3261 [26] as indicated in the second column of table 7.7.1.

The final column reflects the timer meaning as defined in RFC 3261 [26].

Table 7.7.1: SIP timers

SIP Timer	Value to be applied between IM CN subsystem elements	Value to be applied at the UE	Value to be applied at the P-CSCF toward a UE	Meaning
T1	500ms default (see NOTE)	2s default	2s default	RTT estimate
T2	4s (see NOTE)	16s	16s	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s (see NOTE)	17s	17s	Maximum duration a message will remain in the network
Timer A	initially T1	initially T1	initially T1	INVITE request retransmit interval, for UDP only
Timer B	64*T1	64*T1	64*T1	INVITE transaction timeout timer
Timer C	> 3min	> 3 min	> 3 min	proxy INVITE transaction timeout
Timer D	> 32s for UDP	>128s	>128s	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer E	initially T1	initially T1	initially T1	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	64*T1	64*T1	non-INVITE transaction timeout timer
Timer G	initially T1	initially T1	initially T1	INVITE response retransmit interval
Timer H	64*T1	64*T1	64*T1	Wait time for ACK receipt.
Timer I	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for ACK retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer J	64*T1 for UDP	64*T1 for UDP	64*T1 for UDP	Wait time for non-INVITE request retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer K	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
NOTE: As a network option, SIP T1 Timer's value can be extended, along with the necessary modifications of T2 and T4 Timers' values, to take into account the specificities of the supported services when the MRFC and the controlling AS are under the control of the same operator and the controlling AS knows, based on local configuration, that the MRFC implements a longer value of SIP T1 Timer.				

7.8 IM CN subsystem timers

Table 7.8.1 shows recommended values for timers specific to the IM CN subsystem.

Table 7.8.1: IM CN subsystem

Timer	Value to be applied at the UE	Value to be applied at the P-CSCF	Value to be applied at the S-CSCF	Meaning
reg-await-auth	not applicable	not applicable	4 minutes	The timer is used by the S-CSCF during the authentication procedure of the UE. For detailed usage of the timer see subclause 5.4.1.2. The authentication procedure may take in the worst case as long as 2 times Timer F. The IM CN subsystem value for Timer F is 128 seconds.

NOTE: The UE and the P-CSCF use the value of the reg-await-auth timer to set the SIP level lifetime of the temporary set of security associations.

7.9 Media feature tags defined within the current document

7.9.1 General

This subclause describes the media feature tag definitions that are applicable for the 3GPP IM CN subsystem.

7.9.2 Definition of media feature tag g.3gpp.icsi-ref

Media feature-tag name: g.3gpp.icsi-ref.

ASN.1 Identifier: 1.3.6.1.8.2.4

Summary of the media feature indicated by this tag: Each value of the Service Reference media feature-tag indicates the software applications supported by the agent. The values for this tag equal the IMS communication Service Identifier (ICSI) values supported by the agent.

The Service Reference media feature tag is defined to fulfil the requirements for forking to an appropriate UE when multiple UEs are registered and dispatch to an appropriate application within the UE based upon the IMS communication Service Identifier (ICSI) values as stated in 3GPP TS 23.228 [7].

Multiple tag-values can be included in the Service Reference media feature-tag.

Values appropriate for use with this feature-tag: Token with an equality relationship.

The feature-tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms:

> This feature-tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Routeing an IMS Communication Session to a device that supports a particular software application or understands a particular service.

Related standards or documents:

> 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3"

Security Considerations: Security considerations for this media feature-tag are discussed in subclause 11.1 of RFC 3840 [62].

7.9.3 Definition of media feature tag g.3gpp.iari-ref

Media feature-tag name: g.3gpp.iari-ref.

ASN.1 Identifier: 1.3.6.1.8.2.5

Summary of the media feature indicated by this tag: Each value of the Application Reference media feature-tag indicates the software applications supported by the agent. The values for this tag equal IMS Application Reference Identifier (IARI) values supported by the agent

The Application Reference media feature tag is defined to fulfil the requirements for forking to an appropriate UE when multiple UEs are registered and dispatch to an appropriate application within the UE based upon and IMS Application Reference Identifier (IARI) values as stated in 3GPP TS 23.228 [7].

Multiple tag-values can be included in the Application Reference media feature-tag.

Values appropriate for use with this feature-tag: Token with an equality relationship.

The feature-tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms:

> This feature-tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Routeing an IMS Application Session to a device that supports a particular software application or understands a particular application.

Related standards or documents:

> 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3"

Security Considerations: Security considerations for this media feature-tag are discussed in subclause 11.1 of RFC 3840 [62].

7.9.4 Void

7.9.5 Void

7.9.6 Void

7.9A Feature capability indicators defined within the current document

7.9A.1 General

This subclause describes the feature capability indicators definitions, according to draft-ietf-sipcore-proxy-feature [190], that are applicable for the 3GPP IM CN subsystem.

7.9A.2 Definition of feature capability indicator g.3gpp.icsi-ref

Feature capability indicator name: g.3gpp.icsi-ref.

Summary of the feature indicated by this feature capability indicator: Each value of the Service Reference feature capability indicator indicates the software applications supported by the entity. The values for this feature capability indicator equal the IMS communication Service Identifier (ICSI) values supported by the entity.

Multiple feature capability indicator values can be included in the Service Reference feature capability indicators.

When included in the Feature-Caps header field, according to draft-ietf-sipcore-proxy-feature [190], the value of this feature capability indicator contains the IMS communication service identifier (ICSI) of the IMS communication service supported for use:

- in the standalone transaction (if included in a request for a standalone transaction or a response associated with it); or
- in the dialog (if included in an initial request for dialog or a response associated with it);

by the entity which included the Feature-Caps header field.

Editor's note: The feature capability indicator needs to be re-registered with IANA after draft-ietf-sipcore-proxy-feature becomes RFC.

Feature capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature capability indicator: Token with an equality relationship.

Examples of typical use: Indicating support of IMS Communication Services to other network entities.

Security Considerations: Security considerations for this feature capability indicator are discussed in clause 9 of draft-ietf-sipcore-proxy-feature [190].

7.9A.3 Definition of feature capability indicators g.3gpp.trf

Editor's note: This feature capability indicator is to be registered with IANA after draft-ietf-sipcore-proxy-feature becomes RFC

Feature capability indicator name: g.3gpp.trf

Summary of the feature indicated by this feature capability indicator:

This feature capability indicator, when included in a Feature-Caps header field as specified in draft-ietf-sipcore-proxy-feature [190] in a SIP INVITE request, indicates that in a roaming scenario, the visited network supports a transit and roaming functionality in order to allow loopback of session requests to the visited network from the home network. When used, it may indicate the URI of the transit and roaming functionality.

Feature capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature capability indicator:

None or string with an equality relationship. When used in a Feature-Caps header field, the value is string and follows the syntax as described in table 7.9A.1 for g-3gpp-trf.

Table 7.9A.1: ABNF syntax of values of the g.3gpp.trf feature capability indicator

```
g-3gpp-trf = SIP URI
```

The feature capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature capability indicator is used to indicate visited network support of the roaming architecture for voice over IMS with local breakout and to transport the TRF address.

Examples of typical use: A visited network indicating the presence and support of a TRF in a visited network to the home network.

Security Considerations: Security considerations for this feature capability indicator are discussed in clause 9 of draft-ietf-sipcore-proxy-feature [190].

7.9A.4 Definition of feature capability indicator g.3gpp.loopback

Editor's note: This feature capability indicator is to be registered with IANA after draft-ietf-sipcore-proxy-feature becomes RFC

Feature capability indicator name: g.3gpp.loopback

Summary of the feature indicated by this feature capability indicator:

This feature capability indicator, when included in a Feature-Caps header field as specified in draft-ietf-sipcore-proxy-feature [190] in a SIP INVITE request, indicates the support of a the roaming architecture for voice over IMS with local breakout.

Feature capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature capability indicator:

None.

The feature capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature capability indicator is used to indicate support of the roaming architecture for voice over IMS with local breakout and that the INVITE request is a loopback request.

Examples of typical use: The home network indicating when a loopback INVITE request is sent to a visited network.

Security Considerations: Security considerations for this feature capability indicator are discussed in clause 9 of draft-ietf-sipcore-proxy-feature [190].

7.9A.5 Definition of feature capability indicator g.3gpp.home-visited

Editor's note: This feature capability indicator is to be registered with IANA after draft-ietf-sipcore-proxy-feature becomes RFC

Feature capability indicator name: g.3gpp.home-visited

Summary of the feature indicated by this feature capability indicator:

This feature capability indicator, when included in a Feature-Caps header field as specified in draft-ietf-sipcore-proxy-feature [190] in a SIP INVITE request, indicates that the home network supports loopback to the identified visited network for this session. The loopback is expected to be applied at some subsequent entity to the insertion point. The feature capability indicator carries a parameter value which indicates the visited network.

Feature capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature capability indicator:

String with an equality relationship. When used in a Feature-Caps header field, the value follows the syntax as described in table 7.9A.2 for g-3gpp-home-visited.

Table 7.9A.2: ABNF syntax of values of the g.3gpp.home-visited feature capability indicator

```
g-3gpp-home-visited = token/quoted string
```

The value follows that used in the P-Visited-Network-ID header field.

The feature capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature capability indicator is used to indicate the home network supports loopback to the identified visited network for this session. The loopback is expected to be applied at some subsequent entity to the insertion point. The feature capability indicator carries a parameter which indicates the visited network.

Examples of typical use: A home network indicating the home network supports loopback to the identified visited network for this session.

Security Considerations: Security considerations for this feature capability indicator are discussed in clause 9 of draft-ietf-sipcore-proxy-feature [190].

7.9A.6 Definition of feature capability indicator g.3gpp.mrb

Editor's note: This feature capability indicator is to be registered with IANA after draft-ietf-sipcore-proxy-feature [190] becomes RFC.

Feature capability indicator name: g.3gpp.mrb

Summary of the feature indicated by this feature capability indicator:

This feature capability indicator when included in a Feature-Caps header field as specified in draft-ietf-sipcore-proxy-feature [190] in a SIP INVITE request indicates that in a roaming scenario, the visited network supports media resource broker functionality for the allocation of multimedia resources in the visited network. When used, it indicates the URI of the visited network MRB.

Feature capability indicator specification reference:

3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature capability indicator:

String with an equality relationship. When used in a Feature-Caps header field, the value is string and follows the syntax as described in table 7.9A.3 for g-3gpp-mrb.

Table 7.9A.3: ABNF syntax of values of the g.3gpp.mrb feature capability indicator

```
g-3gpp-mrb = "<" SIP URI ">"
```

The feature capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature capability indicator is used to indicate the URI of the media resource broker.

Examples of typical use: Indicating the URI of the visited network MRB to the home network.

Security Considerations: Security considerations for this feature capability indicator are discussed in clause 9 of draft-ietf-sipcore-proxy-feature [190].

7.10 Reg-event package extensions defined within the current document

7.10.1 General

This subclause describes the reg-event package extensions that are applicable for the IM CN subsystem.

7.10.2 Reg-Event package extension to transport wildcarded public user identities

7.10.2.1 Structure and data semantics

This subclause defines an extension to the event registration package (RFC 3680 [43]) to transport policy to transport wildcarded public user identities that are encoded using regular expression.

In order to include a wildcared public user identity in the event registration package, the notifier shall

1. if the registration set of the identity whose registration status is notified contains a wildcarded public user identity, add a <wildcardedIdentity> sub-element defined in subclause 7.10.2.2 of this document to the <registration> element of the wildcarded identiy;

2. for the <registration> element containing a <wildcardedIdentity> sub-element:

a) set the aor attribute to any public user identity that is represented by the wildcarded identity; and

b) set the <wildcardedIdentity> sub-element inside of the <registration> element to the wildcarded identity as received via the Cx interface.

NOTE: The public user identity that is put into the aor attribute does not have any extra priviledges over any other public user identity that is represented by a wildcarded public user identity.

7.10.2.2 XML Schema

Table 7.10.1 in this subclause defines the XML Schema describing the extension to transport wildcarded public user identities which can be included in the reg event package sent from the S-CSCF in NOTIFY requests.

Table 7.10.1: Wildcarded Identity, XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:extRegExp:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="wildcardedIdentity" type="xs:string"/>
</xs:schema>
```

NOTE: Multiple wildcarded elements can be included in one registration element.

7.10.3 Reg-event package extension for policy transport

7.10.3.1 Scope

This subclause describes coding which extends the registration event package defined in RFC 3680 [43] to transport policy associated with a public user identity.

7.10.3.2 Structure and data semantics

The policy associated with a public user identity shall be encoded as follows:

1. add an <actions> element defined in the RFC 4745 [182] in the <registration> element of the public user identity in the registration information;

NOTE: The <actions> element is validated by the <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <registration> elements.

2. if the policy to the usage of the communication resource priority (see RFC 4412 [116]) is associated with the public user identity, then for each allowed usage:

   a. include <rph> child element in the <actions> child element of the <registration> element;

   b. set the 'ns' attribute of the <rph> child element of the <actions> child element of the <registration> element to the allowed resource priority namespace as specified in RFC 4412 [116] and as registered in IANA; and

   c. set the 'val' attribute of the <rph> child element of the <actions> child element of the <registration> element to the allowed resource priority value within the allowed resource priority namespace;

3. if the policy to act as priviledged sender (the P-CSCF passes identities for all calls) is associated with the public user identity, then include a <privSender> child element in the <actions> child element of the <registration> element;

4. if the policy for special treatment of the P-Private-Network-Indication header field (the P-CSCF allows the UE to make private calls) is associated with the public user identity, then include a <pni> child element in the <actions> child element of the <registration> element, and shall:

a. if a P-Private-Network-Indication header field shall be forwarded, if received from the attached equipment, set the "insert" attribute of the <pni> element to a "fwd" value;

b. if a P-Private-Network-Indication header field shall be inserted in all requests received from the attached equipment, insert an "insert" attribute of the <pni> element to a "ins" value; and

c. if the value of the "insert" attribute is "ins", insert a "domain" attribute with the value of the URI to be set in the P-Private-Network-Indication header field; and

5. if the policy to act as priviledged sender for the calls with the P-Private-Network-Indication header field (the P-CSCF allows the UE to make private calls, and the P-CSCF passes identities only for private calls) is associated with the public user identity, then include a <privSenderPNI> child element in the <actions> child element of the <registration> element.

NOTE: If only the <privSender> child element is sent and no <privSenderPNI> child element is sent, then the <privSender> child element applies to both public network traffic and private network traffic (i.e. that with special treatment of the P-Private-Network-Indication header field).

7.10.3.3 XML Schema

Table 7.10.2 in this subclause defines the XML Schema describing the individual policies which can be delivered to the the P-CSCF or UE using the reg event package extension for policy transport.

Table 7.10.2: Reg event package extension for policy transport, XML Schema

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:extRegInfo:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="rph">
  <xs:complexType>
  <xs:attribute name="ns" type="xs:string"/>
  <xs:attribute name="val" type="xs:string"/>
  </xs:complexType>
  </xs:element>
  <xs:element name="privSender">
  <xs:complexType/>
  </xs:element>
  <xs:element name="pni">
  <xs:complexType>
  <xs:attribute name="insert">
    <xs:simpleType>
    <xs:restriction base="xs:string">
    <xs:enumeration value="fwd"/>
    <xs:enumeration value="ins"/>
    </xs:restriction>
    </xs:simpleType>
  </xs:attribute>
  <xs:attribute name="domain" type="xs:anyURI"/>
  </xs:complexType>
  </xs:element>
  <xs:element name="privSenderPNI">
  <xs:complexType/>
  </xs:element>
</xs:schema>
```

Delete 8 SIP compression (not relevant for 1TR114 therefore deleted)

9 IP-Connectivity Access Network aspects when connected to the IM CN subsystem

9.1 Introduction

A UE accessing the IM CN subsystem and the IM CN subsystem itself utilises the services supported by the IP-CAN to provide packet-mode communication between the UE and the IM CN subsystem. General requirements for the UE on the use of these packet-mode services are specified in this clause.

Possible aspects particular to each IP-CAN is described separately for each IP-CAN.

9.2 Procedures at the UE

9.2.1 ~~*Connecting to the IP-CAN and*~~ P-CSCF discovery

For P-CSCF discovery only DNS procedures shall apply.

Prior to communication with the IM CN subsystem, the UE shall:

~~*a) establish a connection with the IP-CAN;*~~

~~*b) obtain an IP address using either the standard IETF protocols (e.g., DHCP or IPCP) or a protocol that is particular to the IP-CAN technology that the UE is utilising. The UE shall fix the obtained IP address throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the last deregistration; and*~~

c) acquire a P-CSCF address(es).

~~*The UE may acquire an IP address via means other than the DHCP. In this case, upon acquiring an IP address, the UE shall request the configuration information (that includes the DNS and P-CSCF addresses) from the DHCP server.*~~

~~*The methods for acquiring a P-CSCF address(es) are:*~~

~~*I. Employ Dynamic Host Configuration Protocol for IPv4 RFC 2131 [40A] or for IPv6 (DHCPv6) RFC 3315 [40]. Employ the DHCP options for SIP servers RFC 3319 [41] or, for IPv6, RFC 3361 [35A]. Employ the DHCP options for Domain Name Servers (DNS) RFC 3646 [56C].*~~

~~*The UE shall either:*~~

~~*in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or*~~

~~*request a list of SIP server IP addresses of P-CSCF(s).*~~

~~*II. Obtain the P-CSCF address(es) by employing a procedure that the IP-CAN technology supports. (e.g. GPRS).*~~

~~*III. The UE may use pre-configured P-CSCF address(es) (IP address or domain name). For example:*~~

~~*a. The UE selects a P-CSCF from the list stored in ISIM or IMC;*~~

~~*b. The UE selects a P-CSCF from the list in IMS management object.*~~

NOTE: Access-specific annexes provide additional guidance on the method to be used by the UE to acquire P-CSCF address(es).

~~*When acquiring a P-CSCF address(es), the UE can freely select either method I or II or III.*~~

The UE *shall*~~*may also*~~ request a DNS Server IP address(es) as specified in RFC 3315 [40] and RFC 3646 [56C] or RFC 2131 [40A].

9.2.2 Handling of the IP-CAN

The means to ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP session is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. I-WLAN is described in annex D. xDSL is described in annex E. DOCSIS is described in Annex H. EPS is described in annex L. cdma2000® packet data subsystem is described in Annex M. EPC via cdma2000® HRPD is described in annex O. cdma2000® Femtocell network is described in annex Q. DVB-RCS2 is described in Annex S. If a particular handling of the IP-CAN is needed for emergency calls, this is described in the annex for each access technology.

9.2.2A P-CSCF restoration procedure

The UE may support P-CSCF restoration procedures.

An IP-CAN may provide means for detecting a P-CSCF failure.

An UE supporting the P-CSCF restoration procedure should either use the keep-alive procedures described in RFC 6223 [143] or the procedure provided by a IP-CAN for monitoring the P-CSCF status.

NOTE 1: The UE can use other means to monitor the P-CSCF status, e.g. ICMP echo request/response. However, those other means are out of scope of this document.

NOTE 2: A UE registered through the procedures described in RFC 5626 [92] can use the keep-alive mechanism to monitor the status of the P-CSCF.

9.2.3 Special requirements applying to forked responses

Since the UE does not know that forking has occurred until a second provisional response arrives, the UE will request the radio/bearer resources as required by the first provisional response. For each subsequent provisional response that may be received, different alternative actions may be performed depending on the requirements in the SDP answer:

- the UE has sufficient radio/bearer resources to handle the media specified in the SDP of the subsequent provisional response, or
- the UE must request additional radio/bearer resources to accommodate the media specified in the SDP of the subsequent provisional response.

NOTE 1: When several forked responses are received, the resources requested by the UE is the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When an 199 (Early Dialog Terminated) response for the INVITE request is received for an early dialogue, the UE shall release reserved radio/bearer resources associated with that early dialogue.

When the first final 200 (OK) response for the INVITE request is received for one of the early dialogues, the UE proceeds to set up the SIP session using the radio/bearer resources required for this session. Upon the reception of the first final 200 (OK) response for the INVITE request, the UE shall release all unneeded radio/bearer resources.

Delete Section 10 Media control (not relevant for 1TR114 therefore deleted)

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

In consideration of this annex the profile tables in 1TR114 shall apply !

A.1 Profiles

A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications which are referenced by this specification, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) which are referenced by this specification and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex.

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column.

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

For all IETF specifications that are not referenced by this document or that are not mentioned within the 3GPP profile of SIP and SDP, the generic rules as defined by RFC 3261 [26] and in addition the rules in clauses 5 and 6 of this specification apply, e.g..

- a proxy which is built in accordance to this specification passes on any unknown method, unknown header field or unknown header field parameter after applying procedures such as filtering, insertion of P-Asserted-Identity header field, etc.;
- an UA which is built in accordance to this specification will
  - handle received unknown methods in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 501 (Not Implemented) response; and
  - handle unknown header fields and unknown header field parameters in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 420 (Bad Extension) if an extension identified by an option-tag in the Require header field of the received request is not supported by the UA.

A.1.2 Introduction to methodology within this profile

This subclause does not reflect dynamic conformance requirements but static ones. In particular, a condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the main part of this specification.

As a consequence, PDU parameter tables in this subclause are not the same as the tables describing the syntax of a PDU in the reference specification, e.g. RFC 3261 [26] tables 2 and 3. It is not rare to see a parameter which is optional in the syntax but mandatory in subclause below.

The various statii used in this subclause are in accordance with the rules in table A.1.

Table A.1: Key to status codes

Status code	Status name	Meaning
m	mandatory	the capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).
o	optional	the capability may or may not be supported. It is an implementation choice.
n/a	not applicable	it is impossible to use the capability. No answer in the support column is required.
x	prohibited (excluded)	It is not allowed to use the capability. This is more common for a profile.
c <integer>	conditional	the requirement on the capability ("m", "o", "n/a" or "x") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.
o.<integer>	qualified optional	for mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options.
i	irrelevant	capability outside the scope of the given specification. Normally, this notation should be used in a base specification ICS proforma only for transparent parameters in received PDUs. However, it may be useful in other cases, when the base specification is in fact based on another standard.

In the context of this specification the "i" status code mandates that the implementation does not change the content of the parameter. It is an implementation option if the implementation acts upon the content of the parameter (e.g. by setting filter criteria to known or unknown parts of parameters in order to find out the route a message has to take).

It must be understood, that this 3GPP SIP profile does not list all parameters which an implementation will treat as indicated by the status code "irrelevant". In general an implementation will pass on all unknown messages, header fields and header field parameters, as long as it can perform its normal behaviour.

The following additional comments apply to the interpretation of the tables in this Annex.

NOTE 1: The tables are constructed according to the conventional rules for ICS proformas and profile tables.

NOTE 2: The notation (either directly or as part of a conditional) of "m" for the sending of a parameter and "i" for the receipt of the same parameter, may be taken as indicating that the parameter is passed on transparently, i.e. without modification. Where a conditional applies, this behaviour only applies when the conditional is met.

As an example, the profile for the MGCF is found by first referring to clause 4.1, which states "The MGCF shall provide the UA role". Profiles are divided at the top level into the two roles in table A.2, user agent and proxy. The UA role is defined in subclause A.2.1 and the proxy role is defined in subclause A.2.2. More specific roles are listed in table A.3, table A.3A, table A.3B and table A.3C. The MGCF role is item 6 in table A.3 (the MGCF role is not found in table A.3A or table A.3B). Therefore, all profile entries for the MGCF are found by searching for A.3/6 in subclause A.2.1.

As a further example, to look up support of the Reason header field, table A.4 item 38 lists the Resaon header field as a major capability that is optional for the user agent role. A subsequent search for A.4/38 in subclause A.2.1 shows that the Reason header field is optional for a user agent role to send and receive for ACK, BYE, CANCEL, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE, and UPDATE requests. Also, table A.162 item 48 lists the Reason header field as a major capability that is optional for the proxy role. A

subsequent search for A.162/48 in subclause A.2.2 shows that, if supported, the Reason header field is mandatory to send and irrelevant to receive for ACK, BYE, CANCEL, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE, and UPDATE requests.

A.1.3 Roles

Table A.2: Roles

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

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status
1	UE	5.1	n/a	o.1
~~1A~~	~~UE containing UICC~~	~~5.1~~	~~n/a~~	~~c5~~
1B	UE without UICC	5.1	n/a	c5
~~2~~	~~P-CSCF~~	~~5.2~~	~~n/a~~	~~o.1~~
~~2A~~	~~P-CSCF (IMS-ALG)~~	~~[7]~~	~~n/a~~	~~c6~~
~~3~~	~~I-CSCF~~	~~5.3~~	~~n/a~~	~~o.1~~
~~3A~~	~~void~~			
~~4~~	~~S-CSCF~~	~~5.4~~	~~n/a~~	~~o.1~~
~~5~~	~~BGCF~~	~~5.6~~	~~n/a~~	~~o.1~~
~~6~~	~~MGCF~~	~~5.5~~	~~n/a~~	~~o.1~~
~~7~~	~~AS~~	~~5.7~~	~~n/a~~	~~o.1~~
~~7A~~	~~AS acting as terminating UA, or redirect server~~	~~5.7.2~~	~~n/a~~	~~c2~~
~~7B~~	~~AS acting as originating UA~~	~~5.7.3~~	~~n/a~~	~~c2~~
~~7C~~	~~AS acting as a SIP proxy~~	~~5.7.4~~	~~n/a~~	~~c2~~
~~7D~~	~~AS performing 3rd party call control~~	~~5.7.5~~	~~n/a~~	~~c2~~
~~8~~	~~MRFC~~	~~5.8~~	~~n/a~~	~~o.1~~
~~8A~~	~~MRB~~	~~5.8A~~	~~n/a~~	~~o.1~~
~~9~~	~~IBCF~~	~~5.10~~	~~n/a~~	~~o.1~~
~~9A~~	~~IBCF (THIG)~~	~~5.10.4~~	~~n/a~~	~~c4~~
~~9B~~	~~IBCF (IMS-ALG)~~	~~5.10.5, 5.10.7~~	~~n/a~~	~~c4~~
~~9C~~	~~IBCF (Screening of SIP signalling)~~	~~5.10.6~~	~~n/a~~	~~c4~~
~~9D~~	~~IBCF (Privacy protection)~~	~~5.10.8~~	~~n/a~~	~~c4~~
~~10~~	~~Additional routeing functionality~~	~~Annex I~~	~~n/a~~	~~c3~~
~~11~~	~~E-CSCF~~	~~5.11~~	~~n/a~~	~~o.1~~
~~11A~~	~~E-CSCF acting as UA~~	~~5.11.1, 5.11.2, 5.11.3~~	~~n/a~~	~~c7~~
~~11B~~	~~E-CSCF acting as a SIP Proxy~~	~~5.11.1, 5.11.2~~	~~n/a~~	~~c7~~
~~12~~	~~LRF~~	~~5.12~~	~~n/a~~	~~o.1~~
~~13~~	~~ISC gateway function~~	~~5.13~~	~~n/a~~	~~o.1~~
~~13A~~	~~ISC gateway function (THIG)~~	~~5.13.4~~	~~n/a~~	~~c8~~
~~13B~~	~~ISC gateway function (IMS-ALG)~~	~~5.13.5~~	~~n/a~~	~~c8~~
~~13C~~	~~ISC gateway function (Screening of SIP signalling)~~	~~5.13.6~~	~~n/a~~	~~c8~~

~~c2: IF A.3/7 THEN o.2 ELSE n/a - - AS.~~
~~c3: IF A.3/3 OR A.3/4 OR A.3/5 OR A.3/6 OR A.3/9 THEN o ELSE o.1 - - I-CSCF, S-CSCF, BGCF, MGCF, IBCF.~~
~~c4: IF A.3/9 THEN o.3 ELSE n/a - - IBCF.~~
c5: IF A.3/1 THEN o.4 ELSE n/a - - UE.
~~c6: IF A.3/2 THEN o ELSE n/a - - P-CSCF.~~
~~c7: IF A.3/11 THEN o.5 ELSE n/a - - E-CSCF.~~
~~c8: IF A.3/13 THEN o ELSE n/a - - ISC gateway function.~~
o.1: It is mandatory to support exactly one of these items.
~~o.2: It is mandatory to support at least one of these items.~~
~~o.3: It is mandatory to support at least one of these items.~~
~~o.4 It is mandatory to support exactly one of these items.~~
~~o.5: It is mandatory to support exactly one of these items.~~

NOTE: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.

Table A.3A: Roles specific to additional capabilities

Item	Roles	Reference	RFC status	Profile status
1	Presence server	3GPP TS 24.141 [8A]	n/a	c1
2	Presence user agent	3GPP TS 24.141 [8A]	n/a	c2
3	Resource list server	3GPP TS 24.141 [8A]	n/a	c3
4	Watcher	3GPP TS 24.141 [8A]	n/a	c4
11	Conference focus	3GPP TS 24.147 [8B]	n/a	c11
12	Conference participant	3GPP TS 24.147 [8B]	n/a	c6
21	CSI user agent	3GPP TS 24.279 [8E]	n/a	c7
22	CSI application server	3GPP TS 24.279 [8E]	n/a	c8
31	Messaging application server	3GPP TS 24.247 [8F]	n/a	c5
32	Messaging list server	3GPP TS 24.247 [8F]	n/a	c5
33	Messaging participant	3GPP TS 24.247 [8F]	n/a	c2
33A	Page-mode messaging participant	3GPP TS 24.247 [8F]	n/a	c2
33B	Session-mode messaging participant	3GPP TS 24.247 [8F]	n/a	c2
34	Session-mode messaging intermediate node	3GPP TS 24.247 [8F]	n/a	c5
50	Multimedia telephony service participant	3GPP TS 24.173 [8H]	n/a	c2
50A	Multimedia telephony service application server	3GPP TS 24.173 [8H]	n/a	c9
51	Message waiting indication subscriber UA	3GPP TS 24.606 [8I]	n/a	c2
52	Message waiting indication notifier UA	3GPP TS 24.606 [8I]	n/a	c3
53	Advice of charge application server	3GPP TS 24.647 [8N]	n/a	c8
54	Advice of charge UA client	3GPP TS 24.647 [8N]	n/a	c2
55	Ut reference point XCAP server for supplementary services	3GPP TS 24.623 [8P]	n/a	c3
56	Ut reference point XCAP client for supplementary services	3GPP TS 24.623 [8P]	n/a	c2
57	Customized alerting tones application server	3GPP TS 24.182 [8Q]	n/a	c8
58	Customized alterting tones UA client	3GPP TS 24.182 [8Q]	n/a	c2
59	Customized ringing signal application server	3GPP TS 24.182 [8R]	n/a	c8
60	Customized ringing signel tone UA client	3GPP TS 24.182 [8R]	n/a	c2
61	SM-over-IP sender	3GPP TS 24.341 [8L]	n/a	c2
62	SM-over-IP receiver	3GPP TS 24.341 [8L]	n/a	c2
63	IP-SM-GW	3GPP TS 24.341 [8L]	n/a	c1
71	IP-SM-GW	3GPP TS 29.311 [15A]	n/a	c10
81	MSC Server enhanced for ICS	3GPP TS 24.292 [8O]	n/a	c12
82	ICS user agent	3GPP TS 24.292 [8O]	n/a	c2

83	SCC application server	3GPP TS 24.292 [8O]	n/a	c9
84	EATF	3GPP TS 24.237 [8M]	n/a	c12
85	In-dialog overlap signalling application server	Annex N.2, Annex N.3.3	n/a	c9
86	In-dialog overlap signalling UA client	Annex N.2, Annex N.3.3	n/a	c2
87	Session continuity controller UE	3GPP TS 24.237 [8M]	n/a	c2
88	ATCF (proxy)	3GPP TS 24.237 [8M]	n/a	c13 (note 4)
89	ATCF (UA)	3GPP TS 24.237 [8M]	n/a	c12 (note 4)
91	Malicious communication identification application server	3GPP TS 24.616 [8S]	n/a	c9
92	USSI UE	3GPP TS 24.390 [8W]	n/a	c2
93	USSI AS	3GPP TS 24.390 [8W]	n/a	c3

c1: IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA.
c2: IF A.3/1 THEN o ELSE n/a - - UE.
c3: IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server.
c4: IF A.3/1 OR A.3/7B THEN o ELSE n/a - - UE or AS acting as originating UA.
c5: IF A.3/7D AND A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control and MRFC (note 2).
c6: IF A.3/1 OR A.3A/11 THEN o ELSE n/a - - UE or conference focus.
c7: IF A.3/1 THEN o ELSE n/a - - UE.
c8: IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.
c9: IF A.3/7A OR A.3/7B OR A.3/7C OR A.3/7D THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA, AS acting as a SIP proxy, AS performing 3rd party call control.
c10: IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.
c11: IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.
c12: IF A.2/1 THEN o ELSE n/a - - UA.
c13: IF A.2/2 THEN o ELSE n/a - - proxy.

NOTE 1: For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.
NOTE 2: The functional split between the MRFC and the AS for page-mode messaging is out of scope of this document and they are assumed to be collocated.
NOTE 3: A.3A/63 is an AS providing the IP-SM-GW role to support the transport level interworking defined in 3GPP TS 24.341 [8L]. A.3A/71 is an AS providing the IP-SM-GW role to support the service level interworking for messaging as defined in 3GPP TS 29.311 [15A].
NOTE 4: An ATCF shall support both the ATCF (proxy) role and the ATCF (UA) role.

Table A.3B: Roles with respect to access technology

Item	Value used in P-Access-Network-Info header field	Reference	RFC status	Profile status
1	3GPP-GERAN	[52] 4.4	o	c1
2	3GPP-UTRAN-FDD	[52] 4.4	o	c1
3	3GPP-UTRAN-TDD	[52] 4.4	o	c1
4	3GPP2-1X	[52] 4.4	o	c1
5	3GPP2-1X-HRPD	[52] 4.4	o	c1
6	3GPP2-UMB	[52] 4.4	o	c1
7	3GPP-E-UTRAN-FDD	[52] 4.4	o	c1
8	3GPP-E-UTRAN-TDD	[52] 4.4	o	c1
9	3GPP2-1X-Femto	[52] 4.4	o	c1
11	IEEE-802.11	[52] 4.4	o	c1
12	IEEE-802.11a	[52] 4.4	o	c1
13	IEEE-802.11b	[52] 4.4	o	c1
14	IEEE-802.11g	[52] 4.4	o	c1
15	IEEE-802.11n	[52] 4.4	o	c1
21	ADSL	[52] 4.4	o	c1
22	ADSL2	[52] 4.4	o	c1
23	ADSL2+	[52] 4.4	o	c1
24	RADSL	[52] 4.4	o	c1
25	SDSL	[52] 4.4	o	c1
26	HDSL	[52] 4.4	o	c1
27	HDSL2	[52] 4.4	o	c1
28	G.SHDSL	[52] 4.4	o	c1
29	VDSL	[52] 4.4	o	c1
30	IDSL	[52] 4.4	o	c1
41	DOCSIS	[52] 4.4	o	c1
51	DVB-RCS2	[52] 4.4	o	c1
c1:	If A.3/1 OR A.3/2 THEN o.1 ELSE n/a - - UE or P-CSCF.			
o.1:	It is mandatory to support at least one of these items.			

Table A.3C: Modifying roles

Item	Roles	Reference	RFC status	Profile status
1	UE performing the functions of an external attached network	4.1		
NOTE:	This table identifies areas where the behaviour is modified from that of the underlying role. Subclause 4.1 indicates which underlying roles are modified for this behaviour.			

Table A.3D: Roles with respect to security mechanism

Item	Security mechanism	Reference	RFC status	Profile status	1TR114
1	IMS AKA plus IPsec ESP	clause 4.2B.1	n/a	c1	n/a
2	SIP digest plus check of IP association	clause 4.2B.1	n/a	c2	M
3	SIP digest plus Proxy Authentication	clause 4.2B.1	n/a	c2	
4	SIP digest with TLS	clause 4.2B.1	n/a	c2	O
5	NASS-IMS bundled authentication	clause 4.2B.1	n/a	c2	n/a
6	GPRS-IMS-Bundled authentication	clause 4.2B.1	n/a	c2	n/a
7	Trusted node authentication	clause 4.2B.1	n/a	c3	
20	End-to-end media security using SDES	clause 4.2B.2	o	c5	n/a
21	End-to-end media security using KMS	clause 4.2B.2	o	c5	n/a
30	End-to-access-edge media security using SDES	clause 4.2B.2	n/a	c4	m
c1:	IF (A.3/1A OR A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE IF A.3/1B THEN o ELSE n/a - - UE containing UICC or P-CSCF or I-CSCF or S-CSCF, UE without UICC.				
c2:	IF (A.3/1 OR A.3/2 OR A.3/3 OR A.3/4) THEN o ELSE n/a - - UE or P-CSCF or I-CSCF or S-CSCF.				
c3:	IF (A.3/3 OR A.3/4) THEN o ELSE n/a - - I-CSCF or S-CSCF.				
c4:	IF (A.3/1 OR A.3/2A) THEN o ELSE n/a - - UE or P-CSCF (IMS-ALG).				
c5:	IF A.3/1 THEN o - - UE.				

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

A.2.1 User agent role

A.2.1.1 Introduction

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

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

A.2.1.2 Major capabilities

Status code in column DT profile	***Status name***	***Meaning***
m	*mandatory*	*The capability shall be supported as specified within 3GPP TS 24.229.* *If the Capability is mentioned as optional this Option has to be supported. The option must be configurable.* *The default support is enabled.*
o	*optional*	*The capability may or may not be supported. It is an implementation choice. If the feature is supported the capability to use the feature shall be configurable. The default configuration for this capability shall be disabled*
i	*informative*	*Capability outside the scope of the given specification.*
n/a	*not applicable*	*It is impossible to use the capability. No answer in the support column is required.*

Editor's note: it needs to be checked whether it should be explicitly clarified that the IBCF (IMS-ALG) is transparent to some presence or conference extensions.

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status	*UE profile*
	Capabilities within main protocol				
1	client behaviour for registration?	[26] subclause 10.2	o	~~c3~~*m*	*m*
2	registrar?	[26] subclause 10.3	o	c4	*m*
2A	registration of multiple contacts for a single address of record	[26] 10.2.1.2, 16.6	o	o	*m*
2B	initiating a session?	[26] subclause 13	o	o	*m*
2C	initiating a session which require local and/or remote resource reservation?	[27]	o	c43	*o*
3	client behaviour for INVITE requests?	[26] subclause 13.2	c18	c18	*m*

Item	Does the implementation support	Reference	RFC status	Profile status	UE profile
4	server behaviour for INVITE requests?	[26] subclause 13.3	c18	c18	m
5	session release?	[26] subclause 15.1	c18	c18	m
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o	m
7	authentication between UA and UA?	[26] subclause 22.2	c34	c34	o
8	authentication between UA and registrar?	[26] subclause 22.2	o	c74	m
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	c75	m
9	server handling of merged requests due to forking?	[26] 8.2.2.2	m	m	m
10	client handling of multiple responses due to forking?	[26] 13.2.2.4	m	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o	m
12	downloading of alerting information?	[26] subclause 20.4	o	o	m
	Extensions				
13	SIP INFO method and package framework?	[25]	o	c90	m
14	reliability of provisional responses in SIP?	[27]	c19	c44	m
15	the REFER method?	[36]	o	c33	m
16	integration of resource management and SIP?	[30] [64]	c19	c44	o
17	the SIP UPDATE method?	[29]	c5	c44	m
19	SIP extensions for media authorization?	[31]	o	c14	o
20	SIP specific event notification?	[28]	o	c13	m
21	the use of NOTIFY to establish a dialog?	[28] 4.2	o	n/a	n/a
22	acting as the notifier of event information?	[28]	c2	c15	m
23	acting as the subscriber to event information?	[28]	c2	c16	m
24	session initiation protocol extension header field for registering non-adjacent contacts?	[35]	o	c6	m
25	private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks?	[34]	o	m	m
26	a privacy mechanism for the Session Initiation Protocol (SIP)?	[33]	o	m	m
26A	request of privacy by the inclusion of a Privacy header indicating any privacy option?	[33]	c9	c11	m
26B	application of privacy based on the received Privacy header?	[33]	c9	n/a	n/a
26C	passing on of the Privacy header transparently?	[33]	c9	c12	m
26D	application of the privacy option "header" such that those headers which cannot be	[33] 5.1	c10	c27	m

Item	Does the implementation support	Reference	RFC status	Profile status	UE profile
	completely expunged of identifying information without the assistance of intermediaries are obscured?				
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	c27	m
26F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	c10	c27	m
26G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c10	n/a	n/a
26H	application of the privacy option "history" such that privacy of the History-Info header is provided by the network?	[66] 7.2	c37	c37	m
27	a messaging mechanism for the Session Initiation Protocol (SIP)?	[50]	o	c7	m
28	session initiation protocol extension header field for service route discovery during registration?	[38]	o	c17	m
29	compressing the session initiation protocol?	[55]	o	c8	o
30	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m	partly m
31	the P-Associated-URI header extension?	[52] 4.1	c21	c22	o
32	the P-Called-Party-ID header extension?	[52] 4.2	c21	~~c23~~m	m
33	the P-Visited-Network-ID header extension?	[52] 4.3	c21	c24	n/a (roaming)
34	the P-Access-Network-Info header extension?	[52] 4.4	c21	c25	m
35	the P-Charging-Function-Addresses header extension?	[52] 4.5	c21	c26	m
36	the P-Charging-Vector header extension?	[52] 4.6	c21	c26	m
37	security mechanism agreement for the session initiation protocol?	[48]	o	c20	o
38	the Reason header field for the session initiation protocol?	[34A]	o	~~c68~~m	m
38A	use of the Reason header field in Session Initiation Protocol (SIP) responses?	[130]	o	c82	m
39	an extension to the session initiation protocol for symmetric response routeing?	[56A]	o	c62	m
40	caller preferences for the session initiation protocol?	[56B]	C29	c29	m
40A	the proxy-directive within caller-preferences?	[56B] 9.1	o.5	o.5	m
40B	the cancel-directive within caller-preferences?	[56B] 9.1	o.5	o.5	m
40C	the fork-directive within caller-preferences?	[56B] 9.1	o.5	c28	m
40D	the recurse-directive within caller-preferences?	[56B] 9.1	o.5	o.5	m

Item	Does the implementation support	Reference	RFC status	Profile status	UE profile
40E	the parallel-directive within caller-preferences?	[56B] 9.1	o.5	c28	m
40F	the queue-directive within caller-preferences?	[56B] 9.1	o.5	o.5	m
41	an event state publication extension to the session initiation protocol?	[70]	o	c30	m
42	SIP session timer?	[58]	c19	c19	m
43	the SIP Referred-By mechanism?	[59]	o	c33	m
44	the Session Inititation Protocol (SIP) "Replaces" header?	[60]	c19	c38 (note 1)	m
45	the Session Inititation Protocol (SIP) "Join" header?	[61]	c19	c19 (note 1)	m
46	the callee capabilities?	[62]	o	c35	m
47	an extension to the session initiation protocol for request history information?	[66]	o	~~O~~c_dt1	m
48	Rejecting anonymous requests in the session initiation protocol?	[67]	o	~~o~~ c_dt1	m
49	session initiation protocol URIs for applications such as voicemail and interactive voice response?	[68]	o	~~o~~ c_dt1	m
50	Session Initiation Protocol's (SIP) non-INVITE transactions?	[84]	m	m	m
51	the P-User-Database private header extension?	[82] 4	o	c94	n/a
52	a uniform resource name for services?	[69]	n/a	c39	n/a
53	obtaining and using GRUUs in the Session Initiation Protocol (SIP)	[93]	o	c40 (note 2)	m
54	an extension to the session initiation protocol for request cpc information?	[95]	o	c41	m
55	the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)?	[96]	o	c42	o
56	the SIP P-Profile-Key private header extension?	[97]	n/a	n/a	n/a
57	managing client initiated connections in SIP?	[92]	o	c45	m
58	indicating support for interactive connectivity establishment in SIP?	[102]	o	c46	m
59	multiple-recipient MESSAGE requests in the session initiation protocol?	[104]	c47	c48	m
60	SIP location conveyance?	[89]	o	c49	m
61	referring to multiple resources in the session initiation protocol?	[105]	c50	c50	m
62	conference establishment using request-contained lists in the session initiation protocol?	[106]	c51	c52	m
63	subscriptions to request-contained resource lists in the session initiation protocol?	[107]	c53	c53	o
64	dialstring parameter for the session initiation	[103]	o	c19	o

Item	Does the implementation support	Reference	RFC status	Profile status	UE profile
	protocol uniform resource identifier?				
65	the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular?	[111]	o	c60	n/a
66	the SIP P-Early-Media private header extension for authorization of early media?	[109] 8	o	c58	m
67	number portability parameters for the 'tel' URI?	[112]	o	c54	m
67A	assert or process carrier indication?	[112]	o	c55	n/a
67B	local number portability?	[112]	o	c57	n/a
68	DAI Parameter for the 'tel' URI?	[113]	o	c56	n/a
69	extending the session initiation protocol Reason header for preemption events	[115]	c69	c69	n/a
70	communications resource priority for the session initiation protocol?	[116]	o	c70	n/a
70A	inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol?	[116] 4.2	c72	c72	n/a
70B	inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol?	[116] 4.2	c72	c72	n/a
70C	resource priority namespace of DSN (Defense switched network)?	[116] 10.2	c71	n/a	n/a
70D	resource priority namespace of DSRN (Defense RED switched network)?	[116] 10.3	c71	n/a	n/a
70E	resource priority namespace of Q735?	[116] 10.4	c71	n/a	n/a
70F	resource priority namespace of ETS (Government Emergency Telecommunications Service)?	[116] 10.5	c71	n/a	n/a
70G	resource priority namespace of WPS (Wireless priority service)?	[116] 10.6	c71	c73	n/a
71	addressing an amplification vulnerability in session initiation protocol forking proxies?	[117]	o	c87	m
72	the remote application identification of applying signalling compression to SIP	[79] 9.1	o	c8	o
73	a session initiation protocol media feature tag for MIME application sub-types?	[120]	o	c59	m
74	Identification of communication services in the session initiation protocol?	[121]	o	c61	o
75	a framework for consent-based communications in SIP?	[125]	c76	c76	o
75A	a relay within the framework for consent-based communications in SIP?	[125]	c77	c78	o
75B	a recipient within the framework for consent-based communications in SIP?	[125]	c80	c79	o
76	transporting user to user information for call centers using SIP?	[126]	o	c81	m
77	The SIP P-Private-Network-Indication private-header (P-Header)?	[134]	o	o	o

Item	Does the implementation support	Reference	RFC status	Profile status	UE profile
78	the SIP P-Served-User private header?	[133] 6	o	c93	o
79	proxy mutual authentication in SIP?	[139]	c84	c83	o
80	the P-Debug-ID header extension?	[140]	o	c85	o
81	the 199 (Early Dialog Terminated) response code)	[142]	o	c86	m
82	message body handling in SIP?	[150]	m	m	m
83	indication of support for keep-alive	[143]	o	c88	o
84	SIP Interface to VoiceXML Media Services?	[145]	o	c89	m
85	common presence and instant messaging (CPIM): message format?	[151]	o	c91	o
86	instant message disposition notification?	[157]	o	c91	o
87	requesting answering modes for SIP?	[158]	o	c60	o
88	SOS URI parameter for marking SIP requests related to emergency calls?	[159]	o	c92	n/a
89	the early session disposition type for SIP?	[74B]	o	o	o
DT1	XML Schema for PSTN?	3GPP TS 29.163 [11B]	o	o	c_dt4
90	delivery of Request-URI targets to user agents?	[66]	o	c95	m
91	The Session-ID header?	[162]	o	c102	m
92	correct transaction handling for 2xx responses to Session Initiation Protocol INVITE requests?	[163]	c18	c18	m
93	addressing Record-Route issues in the Session Initiation Protocol (SIP)?	[164]	n/a	n/a	n/a
94	essential correction for IPv6 ABNF and URI comparison in RFC3261?	[165]	m	m	m
95	suppression of session initiation protocol REFER method implicit subscription?	[173]	o	c99	o
96	Alert-Info URNs for the Session Initiation Protocol?	[175]	o	o	m
97	multiple registrations?	Subclause 3.1	n/a	c103	o
98	the SIP P-Refused-URI-List private-header?	[183]	o	c104	o
99	request authorization through dialog Identification in the session initiation protocol?	[184]	o	c105	o
100	indication of features supported by proxy?	[190]	o	c106	m
101	registration of bulk number contacts?	[191]	o	c107	o
102	media control channel framework?	[146]	o	c108	o
103	S-CSCF restoration procedures?	Subclause 3.1	n/a	c110	m
104	SIP overload control?	[198]	o	c112	o
104A	feedback control?	[199]	c113	c113	o
104B	distribution of load filters?	[201]	c113	c114	o
105	handling of a 380 (Alternative service) response?	Subclauses 5.1.3.1 , 5.1.6.8, and 5.2.10	n/a	c111	o

Conditions:

c2:	IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.
c3:	IF A.3/1 OR A.3/4 OR A.3A/81 THEN m ELSE n/a - - UE or S-CSCF functional entity or MSC Server enhanced for ICS.
c4:	IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.
c5:	IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.
c6:	IF A.3/4 OR A.3/1 OR A.3A/81 THEN m ELSE n/a. - - S-CSCF or UE or MSC Server enhanced for ICS.
c7:	IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B OR A.3A/83 OR A.3A/89 THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), SCC application server, ATCF (UA).
c8:	IF A.3/1 THEN (IF (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3B/7 OR A.3B/8 OR A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3B/15) THEN m ELSE o) ELSE n/a - - UE behaviour (based on P-Access-Network-Info usage).
c9:	IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.
c11:	IF A.3/1 OR A.3/6 OR A.3A/81 THEN o ELSE IF A.3/9B OR A.3/13B THEN m ELSE n/a - - UE or MGCF, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MSC Server enhanced for ICS.
c12:	IF A.3/7D OR A3A/84 OR A.3A/89 THEN m ELSE n/a - - AS performing 3rd-party call control, EATF, ATCF (UA).
c13:	IF A.3/1 OR A.3/2 OR A.3/4 OR A.3/9B OR A.3/11 OR A.3/12 OR A.3/13B OR A.3A/81 THEN m ELSE o - - UE or S-CSCF or IBCF (IMS-ALG) or E-CSCF or LRF or ISC gateway function (IMS-ALG) or MSC Server enhanced for ICS.
c14:	IF A.3/1 AND A4/2B AND (A.3B/1 OR A.3B/2 OR A.3B/3) THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE and initiating sessions and GPRS IP-CAN or P-CSCF.
c15:	IF A.4/20 AND (A.3/4 OR A.3/9B OR A.3/11 OR A.3/13B) THEN m ELSE o – SIP specific event notification extensions and S-CSCF or IBCF (IMS-ALG) or E-CSCF or ISC gateway function (IMS-ALG).
c16:	IF A.4/20 AND (A.3/1 OR A.3/2 OR A.3/9B OR A.3/12 OR A.3/13B OR A.3A/81) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF or IBCF (IMS-ALG) or MSC Server enhanced for ICS or LRF or ISC gateway function (IMS-ALG).
c17:	IF A.3/1 OR A.3/4 OR A.3A/81 THEN m ELSE n/a - - UE or S-CSCF or MSC Server enhanced for ICS.
c18:	IF A.4/2B THEN m ELSE n/a - - initiating sessions.
c19:	IF A.4/2B THEN o ELSE n/a - - initiating sessions.
c20:	IF A.3/1 AND (A.3D/1 OR A.3D/4) THEN m ELSE n/a - - UE and (IMS AKA plus IPsec ESP or SIP digest with TLS).
c21:	IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).
c22:	IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3A/81) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UE or MSC Server enhanced for ICS.
c23:	IF A.4/30 AND (A.3/1 OR A.3A/81) THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE or MSC Server enhanced for ICS.
c24:	IF A.4/30 AND (A.3/4 OR A.3A/81) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or MSC Server enhanced for ICS.
c25:	IF A.4/30 AND (A.3A/81 OR A.3/4 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9B OR A.3/13B OR A3A/84) THEN m ELSE IF A.4/30 AND A.3/1 AND (A.3B/1OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3A/7 OR A.3A/8 OR A.3B/11OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3A/15 OR A.3B/41) THEN m ELSE IF A4/30 AND A.3/1 AND (A.3B/21 OR A.3B/22 OR A.3B/23 OR A.3B/24 OR A.3B/25 OR A.3B/26 OR A.3A/27 OR A.3A/28 OR A.3B/29 OR A.3B/30) THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP), MSC Server enhanced for ICS, S-CSCF, MGCF or AS acting as terminating UA or AS acting as third-party call controller or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, EATF, P-Access-Network-Info values.
c26:	IF A.4/30 AND (A.3A/81 OR (A.3/4 AND A.4/2) OR A.3/6 OR A.3/7A OR A.3/7B or A.3/7D OR A.3/9B OR A.3/13B OR A3A/84 OR A.3A/89) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) MSC Server enhanced for ICS, S-CSCF, registrar, MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller , IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF, ATCF (UA).
c27:	IF A.3/7D OR A.3/9D THEN o ELSE x - - AS performing 3rd party call control, IBCF (Privacy).
c29:	IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.
c30:	IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS.

c33:	IF A.3/9B OR A.3/12 OR A.3/13B OR A.3A/81 OR A.3A/11 OR A.3A/12 OR A.4/44 THEN m ELSE o - - IBCF (IMS-ALG) or LRF or ISC gateway function (IMS-ALG) or MSC Server enhanced for ICS or conference focus or conference participant or the Session Inititation Protocol (SIP) "Replaces" header.
c34:	IF A.4/44 OR A.4/45 OR A.3/9B OR A.3/13 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header or the Session Inititation Protocol (SIP) "Join" header or IBCF (IMS-ALG) or ISC gateway function (IMS-ALG).
c35:	IF A.3/4 OR A.3/9B OR A.3/13B OR A.3A/82 OR A.3A/83 OR A.3A/21 OR A.3A/22 OR A3A/84 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3A/81) THEN o ELSE n/a - - S-CSCF or IBCF (IMS-ALG) or ISC gateway function (IMS-ALG) functional entities or ICS user agent or SCC application server or CSI user agent or CSI application server, UE or MGCF or AS or MRFC functional entity or MSC Server enhanced for ICS or EATF.
c37	IF A.4/47 THEN o.3 ELSE n/a - - an extension to the session initiation protocol for request history information.
c38:	IF A.4/2B AND (A.3A/11 OR A.3A/12 OR A.3/7D) THEN m ELSE IF A.4/2B THEN o ELSE n/a - - initiating sessions, conference focus, conference participant, AS performing 3rd party call control.
c39:	IF A.3/1 THEN m ELSE IF A.3/7B OR A.3/7D OR A.3/9 THEN o ELSE n/a - - UE, AS acting as an originating UA, or AS acting as third-party call controller, IBCF.
c40	IF A.3/4 OR (A.3/1 AND NOT A.3C/1) OR A.3A/81 THEN m ELSE IF (A.3/7A OR A.3/7B OR A.3/7D) THEN o ELSE n/a - - S-CSCF, UE, UE performing the functions of an external attached network, MSC Server enhanced for ICS, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.
c42:	IF A.3/1 THEN n/a ELSE o - - UE.
c43:	IF A.4/2B THEN o ELSE n/a - - initiating sessions.
c44:	IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.
c45:	IF A.4/97 THEN m ELSE n/a - - multiple registrations.
c46	IF A.3/1 OR A.3/4 THEN o ELSE n/a - - UE, S-CSCF.
c47:	IF A.4/27 THEN o ELSE n/a - - a messaging mechanism for the Session Initiation Protocol (SIP).
c48:	IF A.3A/32 AND A.4/27 THEN m ELSE IF A.4/27 THEN o ELSE n/a - - messaging list server, a messaging mechanism for the Session Initiation Protocol (SIP).
c49:	IF A.3/1 OR A.3/9B OR A.3/13B OR A.3A/81 OR A/3/11 OR A.3/12 OR A3A/84 THEN m ELSE o - - UE, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MSC Server enhanced for ICS, E-CSCF, LRF, EATF.
c50:	IF A.3A/81 THEN n/a ELSE IF A.4/15 THEN o ELSE n/a - - MSC Server enhanced for ICS, the REFER method.
c51:	IF A.4/2B THEN o ELSE n/a - - initiating a session.
c52:	IF A.3A/11 AND A.4/2B THEN m ELSE IF A.4/2B THEN o ELSE n/a - - conference focus, initiating a session.
c53:	IF A.3A/81 THEN n/a ELSE IF A.4/20 THEN o ELSE n/a - - MSC Server enhanced for ICS, SIP specific event notification.
c54:	IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9 THEN o, ELSE n/a - - UE, MGCF, AS acting as originating UA, AS performing 3rd party call control, IBCF.
c55:	IF A.4/67 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.
c57:	IF A.4/67 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.
c58:	IF A.3/9B OR A.3/13B OR A.3/6 OR A.3A/81 THEN m ELSE o - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MGCF, MSC Server enhanced for ICS.
c59:	IF A.3/4 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8) THEN o ELSE n/a - - S-CSCF, UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC.
c60:	IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.
c61:	IF (A.3/1 OR A.3A/81 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8 OR A.3/9B OR A.3/13 OR A3A/84) THEN o ELSE n/a - - UE, MSC Server enhanced for ICS, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF.
c62:	IF A.3/1 THEN o ELSE n/a - - UE.
c68:	IF A.4/69 OR A.3A/83 THEN m ELSE o - - extending the session initiation protocol Reason header for preemption events and Q.850 causes, SCC application server.
c69:	IF A.4/70 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.
c70:	IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3A/81 THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, MSC Server enhance for ICS.
c72:	IF A.4/70 THEN o ELSE n/a - - communications resource priority for the session initiation protocol

c74:	IF A.3/4 OR A.3/1 THEN o ELSE n/a. - - S-CSCF or UE.
c75:	IF A.3/1 THEN o ELSE n/a. - - UE.
c76:	IF A.4/75A OR A.4/75B THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP, a recipient within the framework for consent-based communications in SIP.
c77:	IF A.4/59 OR A.4/61 OR A.4/62 OR A.4/63 THEN m ELSE o - - multiple-recipient MESSAGE requests in the session initiation protocol, referring to multiple resources in the session initiation protocol, conference establishment using request-contained lists in the session initiation protocol, subscriptions to request-contained resource lists in the session initiation protocol.
c78:	IF (A.4/59 OR A.4/61 OR A.4/62 OR A.4/63) AND (A.3A/11 OR A.3A/31) THEN m ELSE o - - multiple-recipient MESSAGE requests in the session initiation protocol, referring to multiple resources in the session initiation protocol, conference establishment using request-contained lists in the session initiation protocol, subscriptions to request-contained resource lists in the session initiation protocol, conference focus, messaging application server.
c79:	IF A.3/9B OR A.3/13B OR (A.3/1 AND (A.4/2B OR A.4/15 OR A.4/20 OR A.4/27)) THEN m ELSE IF A.3/6 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, initiating a session, the REFER method, SIP specific event notification, a messaging mechanism for the Session Initiation Protocol (SIP), AS acting as terminating UA, or redirect server, AS performing 3rd party call control.
c80:	IF A.4/2B OR A.4/15 OR A.4/20 OR A.4/27 THEN m ELSE n/a - - initiating a session, the REFER method, SIP specific event notification, a messaging mechanism for the Session Initiation Protocol (SIP).
c81:	IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE IF A.3/9B OR A.3/13B THEN m ELSE n/a - - UE, MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).
c82:	IF A.3/6 THEN m ELSE n/a - - MGCF.
c85:	IF A.3/1 OR A.3A/81 OR A.3/2 OR A.3/7B THEN m ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS acting as originating UA.
c86:	IF A.4/3 OR A.4/4 THEN m ELSE n/a - - client behaviour for INVITE requests, server behaviour for INVITE requests.
c87:	IF A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C THEN m ELSE o - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).
c88:	IF A.3/1 OR A.3/2 THEN m ELSE o - - UE, P-CSCF.
c89:	IF A.3/7A OR A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control, MRFC.
c90:	IF A.4/13 OR A.3A/53 OR A.3A/54 OR A.3A/91 OR A.3A/85 OR A.3A/86 THEN m ELSE o - - SIP INFO method and package framework, advice of charge application server, advice of charge UA client, malicious communication identification application server, in-dialog overlap signalling application server, in-dialog overlap signalling UA client.
c91:	IF A.3A/61 OR A.3A/62 OR A.3A/63 OR A.3A/71 THEN m ELSE o - - SM-over-IP sender, SM-over-IP receiver, IP-SM-GW, IP-SM-GW.
c93:	IF A.3/7B OR A.3/7D OR A3A/84 THEN o ELSE n/a - - AS acting as originating UA, AS performing 3rd party call control, EATF.
c94:	IF A.3/4 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - S-CSCF and AS acting as terminating UA or redirect server or AS performing 3rd party call control.
c95	IF A.3/7 THEN o else n/a - - AS.
c96:	IF A.4/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c97:	IF (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) AND A.4/30 THEN m ELSE IF (A.3/7D OR A.3/11 OR A.3C/1) AND A.4/30 THEN o ELSE n/a - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), AS performing 3rd party call control, E-CSCF, UE performing the functions of an external attached network and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c98:	IF A.3/7D OR A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C OR A.3C/1 OR A3A/84 OR A.3A/89 THEN m ELSE n/a - - AS performing 3rd party call control, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE performing the functions of an external attached network, EATF, ATCF (UA).
c99:	IF A.4/15 AND (A.3/9B OR A.3/9C OR A.13/B OR A.13/C) THEN m ELSE IF A.4/15 THEN o ELSE n/a - - the REFER method, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).
c100:	IF A.3/6 OR A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 THEN m ELSE o - - MGCF, customized alerting tones application server, customized alerting tones UA client, customized ringing signal application server, customized ringing signal UA client.
c101:	IF A.3D/30 THEN m ELSE n/a - - end-to-access-edge media security using SDES.
c102:	IF A.3A/11 OR A.3A/12 OR A.3/9 THEN m ELSE n/a - - conference focus, conference participant, IBCF.
c103:	IF A.3/1 THEN o ELSE IF A.3/2 OR A.3/4 THEN m ELSE n/a - - UE, P-CSCF, S-CSCF.
c104:	IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.

c105: IF A.3/9B OR A.3/13B OR A.3A/82 OR A.3A/83 OR A.3A/87 OR A.3A/89 THEN m ELSE o - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), ICS user agent, SCC application server, Session continuity controller UE, ATCF (UA).
c106: IF A.3A/50A OR A.3A/83 OR A.3A/89 THEN m ELSE o - - Multimedia telephony application server, SCC application server, ATCF (UA).
c107: IF A.3C/1 OR A.4/2 THEN o ELSE n/a - - UE performing the functions of an external attached network, registrar.
c108: IF A.3/7 OR A.3/8 OR A.3/8A THEN o ELSE n/a - - AS, MRFC, MRB.
c109: IF A.4/76 THEN o ELSE n/a - - a mechanism for transporting user to user call control information in SIP.
c110: IF A.3/1 THEN m ELSE IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE n/a - - UE, P-CSCF, I-CSCF, S-CSCF.
c111: IF A.3/1 OR A.3/2 THEN m ELSE n/a - - UE, P-CSCF.
c112: IF NOT (A.3/1 AND NOT A.3C/1) THEN o ELSE n/a - - not UE, UE performing the functions of an external attached network.
c113: IF A.4/104 THEN o.7 ELSE n/a - - SIP overload control.
c114: IF A.4/104 THEN IF A.3/4 OR A.3/7 OR A.3/10 THEN o.7 ELSE n/a - - SIP overload control, S-CSCF, AS, additional routeing functionality.
o.1: At least one of these capabilities is supported.
o.2: At least one of these capabilities is supported.
o.3: At least one of these capabilities is supported.
o.4: At least one of these capabilities is supported.
o.5: At least one of these capabilities is supported.
o.6: It is mandatory to support at least one of these items.
o.7: At least one of these capabilities is supported.
c_dt1 IF CDIV OR interworking with CDIV THEN m ELSE o

c_dt2 IF ACR OR interworking with ACR THEN m ELSE n/a

c_dt3 IF 3PTY (INVITE) OR ECT THEN m OR IF end to end correlation (all succeeding SIP messages following Initial Request within the Dialog) THEN o ; Session ID must contain the hashed call id value.

c_dt4 IF support of DSS1 access THEN m ELSE n/a.

NOTE 1: An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.

NOTE 2: If a UE is unable to become engaged in a service that potentially requires the ability to identify and interact with a specific UE even when multiple UEs share the same single Public User Identity then the UE support can be "o" instead of "m". Examples include telemetry applications, where point-to-point communication is desired between two users.

NOTE3; Void

NOTE 4: Future Requirement with regard to End to end correlation.

NOTE 5: This Reference is shown within Section 2 of this document.

Editor's note: [WI: IMSProtoc3, CR#3107] In table A.4, item 90, the reference needs to be draft-ietf-sipcore-rfc4244bis-00 (February 2010): "An Extension to the Session Initiation Protocol (SIP) for Request History Information" which will replace document [66] in the future.

Prerequisite A.4/20 - - SIP specific event notification

Table A.4A: Supported event packages

Item	Does the implementation support	Subscriber				Notifier			
		Ref.	RFC status	Profile status	*UE profile*	Ref.	RFC status	Profile status	*UE profile*
1	reg event package?	[43]	c1	c3	*o*	[43]	c2	c4	*o*

1A	reg event package extension for GRUUs?	[94]	c1	c25	c_dt2	[94]	c2	c4	c_dt2
2	refer package?	[36] 3	c13	c13	m	[36] 3	c13	c13	m
3	presence package?	[74] 6	c1	c5	o	[74] 6	c2	c6	o
4	eventlist with underlying presence package?	[75], [74] 6	c1	c7	o	[75], [74] 6	c2	c8	o
5	presence.winfo template-package?	[72] 4	c1	c9	o	[72] 4	c2	c10	o
6	xcap-diff package?	[77] 4	c1	c11	o	[77] 4	c2	c12	o
7	conference package?	[78] 3	c1	c21	o	[78] 3	c1	c22	o
8	message-summary package?	[65]	c1	c23	m	[65] 3	c2	c24	m
9	poc-settings package?	[110]	c1	c26	o	[110]	c2	c27	o
10	debug event package?	[140]	c1	c28	o	[140]	c2	c4	o
11	dialog event package?	[171]	c1	c14	o	[171]	c2	c15	o
12	load-control package?	[201]	c29	c30	o	[201]	c29	c31	o
13	call completion event package?	See [Ref_dt2] Note 2	c1	c_dt1	m	See [Ref_dt2] Note 2	c2	c_dt1	M
14	ua-profile package?	1TR126	c1	c11	m	1TR126	c2	c12	m

Conditions:

c1: IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.
c2: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c3: IF A.3/1 OR A.3A/81 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS.
c4: IF A.3/4 THEN m ELSE IF A.3C/1 THEN o ELSE n/a - - S-CSCF, UE performing the functions of an external attached network.
c5: IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.
c6: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c7: IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.
c8: IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.
c9: IF A.3A/2 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.
c10: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c11: IF A.3A/2 OR A.3A/4 OR A.3A/56 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent or watcher or Ut reference point XCAP client for supplementary services, acting as the subscriber to event information.
c12: IF A.3A/1 OR A.3A/3 OR A.3A/55 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server or Ut reference point XCAP server for supplementary services, acting as the notifier of event information.
c13: IF A.4/15 THEN m ELSE n/a - - the REFER method.
c14: IF A.3/12 OR A.3A/87 THEN m ELSE IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - LRF, session continuity controller UE, UE, AS acting as originating UA, AS performing 3rd party call control.
c15: IF A.3/11 OR A.3A/83 THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - E-CSCF, SCC application server, UE, AS acting as terminating UA, or redirect server, AS performing 3rd party call control.
c21: IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.
c22: IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.
c23: IF A.3A/52 THEN m ELSE (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/23 THEN o ELSE n/a - - message waiting indication subscriber UA, UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as subscriber of event information.
c24: IF A.3A/52 THEN m ELSE (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/22 THEN o ELSE n/a - - message waiting indication notifier UA, UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as notifier of event information.
c25: IF A.4A/1 THEN (IF A.3/1 AND A.4/53 THEN m ELSE o) ELSE n/a - - reg event package, UE, reg event package extension for GRUUs.
c26: IF (A.3/7B OR A.3/1) AND (A.4/23 OR A.4/41) THEN o ELSE n/a - - AS acting as originating UA, UE ,acting as the subscriber to event information, an event state publication extension to the session initiation protocol.
c27: IF (A.4/22 OR A.4/41) AND A.3/1 THEN o ELSE n/a - - UE, acting as the notifier of event information, an event state publication extension to the session initiation protocol.
c28: IF A.3/1 OR A.3A/81 OR A.3/2 OR A.3/7B THEN m ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS acting as originating UA.
c29: IF A.4/104B THEN m ELSE n/a - - distribution of load filters.
c30: IF A.4/104B THEN IF A.3/4 OR A.3/7 OR A.3/9 THEN m ELSE n/a - - distribution of load filters. S-CSCF, IBCF, AS.
c31: IF A.4/104B THEN If A.3/7 THEN m ELSE n/a - - distribution of load filters, AS.

c_dt1: IF CCBS THEN m ELSE n/a (only used between AS).

c_dt2: IF A.4A/1 THEN m ELSE o.

Note 1: The event Packages could be also used within the context of Publisher

Note 2: This Reference is shown within Section 2 of this document, This draft is needed to support CCBS.

Editor's Note: It is FFS whether other IMS entities will be added to condition c28.

Prerequisite A.4/13 - - SIP INFO method and package framework.

Table A.4B: Supported info packages

Item	Does the implementation support	Sender			Receiver		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	DTMF info package?	Annex P	n/a	c1	Annex P	n/a	c1
2	g.3gpp.mid-call?	[8M]	n/a	~~c2~~ n/a	[8M]	n/a	~~c3~~ n/a
3	g.3gpp.ussd?	[8W]	n/a	~~c4~~ n/a	[8W]	n/a	~~c4~~ n/a
c1:	IF A.3/6 OR A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 THEN m ELSE o - - MGCF, customized alerting tones application server, customized alerting tones UA client, customized ringing signal application server, customized ringing signal UA client.						
c2:	IF A.3A/83 THEN o ELSE n/a - - SCC application server.						
c3:	IF A.3A/81 THEN o ELSE n/a - - MSC server enhanced for ICS.						
c4:	IF A.3A/92 OR A.3A/93 THEN m ELSE n/a - - USSI UE, USSI AS.						

Table A.4C: Supported media control packages

Item	Does the implementation support	Sender			Receiver		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	msc-ivr/1.0	[147]		~~c1~~ n/a	[147]		~~c2~~ n/a
2	msc-mixer/1.0	[148]		~~c1~~ n/a	[148]		~~c2~~ n/a
3	mrb-publish/1.0	[192]		~~c3~~ n/a	[192]		~~c4~~ n/a
c1:	IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.						
c2:	IF A.3/8 THEN o ELSE n/a - - MRFC.						
c3:	IF A.3/8 THEN o ELSE n/a - - MRFC.						
c4:	IF A.3/8A THEN o ELSE n/a - - MRB.						

A.2.1.3 PDUs

Table A.5: Supported methods

See Baseline document 1TR114 Table 7-2

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	c10	c10	[26] 13	c11	c11
2	BYE request	[26] 15.1	c12	c12	[26] 15.1	c12	c12
3	BYE response	[26] 15.1	c12	c12	[26] 15.1	c12	c12
4	CANCEL request	[26] 9	m	m	[26] 9	m	m
5	CANCEL response	[26] 9	m	m	[26] 9	m	m
6	INFO request	[25] 4.2	c21	c21	[25] 4.2	c21	c21
7	INFO response	[25] 4.2	c21	c21	[25] 4.2	c21	c21
8	INVITE request	[26] 13	c10	c10	[26] 13	c11	c11
9	INVITE response	[26] 13	c11	c11	[26] 13	c10	c10
9A	MESSAGE request	[50] 4	c7	c7	[50] 7	c7	c7
9B	MESSAGE response	[50] 4	c7	c7	[50] 7	c7	c7
10	NOTIFY request	[28] 8.1.2	c4	c4	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c4	c4
12	OPTIONS request	[26] 11	m	m	[26] 11	m	m
13	OPTIONS response	[26] 11	m	m	[26] 11	m	m
14	PRACK request	[27] 6	c5	c5	[27] 6	c5	c5
15	PRACK response	[27] 6	c5	c5	[27] 6	c5	c5
15A	PUBLISH request	[70] 11.1.3	c20	c20	[70] 11.1.3	c20	c20
15B	PUBLISH response	[70] 11.1.3	c20	c20	[70] 11.1.3	c20	c20
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 10	c8	c8	[26] 10	c9	c9
19	REGISTER response	[26] 10	c9	c9	[26] 10	c8	c8
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c4	c4
21	SUBSCRIBE response	[28] 8.1.1	c4	c4	[28] 8.1.1	c3	c3
22	UPDATE request	[29] 6.1	c6	c6	[29] 6.2	c6	c6
23	UPDATE response	[29] 6.2	c6	c6	[29] 6.1	c6	c6

c1: IF A.4/15 THEN m ELSE n/a - - the REFER method extension.
c3: IF A.4/23 THEN m ELSE n/a - - recipient for event information.
c4: IF A.4/22 THEN m ELSE n/a - - notifier of event information.
c5: IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses extension.
c6: IF A.4/17 THEN m ELSE n/a - - the SIP update method extension.
c7: IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.
c8: IF A.4/1 THEN m ELSE n/a - - client behaviour for registration.
c9: IF A.4/2 THEN m ELSE n/a - - registrar.
c10: IF A.4/3 THEN m ELSE n/a - - client behaviour for INVITE requests.
c11: IF A.4/4 THEN m ELSE n/a - - server behaviour for INVITE requests.
c12: IF A.4/5 THEN m ELSE n/a - - session release.
c20: IF A.4/41 THEN m ELSE n/a - - event state publication extension.
c21: IF A.4/13 OR A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.

A.2.1.4 PDU parameters

A.2.1.4.1 Status-codes

Table A.6: Supported status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status UNI(Gm)	Ref.	RFC status	Profile status UNI(Gm)
1	100 (Trying)	[26] 21.1.1	c21	c21	[26] 21.1.1	c11	c11
101	1xx response	[26] 21.1	p21	p21	[26] 21.1	p21	p21
101A	18x response	[26] 21.1	p21	p21	[26] 21.1	p21	p21
2	180 (Ringing)	[26] 21.1.2	c2	c2	[26] 21.1.2	c1	c1
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c2	c2	[26] 21.1.3	c1	c1
4	182 (Queued)	[26] 21.1.4	c2	c2	[26] 21.1.4	c1	c1
5	183 (Session Progress)	[26] 21.1.5	c34	c34	[26] 21.1.5	c1	c1
5A	199 (Early Dialog Terminated)	[142] 11.1	c32	c32	[142] 11.1	c32	c32
102	2xx response	[26] 21.2	p22	p22	[26] 21.1	p22	p22
6	200 (OK)	[26] 21.2.1	m	m	[26] 21.2.1	m	m
7	202 (Accepted)	[28] 8.3.1	c3	c3	[28] 8.3.1	c3	c3
103	3xx response	[26] 21.3	p23	p23	[26] 21.1	p23	p23
8	300 (Multiple Choices)	[26] 21.3.1	m	~~m~~ n/a (Note 3)	[26] 21.3.1	m	~~m~~ n/a (Note 4)
9	301 (Moved Permanently)	[26] 21.3.2	m	~~m~~ n/a (Note 3)	[26] 21.3.2	m	~~m~~ n/a (Note 4)
10	302 (Moved Temporarily)	[26] 21.3.3	m	~~m~~	[26] 21.3.3	m	~~m~~ n/a (Note 4)
11	305 (Use Proxy)	[26] 21.3.4	m	~~m~~	[26] 21.3.4	m	m
12	380 (Alternative Service)	[26] 21.3.5	m	~~m~~	[26] 21.3.5	m	~~m~~ n/a (Note 4)
104	4xx response	[26] 21.4	p24	p24	[26] 21.4	p24	p24
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	m	m
14	401 (Unauthorized)	[26] 21.4.2	o	c12	[26] 21.4.2	m	M (Note 2)
15	402 (Payment Required)	[26] 21.4.3	n/a	n/a	[26] 21.4.3	n/a	n/a
16	403 (Forbidden)	[26] 21.4.4	m	m	[26] 21.4.4	m	M (Note 5)
17	404 (Not Found)	[26] 21.4.5	m	m	[26] 21.4.5	m	M
18	405 (Method Not Allowed)	[26] 21.4.6	m	m	[26] 21.4.6	m	m
19	406 (Not Acceptable)	[26] 21.4.7	m	m	[26] 21.4.7	m	m
20	407 (Proxy Authentication Required)	[26] 21.4.8	o	o	[26] 21.4.8	m	m
21	408 (Request Timeout)	[26] 21.4.9	c2	c2	[26] 21.4.9	m	m
22	410 (Gone)	[26] 21.4.10	m	m	[26] 21.4.10	m	m
22A	412 (Conditional Request Failed)	[70] 11.2.1	c20	c20	[70] 11.2.1	c20	c20
23	413 (Request Entity Too Large)	[26] 21.4.11	m	m	[26] 21.4.11	m	m
24	414 (Request-URI Too Large)	[26] 21.4.12	m	m	[26] 21.4.12	m	m
25	415 (Unsupported Media Type)	[26] 21.4.13	m	m	[26] 21.4.13	m	m
26	416 (Unsupported URI Scheme)	[26] 21.4.14	m	m	[26] 21.4.14	m	m
26A	417 (Unknown Resource Priority)	[116] 4.6.2	c24	c24	[116] 4.6.2	c24	c24
27	420 (Bad Extension)	[26] 21.4.15	m	c13	[26] 21.4.15	m	m
28	421 (Extension Required)	[26] 21.4.16	o	o	[26] 21.4.16	i	i
28A	422 (Session Interval Too Small)	[58] 6	c7	c7	[58] 6	c7	c7
29	423 (Interval Too Brief)	[26] 21.4.17	c4	c4	[26] 21.4.17	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status UNI(Gm)	Ref.	RFC status	Profile status UNI(Gm)
29A	424 (Bad Location Information)	[89] 4.2	c23	c23	[89] 4.2	c23	c23
29B	429 (Provide Referrer Identity)	[59] 5	c8	c8	[59] 5	c9	c9
29C	430 (Flow Failed)	[92] 11	n/a	n/a	[92] 11	c22	c22
29D	433 (Anonymity Disallowed)	[67] 4	c14	c14	[67] 4	c14	c14
29E	439 (First Hop Lacks Outbound Support)	[92] 11	c28	c28	[92] 11	c29	c29
29F	440 (Max Breadth Exceeded)	[117] 5	n/a	c30	[117] 5	c31	c31
29G	469 (Bad INFO Package)	[25] 4.2	c33	c33	[25] 4.2	c33	c33
30	480 (Temporarily Unavailable)	[26] 21.4.18	m	m	[26] 21.4.18	m	m
31	481 (Call/Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	m	m
32	482 (Loop Detected)	[26] 21.4.20	m	m	[26] 21.4.20	m	m
33	483 (Too Many Hops)	[26] 21.4.21	m	m	[26] 21.4.21	m	m
34	484 (Address Incomplete)	[26] 21.4.22	o	o	[26] 21.4.22	m	m
35	485 (Ambiguous)	[26] 21.4.23	o	o	[26] 21.4.23	m	m
36	486 (Busy Here)	[26] 21.4.24	m	m	[26] 21.4.24	m	m
37	487 (Request Terminated)	[26] 21.4.25	m	m	[26] 21.4.25	m	m
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	m	m
39	489 (Bad Event)	[28] 7.3.2	c3	c3	[28] 7.3.2	c3	c3
40	491 (Request Pending)	[26] 21.4.27	m	m	[26] 21.4.27	m	m
41	493 (Undecipherable)	[26] 21.4.28	m	m	[26] 21.4.28	m	m
41A	494 (Security Agreement Required)	[48] 2	c5	c5	[48] 2	c6	c6
105	5xx response	[26] 21.5	p25	p25	[26] 21.5	p25	p25
42	500 (Internal Server Error)	[26] 21.5.1	m	m	[26] 21.5.1	m	m
43	501 (Not Implemented)	[26] 21.5.2	m	m	[26] 21.5.2	m	m
44	502 (Bad Gateway)	[26] 21.5.3	o	o	[26] 21.5.3	m	m
45	503 (Service Unavailable)	[26] 21.5.4	m	m	[26] 21.5.4	m	m
46	504 (Server Time-out)	[26] 21.5.5	m	m	[26] 21.5.5	m	m
47	505 (Version not supported)	[26] 21.5.6	m	m	[26] 21.5.6	m	m
48	513 (Message Too Large)	[26] 21.5.7	m	m	[26] 21.5.7	m	m
49	580 (Precondition Failure)	[30] 8	c35	c35	[30] 8	c35	c35
106	6xx response	[26] 21.6	p26	p26	[26] 21.6	p26	p26
50	600 (Busy Everywhere)	[26] 21.6.1	m	m	[26] 21.6.1	m	m
51	603 (Decline)	[26] 21.6.2	c10	c10	[26] 21.6.2	m	m
52	604 (Does Not Exist Anywhere)	[26] 21.6.3	m	m	[26] 21.6.3	m	m
53	606 (Not Acceptable)	[26] 21.6.4	m	m	[26] 21.6.4	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status UNI(Gm)	Ref.	RFC status	Profile status UNI(Gm)

c1: IF A.5/9 THEN m ELSE n/a - - INVITE response.
c2: IF A.5/9 THEN o ELSE n/a - - INVITE response.
c3: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c4: IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c5: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c6: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c7: IF A.4/42 AND (A.5/9 OR A.5/23) THEN m ELSE n/a - - the SIP session timer AND (INVITE response OR UPDATE response).
c8: IF A.4/43 AND A.5/17 THEN o ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c9: IF A.4/43 AND A.5/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c10: IF A.4/44 THEN m ELSE o - - the Session Inititation Protocol (SIP) "Replaces" header.
c11: IF A.5/3 OR A.5/9 OR A.5/9B OR A.5/11OR A.5/13 OR A.5/15 OR A.5/15B OR A.5/17 OR A.5/19 OR A.5/21 OR A.5/23 THEN m ELSE n/a - - BYE response or INVITE response or MESSAGE response or NOTIFY response or OPTIONS response or PRACK response or PUBLISH response or REFER response or REGISTER response or SUBSCRIBE response or UPDATE response.
c12: IF A.3/4 THEN m ELSE o - - S-CSCF.
c13: IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE, P-CSCF, S-CSCF.
c14: IF A.4/48 THEN m ELSE n/a - - rejecting anonymous requests in the session initiation protocol.
c20: IF A.4/41 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.
c21: IF A.5/3 OR A.5/9 OR A.5/9B OR A.5/11 or A.5/13 OR A.5/15 OR A.5/15B OR A.5/17 OR A.5/19 OR A.5/21 OR A.5/23 THEN o ELSE n/a - - BYE response or INVITE response or MESSAGE response or NOTIFY response or OPTIONS response or PRACK response or PUBLISH response or REFER response or REGISTER response or SUBSCRIBE response or UPDATE response.
c22: IF A.4/57 THEN m ELSE n/a - - managing client initiated connections in SIP.
c23: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c24: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c26: IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.
c27: IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.
c28: IF A.4/2 AND A.4/57 THEN m ELSE n/a - - registrar, managing client initiated connections in SIP.
c29: IF A.4/1 AND A.4/57 THEN m ELSE n/a - - client behaviour for registration, managing client initiated connections in SIP.
c30: IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).
c31: IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c32: IF A.5/9 AND A.4/81 THEN m ELSE n/a - - INVITE response and 199 (Early Dialog Terminated) response.
c33: IF A.4/13 THEN m ELSE n/a - - SIP INFO method and package framework.
c34: IF A.4/16 OR A.3/6 THEN m ELSE IF A.5/9 THEN o ELSE n/a - - initiating a session which require local and/or remote resource reservation, MGCF, INVITE response.
c35: IF A.4/16 THEN m ELSE n/a - - integration of resource management and SIP.
p21: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 OR A.6/5A - - 1xx response.
p22: A.6/6 OR A.6/7 - - 2xx response.
p23: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 - - 3xx response.
p24: A.6/13 OR A.6/14 OR A.6/15 OR A.6/16 OR A.6/17 OR A.6/18 OR A.6/19 OR A.6/20 OR A.6/21 OR A.6/22 OR A.6/22A OR A.6/23 OR A.6/24 OR A.6/25 OR A.6/26 OR A.6/26A OR A.6/27 OR A.6/28 OR A.6/28A OR A.6/29 OR A.6/29A OR A.6/29B OR A.6/29C OR A.6/29D OR A.6/29E OR A.6/29F OR A.6/29G OR A.6/29H OR A.6/30 OR A.6/31 OR A.6/32 OR A.6/33 OR A.6/34 OR A.6/35 OR A.6/36 OR A.6/436 OR A.6/38 OR A.6/39 OR A.6/40 OR A.6/41 OR A.6/41A. - 4xx response.
p25: A.6/42 OR A.6/43 OR A.6/44 OR A.6/45 OR A.6/46 OR A.6/47 OR A.6/48 OR A.6/49 - - 5xx response
p26: A.6/50 OR A.6/51 OR A.6/52 OR A.6/53 - - 6xx response.

NOTE: Conditions c1-c21 and p21-p26 are taken over from Annex B.
Note 1: This Response is within SIP for future use defined.
Note 2: These Responses are sent in cases for Registration. Registration in another domain than the home domain is not allowed. Therefore a re INVITE can not be expected.
Note 3: IF send by an UE the NGN may ignore the Response.
Note 4: Normally not send by UE.
Note 5: General a 403 is a Indication that the user is not provisioned within the HSS. Nevertheless if 403 (Forbidden) has been received as a response to a REGISTER request, a further registration attempts shall be done after 15 sec. In case further 403 response received a with the same URI in the Contact header field Register requests are allowed with a random delay of 30- 60 minutes. .

A.2.1.4.2 ACK method

Prerequisite A.5/1 – ACK request

Table A.7: Supported header fields within the ACK request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Contact	[56B] 9.2	c9	c9	[56B] 9.2	c10	c10
2	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
7	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
8	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
11	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
13	From	[26] 20.20	m	m	[26] 20.20	m	m
13A	Max-Breadth	[117] 5.8	n/a	c14	[117] 5.8	c15	c15
14	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c16
15	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
15A	P-Access-Network-Info	[52] 4.4	c19	c20	[52] 4.4	c19	c21
15B	P-Debug-ID	[33] 4.2	c6	c12	[33] 4.2	c6	c13
15C	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
16	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
17	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
17A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
17B	Recv-Info	[25] 5.2.3	c17	c17	[25] 5.2.3	c17	c17
17C	Reject-Contact	[56B] 9.2	c9	c9	[56B] 9.2	c10	c10
18	Request-Disposition	[26] 20.32	c9	c9	[26] 20.32	c10	c10
18	Require	[26] 20.32	n/a	n/a	[26] 20.32	n/a	n/a
18A	Resource-Priority	[116] 3.1	c11	c11	[116] 3.1	c11	c11
19	Route	[26] 20.34	m	m	[26] 20.34	n/a	c16
19A	Session-ID	[162]	o	c18	[162]	o	c18
20	Timestamp	[26] 20.38	c7	c7	[26] 20.38	m	m
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o	o	[26] 20.41	m	m
23	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c2:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c8:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c10:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c11:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c12:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c13:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c14:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).
c15:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c16:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c17:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c18:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c19:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c20:	IF A.4/34 AND A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), AS, MSC Server enhanced for ICS.
c21:	IF A.4/34 AND A.3/1 OR A.3/7 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, AS.

Prerequisite A.5/1 – ACK request

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

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

A.2.1.4.3 BYE method

Prerequisite A.5/2 - - BYE request

Table A.9: Supported header fields within the BYE request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c18	c18	[56B] 9.2	c22	c22
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
9	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	From	[26] 20.20	m	m	[26] 20.20	m	m
14A	Geolocation	[89] 4.1	c23	c23	[89] 4.1	c23	c23
14B	Geolocation-Routing	[89] 4.2	c23	c23	[89] 4.2	c23	c23
14C	Max-Breadth	[117] 5.8	n/a	c29	[117] 5.8	c30	c30
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c31
16	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
16A	P-Access-Network-Info	[52] 4.4	c9	c10	[52] 4.4	c9	c11
16B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
16C	P-Charging-Function-Addresses	[52] 4.5	c13	c14	[52] 4.5	c13	c14
16D	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c12	n/a
16E	P-Debug-ID	[140]	o	c27	[140]	o	c28
16F	P-Preferred-Identity	[34] 9.2	c6	x	[34] 9.2	n/a	n/a
16G	Privacy	[33] 4.2	c7	n/a	[33] 4.2	c7	c7
17	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
18	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
18A	Reason	[34A] 2	c17	c21	[34A] 2	c24	c24
19	Record-Route	[26] 20.30	n/a	c31	[26] 20.30	n/a	c31
19A	Referred-By	[59] 3	c19	c19	[59] 3	c20	c20
19B	Reject-Contact	[56B] 9.2	c18	c18	[56B] 9.2	c22	c22
19C	Request-Disposition	[56B] 9.1	c18	c18	[56B] 9.1	c22	c22
20	Require	[26] 20.32	m	m	[26] 20.32	m	m
20A	Resource-Priority	[116] 3.1	c25	c25	[116] 3.1	c25	c25
21	Route	[26] 20.34	m	m	[26] 20.34	n/a	c31
21A	Security-Client	[48] 2.3.1	c15	c15	[48] 2.3.1	n/a	n/a
21B	Security-Verify	[48] 2.3.1	c16	c16	[48] 2.3.1	n/a	n/a
21C	Session-ID	[162]	o	c32	[162]	o	c32
22	Supported	[26] 20.37	o	o	[26] 20.37	m	m
23	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
24	To	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
25A	User-to-User	[126] 7	c26	c26	[126] 7	c26	c26
26	Via	[26] 20.42	m	m	[20] 20.42	m	m

c1:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c2:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c10:	IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG) or AS.
c11:	IF A.4/34 AND (A.3/2A OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), AS acting as terminating UA, AS acting as third-party call controller or EATF.
c12:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c13:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c14:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note).
c16:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c17:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c18:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c19:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c20:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c21:	IF A.3/2 THEN m ELSE IF A.4/38 THEN o ELSE n/a - - P-CSCF, the Reason header field for the session initiation protocol.
c22:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c23:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c24:	IF A.4/38 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c25:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.
c26:	IF A.4/76 THEN o ELSE n/a - - transporting user to user information for call centers using SIP.
c27:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c28:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c29:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c30:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c31:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c32:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
NOTE:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/2 - - BYE request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	XML Schema for PSTN	[11B]		c1	[11B]		c1
2	VoiceXML expr / namelist data	[145] 4.2	m	c2	[145] 4.2	m	c2
3	application/vnd.3gpp.ussd	[8W]		c3	[8W]		c4
c1:	IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).						
c2:	IF A.4/84 THEN m ELSE n/a - - SIP Interface to VoiceXML Media Services.						
c3:	IF A.3A/93 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI AS, IBCF, P-CSCF, ATCF (UA).						
c4:	IF A.3A/92 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI UE, IBCF, P-CSCF, ATCF (UA).						

Table A.11: Void

Prerequisite A.5/3 - - BYE response

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

Table A.11A: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/3 - - BYE response for all remaining status-codes

Table A.12: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c11	c11	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c12	c12	[89] 4.3	c12	c12
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c10	[52] 4.5	c9	c10
10D	P-Charging-Vector	[52] 4.6	c8	n/a	[52] 4.6	c8	n/a
10E	P-Debug-ID	[140]	o	c14	[140]	o	c15
10E	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10F	Privacy	[33] 4.2	c4	n/a	[33] 4.2	c4	c4
10G	Require	[26] 20.32	m	m	[26] 20.32	m	m
10H	Server	[26] 20.35	o	o	[26] 20.35	o	o
10I	Session-ID	[162]	o	c16	[162]	o	c16
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
12B	User-to-User	[126] 7	c13	c13	[126] 7	c13	c13
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	o (note)	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c4:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c5:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c6:	IF A.4/34 AND (A.3/1 OR A.3/2A ORA.3/7) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), or AS.						
c7:	IF A.4/34 AND (A.3/2A OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), AS acting as terminating UA, AS acting as third-party call controller or EATF.						
c8:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).						
c12:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c13:	IF A.4/76 THEN o ELSE n/a - - transporting user to user information for call centers using SIP.						
c14:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c15:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c16:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.13: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept-Resource-Priority	[116] 3.2	c5	c5	[116] 3.2	c5	c5
0B	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
4	Supported	[26] 20.37	o	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c4:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c5:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.13A: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.14: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0B	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
NOTE:	RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/3 - - BYE response

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

Table A.15: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.16: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.17: Void

Prerequisite A.5/3 - - BYE response

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

Table A.18: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/3 - - BYE response

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

Table A.19: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.19A: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						

Prerequisite A.5/3 - - BYE response

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

Table A.20: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/3 - - BYE response

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

Table A.20A: Supported header fields within the BYE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.21: Void

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/6 - - Additional for 200 (OK) response

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	VoiceXML expr / namelist data	[145] 4.2	o	c1	[145] 4.2	o	c1
c1:	IF A.4/84 THEN o ELSE n/a - - SIP Interface to VoiceXML Media Services.						

A.2.1.4.4 CANCEL method

Prerequisite A.5/4 - - CANCEL request

Table A.23: Supported header fields within the CANCEL request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Contact	[56B] 9.2	c9	c9	[56B] 9.2	c11	c11
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
9	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
10	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
11	From	[26] 20.20	m	m	[26] 20.20	m	m
11A	Max-Breadth	[117] 5.8	n/a	c16	[117] 5.8	c17	c17
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c18
13	P-Debug-ID	[140]	o	c14	[140]	o	c15
14	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
15	Reason	[34A] 2	c7	c10	[34A] 2	c12	c12
16	Record-Route	[26] 20.30	n/a	c18	[26] 20.30	n/a	c18
17	Reject-Contact	[56B] 9.2	c9	c9	[56B] 9.2	c11	c11
17A	Request-Disposition	[56B] 9.1	c9	c9	[56B] 9.1	c11	c11
17B	Resource-Priority	[116] 3.1	c13	c13	[116] 3.1	c13	c13
18	Route	[26] 20.34	m	m	[26] 20.34	n/a	c18
18A	Session-ID	[162]	o	c19	[162]	o	c19
19	Supported	[26] 20.37	o	o	[26] 20.37	m	m
20	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
21	To	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c6:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c7:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						
c8:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c9:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.						
c10:	IF A.3/2 THEN m ELSE IF A.4/38 THEN o ELSE n/a - - P-CSCF, the Reason header field for the session initiation protocol.						
c11:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.						
c12:	IF A.4/38 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.						
c13:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						
c14:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c15:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c16:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network..						
c17:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.						
c18:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.						
c19:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						

Prerequisite A.5/4 - - CANCEL request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	XML Schema for PSTN	[11B]		c1	[11B]		c1
c1:	IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting						

as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).

Prerequisite A.5/5 - - CANCEL response for all status-codes

Table A.25: Supported header fields within the CANCEL response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c4	[140]	o	c5
5B	Privacy	[33] 4.2	c3	n/a	[33] 4.2	c3	n/a
5C	Session-ID	[162]	o	c6	[162]	o	c6
6	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
7	To	[26] 20.39	m	m	[26] 20.39	m	m
7A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
8	Via	[26] 20.42	m	m	[26] 20.42	m	m
9	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c4:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c5:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c6:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.26: Supported header fields within the CANCEL response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
2	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
4	Supported	[26] 20.37	o	m	[26] 20.37	m	m
c1:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.26A: Supported header fields within the CANCEL response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Table A.27: Void

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.28: Supported header fields within the CANCEL response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.29: Void

Table A.30: Void

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.30A: Supported header fields within the CANCEL response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						

Prerequisite A.5/5 - - CANCEL response

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

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

A.2.1.4.5 COMET method

Void

A.2.1.4.6 INFO method

Prerequisite A.5/9A - - INFO request

Table A.32: Supported header fields within the INFO request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
4	Allow	[26] 20.5	o	o	[26] 20.5	m	m
5	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
6	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
7	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 29.15	m	m
14	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Geolocation	[89] 4.1	c29	c29	[89] 4.1	c29	c29
17A	Geolocation-Routing	[89] 4.2	c29	c29	[89] 4.2	c29	c29
18	Info-Package	[25] 7.2	c42	c42	[25] 7.2	c42	c42
19	Max-Breadth	[117] 5.8	n/a	c39	[117] 5.8	c40	c40
20	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c41
21	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
22	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
23	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
24	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
25	P-Debug-ID	[140]	o	c37	[140]	o	c38
26	Privacy	[33] 4.2	c12	c12	[33] 4.2	c12	c12
27	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
28	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
29	Reason	[34A] 2	c6	c6	[34A] 2	c6	c6
30	Record-Route	[26] 20.30	n/a	c41	[26] 20.30	n/a	c41
31	Referred-By	[59] 3	c25	c25	[59] 3	c26	c26
33	Request-Disposition	[56B] 9.1	c24	c24	[56B] 9.1	c28	c28
34	Require	[26] 20.32	m	m	[26] 20.32	m	m
35	Resource-Priority	[116] 3.1	c30	c30	[116] 3.1	c30	c30
36	Route	[26] 20.34	m	m	[26] 20.34	n/a	c41
37	Security-Client	[48] 2.3.1	c22	c22	[48] 2.3.1	n/a	n/a
38	Security-Verify	[48] 2.3.1	c23	c23	[48] 2.3.1	n/a	n/a
38A	Session-ID	[162]	o	c43	[162]	o	c43
39	Subject	[26] 20.35	o	o	[26] 20.36	o	o
40	Supported	[26] 20.37	m	m	[26] 20.37	m	m
41	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m
42	To	[26] 20.39	m	m	[26] 20.39	m	m
43	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
44	Via	[26] 20.42	m	m	[26] 20.42	m	m

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c1:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c2:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.						
c6:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						
c10:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c12:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c15:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c16:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c17:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.						
c18:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c19:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c20:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c21:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c22:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media? (note 2).						
c23:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.						
c24	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.						
c25:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.						
c26:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.						
c28:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.						
c29:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c30:	IF A.4/70A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						
c37:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c38:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c39:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.						
c40:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.						
c41:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.						
c42:	IF A.4/13A THEN n/a ELSE m - - legacy INFO usage.						
c43:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE 2:	Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].						

Prerequisite A.5/9A - - INFO request

Table A.33: Supported message bodies within the INFO request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Info-Package	[25]	m	m	[25]	m	m

Prerequisite A.5/9B - - INFO response

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

Table A.34: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/9B - - INFO response for all remaining status-codes

Table A.35: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
3	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
4	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
5	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
10	From	[26] 20.20	m	m	[26] 20.20	m	m
11	Geolocation-Error	[89] 4.3	c14	c14	[89] 4.3	c14	c14
12	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
13	Organization	[26] 20.25	o	o	[26] 20.25	o	o
14	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
15	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
16	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
17	P-Debug-ID	[140]	o	c15	[140]	o	c16
18	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
19	Require	[26] 20.32	m	m	[26] 20.32	m	m
20	Server	[26] 20.35	o	o	[26] 20.35	o	o
20A	Session-ID	[162]	o	c17	[162]	o	c17
21	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
22	To	[26] 20.39	m	m	[26] 20.39	m	m
23	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
24	Via	[26] 20.42	m	m	[26] 20.42	m	m
25	Warning	[26] 20.43	o	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c4:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c5:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c6:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c7:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.						
c8:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c10:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c12:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).						
c14:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c15:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c16:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c17:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.36: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m

4	Accept-Resource-Priority	[116] 3.2	c5	c5	[116] 3.2	c5	c5
5	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
6	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
9	Supported	[26] 20.37	o	o	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c4:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c5:	IF A.4/70A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.37: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/103 - - Additional for 3xx or 485 (Ambiguous) response

Table A.37A: Void

Prerequisite A.5/9B - - INFO response

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

Table A.38: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.39: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.40: Void

Prerequisite A.5/9B - - INFO response

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

Table A.41: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.41A: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						

Prerequisite A.5/9B - - INFO response

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

Table A.42: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9B - - INFO response

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

Table A.42A: Supported header fields within the INFO response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.43: Void

Table A.44: Void

Prerequisite A.5/9B - - INFO response

Table A.45: Supported message bodies within the INFO response

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

A.2.1.4.7 INVITE method

Prerequisite A.5/8 - - INVITE request

Table A.46: Supported header fields within the INVITE request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	c47	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c24	c24	[56B] 9.2	c32	c32
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
4	Alert-Info	[26] 20.4	o	o	[26] 20.4	c1	c1
5	Allow	[26] 20.5, [26] 5.1	o (note 1)	o	[26] 20.5, [26] 5.1	m	m
6	Allow-Events	[28] 7.2.2	c2	c2	[28] 7.2.2	c53	c53
7	Answer-Mode	[158]	c49	c49	[158]	c50	c50
8	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
9	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
10	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
11	Contact	[26] 20.10	m	m	[26] 20.10	m	m
12	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
13	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
14	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
17	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
19	Expires	[26] 20.19	o	o	[26] 20.19	o	o
19A	Feature-Caps	[190]	c59	c59	[190]	c58	c58
20	From	[26] 20.20	m	m	[26] 20.20	m	m
20A	Geolocation	[89] 4.1	c33	c33	[89] 4.1	c33	c33
20B	Geolocation-Routing	[89] 4.2	c33	c33	[89] 4.2	c33	c33
20C	History-Info	[66] 4.1	c31	c31	[66] 4.1	c31	c31
21	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
21A	Join	[61] 7.1	c30	c30	[61] 7.1	c30	c30
21B	Max-Breadth	[117] 5.8	n/a	c45	[117] 5.8	c46	c46
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c52
23	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
23A	Min-SE	[58] 5	c26	c26	[58] 5	c25	c25
24	Organization	[26] 20.25	o	o	[26] 20.25	o	o
24A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
24B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c7	c7
24C	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c38	c38
24D	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
24E	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
24F	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
24G	P-Debug-ID	[140]	o	c43	[140]	o	c44
24H	P-Early-Media	[109] 8	c34	c34	[109] 8	c34	c34
25	P-Media-Authorization	[31] 5.1	n/a	n/a	[31] 5.1	c11	c12
25A	P-Preferred-Identity	[34] 9.2	c7	c5	[34] 9.2	n/a	n/a
25B	P-Preferred-Service	[121] 4.2	c37	c36	[121] 4.2	n/a	n/a
25C	P-Private-Network-Indication	[134]	c42	c42	[134]	c42	c42
25D	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
25E	P-Served-User	[133] 6	c51	c51	[133] 6	c51	c51
25F	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
25G	P-Visited-Network-ID	[52] 4.3	x (note 3)	x	[52] 4.3	c14	n/a
26	Priority	[26] 20.26	o	o	[26] 20.26	o	o
26A	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
26B	Priv-Answer-Mode	[158]	c49	c49	[158]	c50	c50
27	Proxy-Authorization	[26] 20.28	c6	c6	[26] 20.28	n/a	n/a
28	Proxy-Require	[26] 20.29	o (note 2)	o (note 2)	[26] 20.29	n/a	n/a
28A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c55

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
29	Record-Route	[26] 20.30	n/a	c52	[26] 20.30	m	m
29A	Recv-Info	[25] 5.2.3	c48	c48	[25] 5.2.3	c48	c48
30	Referred-By	[59] 3	c27	c27	[59] 3	c28	c28
31	Reject-Contact	[56B] 9.2	c24	c24	[56B] 9.2	c32	c32
31A	Replaces	[60] 6.1	c29	c29	[60] 6.1	c29	c29
31B	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
31C	Request-Disposition	[56B] 9.1	c24	c24	[56B] 9.1	c32	c32
32	Require	[26] 20.32	m	m	[26] 20.32	m	m
32A	Resource-Priority	[116] 3.1	c35	c35	[116] 3.1	c35	c35
33	Route	[26] 20.34	m	m	[26] 20.34	n/a	c52
33A	Security-Client	[48] 2.3.1	c22	c22	[48] 2.3.1	n/a	n/a
33B	Security-Verify	[48] 2.3.1	c23	c23	[48] 2.3.1	n/a	n/a
33D	Session-Expires	[58] 4	c25	c25	[58] 4	c25	c25
33E	Session-ID	[162]	o	c54	[162]	o	c54
34	Subject	[26] 20.36	o	o	[26] 20.36	o	o
35	Supported	[26] 20.37	m	m	[26] 20.37	m	m
35A	Target-Dialog	[184] 7	c56	c56	[xxa] 7	c57	c57
36	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m
37	To	[26] 20.39	m	m	[26] 20.39	m	m
37A	Trigger-Consent	[125] 5.11.2	c39	c39	[125] 5.11.2	c40	c40
38	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
38A	User-to-User	[126] 7	c41	c41	[126] 7	c41	c41
39	Via	[26] 20.42	m	m	[26] 20.42	m	m

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c1:	IF A.4/12 THEN m ELSE n/a - - downloading of alerting information.						
c2:	IF A.4/22 THEN m ELSE n/a - - acting as the notifier of event information.						
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c5:	IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c6:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.						
c7:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c8:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c10:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c11:	IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.						
c12:	IF A.3/1 AND A.4/19 THEN m ELSE n/a - - UE, SIP extensions for media authorization.						
c13:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.						
c14:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.						
c15:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c16:	IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), the AS or the MSC server enhanced for ICS.						
c17:	IF A.4/34 AND (A.3/2A OR A.3A/81 OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), the MSC server enhanced for ICS, AS acting as terminating UA, AS acting as third-party call controller or EATF.						
c18:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c19:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c20:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c21:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c22:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 4).						
c23:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.						
c24:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.						
c25:	IF A.4/42 THEN m ELSE n/a - - the SIP session timer.						
c26:	IF A.4/42 THEN o ELSE n/a - - the SIP session timer.						
c27:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.						
c28:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.						
c29:	IF A.4/44 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Replaces" header.						
c30:	IF A.4/45 THEN m ELSE n/a - - the Session Inititation Protocol (SIP) "Join" header.						
c31:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c32:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.						
c33:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c34:	IF A.4/66 THEN m ELSE n/a - - The SIP P-Early-Media private header extension for authorization of early media.						
c35:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						
c36:	IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.						
c37:	IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.						
c38:	IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.						
c39:	IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.						
c40:	IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.						
c41:	IF A.4/76 THEN o ELSE n/a - - transporting user to user information for call centers using SIP.						
c42:	IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).						
c43:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c44:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c45:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.						
c46:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.						
c47:	IF A.3/1 AND A.4/2B THEN m ELSE o - - UE and initiating a session.						
c48:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.						

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c49:	IF A.4/87 THEN o ELSE n/a - - requesting answering modes for SIP.						
c50:	IF A.4/87 THEN m ELSE n/a - - requesting answering modes for SIP.						
c51:	IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.						
c52:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.						
c53:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c54:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
c55:	IF A.4/38 THEN IF A.3A/83 THEN m ELSE o ELSE n/a - - the Reason header field for the session initiation protocol, SCC application server.						
c56:	IF A.4/99 THEN o ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.						
c57:	IF A.4/99 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.						
c58:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						
c59:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.						
o.1:	At least one of these shall be supported.						
NOTE 1:	RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						
NOTE 2:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.						
NOTE 3:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.						
NOTE 4:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].						

Prerequisite A.5/8 - - INVITE request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	XML Schema for PSTN	[11B]		c1	[11B]		c1
2	application/vnd.3gpp.ussd	[8W]		c2	[8W]		c3
c1:	IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).						
c2:	IF A.3A/92 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI UE, IBCF, P-CSCF, ATCF (UA).						
c3:	IF A.3A/93 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI AS, IBCF, P-CSCF, ATCF (UA).						

Prerequisite A.5/9 - - INVITE response

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

Table A.48: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/9 - - INVITE response for all remaining status-codes

Table A.49: Supported headerfields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
8[a]	Expires	[26] 20.19	o	o	[26] 20.19	o	o
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c14	c14	[89] 4.3	c14	c14
9B	History-Info	[66] 4.1	c13	c13	[66] 4.1	c13	c13
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
11B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
11C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c11	c11
11D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
11E	P-Debug-ID	[140]	o	c16	[140]	o	c17
11F	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
11G	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
11H	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
11I	Require	[26] 20.32	m	m	[26] 20.32	m	m
11J	Server	[26] 20.35	o	o	[26] 20.35	o	o
11K	Session-ID	[162]	o	c18	[162]	o	c18
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13B	User-to-User	[126] 7	c15	c15	[126] 7	c15	c15
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), AS or MSC server enhanced for ICS.
c7: IF A.4/34 AND (A.3/2A OR A.3A/81 OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), MSC server enhanced for ICS, AS acting as terminating UA, AS acting as third-party call controller or EATF.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/6 OR A.6/18 THEN m ELSE o - - 200 (OK), 405 (Method Not Allowed).
c13: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c14: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c15: IF A.4/76 THEN o ELSE n/a - - transporting user to user information for call centers using SIP.
c16: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c17: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c18: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/101A - - Additional for 18x response

Table A.50: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	o	m	[26] 20.10	m	m
4A	Feature-Caps	[190]	c17	c17	[190]	c16	c16
5	P-Answer-State	[111]	c13	c13	[111]	c13	c13
5A	P-Early-Media	[109] 8	c14	c14	[109] 8	c14	c14
6	P-Media-Authorization	[31] 5.1	n/a	n/a	[31] 5.1	c11	c12
6A	Reason	[130]	o	c15	[130]	o	c15
7	Record-Route	[26] 20.30	o	m	[26] 20.30	m	m
8	Recv-Info	[25] 5.2.3	c4	c4	[25] 5.2.3	c4	c4
9	RSeq	[27] 7.1	c2	m	[27] 7.1	c3	m

c2: IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP.
c3: IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP.
c4: IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c11: IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.
c12: IF A.3/1 AND A.4/19 THEN m ELSE n/a - - UE, SIP extensions for media authorization.
c13: IF A.4/65 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.
c14: IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.
c15: IF A.4/38A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses.
c16: IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c17: IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/2 - - Additional for 180 (Ringing) response

Table A.50A: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Alert-Info	[26] 20.4	o	c1	[26] 20.4	o	c1
c1:	IF A.4/96 THEN m ELSE o - - Alert-Info URNs for the Session Initiation Protocol.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/5A - - Additional for 199 (Early Dialog Terminated) response

Table A.50B: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	o	m	[26] 20.10	m	m
5	Reason	[130]	o	c5	[130]	o	c5
7	Record-Route	[26] 20.30	o	m	[26] 20.30	m	m
8	Recv-Info	[25] 5.2.3	c4	c4	[25] 5.2.3	c4	c4
9	RSeq	[27] 7.1	c2	m	[27] 7.1	c3	m
c2:	IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP.						
c3:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP.						
c4:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.						
C5:	IF A.4/38A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses?						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.51: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
1C	Accept-Resource-Priority	[116] 3.2	c15	c15	[116] 3.2	c15	c15
2	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
3	Answer-Mode	[158]	c6	c6	[158]	c7	c7
4	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
6	Contact	[26] 20.10	m	m	[26] 20.10	m	m
6A	Feature-Caps	[190]	c18	c18	[190]	c17	c17
7	P-Answer-State	[111]	c14	c14	[111]	c14	c14
8	P-Media-Authorization	[31] 5.1	n/a	n/a	[31] 5.1	c11	c12
8A	Priv-Answer-Mode	[158]	c6	c6	[158]	c7	c7
9	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
9A	Recv-Info	[25] 5.2.3	c5	c5	[25] 5.2.3	c5	c5
10	Session-Expires	[58] 4	c13	c13	[58] 4	c13	c13
13	Supported	[26] 20.37	m	m	[26] 20.37	m	m

c1: IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.
c2: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c3: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c4: IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c5: IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c6 IF A.4/87 THEN o ELSE n/a - - requesting answering modes for SIP.
c7 IF A.4/87 THEN m ELSE n/a - - requesting answering modes for SIP.
c11: IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.
c12: IF A.3/1 AND A.4/19 THEN m ELSE n/a - - UE, SIP extensions for media authorization.
c13: IF A.4/42 THEN m ELSE n/a - - the SIP session timer.
c14: IF A.4/65 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.
c15: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c17: IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c18: IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.51A: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
2	Reason	[130]	o	c1	[130]	o	c1
c1:	IF A.4/38A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses?						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.52: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	o (note 1)	o	[26] 20.10	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9 - - INVITE response

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

Table A.53: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	c3	c3
13	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/16 - - Additional for 403 (Forbidden) response

Table A.53A: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	P-Refused-URI-List	[183]	c1	c1	[183]	c1	c1
c1:	IF A.4/98 THEN m ELSE n/a -- The SIP P-Refused-URI-List private-header.						

Table A.54: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.55: Void

Prerequisite A.5/9 - - INVITE response

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

Table A.56: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
11	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9 - - INVITE response

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

Table A.57: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.57A: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						

Prerequisite A.5/9 - - INVITE response

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

Table A.58: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
10	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9 - - INVITE response

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

Table A.58A: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

Table A.58B: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Min-SE	[58] 5	c1	c1	[58] 5	c1	c1
c1:	IF A.4/42 THEN o ELSE n/a - - the SIP session timer.						

Table A.59: Void

Table A.60: Void

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

Table A.60A: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Permission-Missing	[125] 5.9.3	m	m	[125] 5.9.3	m	m

Prerequisite A.5/9 - - INVITE response

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

Table A.61: Supported header fields within the INVITE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m

Table A.61A: Void

Prerequisite A.5/9 - - INVITE response

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	XML Schema for PSTN	[11B]		c1	[11B]		c1
2	Recipient list	[183]	c2	c2	[183]	c2	c2
3	3GPP IM CN subsystem XML body	subclause 7.6	n/a	c3	subclause 7.6	n/a	c4 (note)
c1:	IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).						
c2:	IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.						
c3:	IF A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C OR (A.4/103 AND A.3/2) OR (A.4/103 AND A.3/4) THEN m ELSE n/a - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), S-CSCF restoration procedures, P-CSCF, S-CSCF.						
c4:	IF A.3/1 OR A.3/2 OR A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C THEN m ELSE IF A.3/4 THEN o ELSE n/a - - UE, P-CSCF, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), S-CSCF.						
NOTE:	If a IBCF (IMS-ALG) or a IBCF (Screening of SIP signalling) is unable to receive a 3GPP IM CN subsystem XML body from a S-CSCF in a serving network then the IBCF (IMS-ALG) or the IBCF (Screening of SIP signalling) support can be "o" instead of "m". Examples include an S-CSCF supporting S-CSCF restoration procedures.						

A.2.1.4.7A MESSAGE method

Prerequisite A.5/9A - - MESSAGE request

Table A.62A: Supported header fields within the MESSAGE request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Contact	[56B] 9.2	c24	c24	[56B] 9.2	c28	c28
1A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
6	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
7	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
8	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 29.15	m	m
11	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
13	Expires	[26] 20.19	o	o	[26] 20.19	o	o
13A	Feature-Caps	[190]	c45	c45	[190]	c44	c44
14	From	[26] 20.20	m	m	[26] 20.20	m	m
14A	Geolocation	[89] 4.1	c29	c29	[89] 4.1	c29	c29
14B	Geolocation-Routing	[89] 4.2	c29	c29	[89] 4.2	c29	c29
14C	History-Info	[66] 4.1	c27	c27	[66] 4.1	c27	c27
15	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
15A	Max-Breadth	[117] 5.8	n/a	c39	[117] 5.8	c40	c40
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c42
17	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
18	Organization	[26] 20.25	o	o	[26] 20.25	o	o
18A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c16
18B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c11	c11
18C	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c33	c33
18D	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
18E	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
18F	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
18G	P-Debug-ID	[140]	o	c37	[140]	o	c38
18H	P-Preferred-Identity	[34] 9.2	c11	c7	[34] 9.2	n/a	n/a
18I	P-Preferred-Service	[121] 4.2	c32	c31	[121] 4.2	n/a	n/a
18J	P-Private-Network-Indication	[134]	c36	c36	[134]	c36	c36
18K	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
18L	P-Served-User	[133] 6	c41	c41	[133] 6	c41	c41
18M	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
18N	P-Visited-Network-ID	[52] 4.3	x (note 1)	x	[52] 4.3	c14	n/a
19	Priority	[26] 20.26	o	o	[26] 20.26	o	o
19A	Privacy	[33] 4.2	c12	c12	[33] 4.2	c12	c12
20	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
21	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
21A	Reason	[34A] 2	c6	c6	[34A] 2	c6	c6
22	Record-Route	[26] 20.30	n/a	c42	[26] 20.30	n/a	c42
22A	Referred-By	[59] 3	c25	c25	[59] 3	c26	c26
23	Reject-Contact	[56B] 9.2	c24	c24	[56B] 9.2	c28	c28
23A	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
23B	Request-Disposition	[56B] 9.1	c24	c24	[56B] 9.1	c28	c28
24	Require	[26] 20.32	m	m	[26] 20.32	m	m
24A	Resource-Priority	[116] 3.1	c30	c30	[116] 3.1	c30	c30
25	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
25A	Security-Client	[48] 2.3.1	c22	c22	[48] 2.3.1	n/a	n/a
25B	Security-Verify	[48] 2.3.1	c23	c23	[48] 2.3.1	n/a	n/a
25C	Session-ID	[162]	o	c43	[162]	o	c43

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
26	Subject	[26] 20.35	o	o	[26] 20.36	o	o
27	Supported	[26] 20.37	c9	m	[26] 20.37	m	m
28	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m
29	To	[26] 20.39	m	m	[26] 20.39	m	m
29A	Trigger-Consent	[125] 5.11.2	c34	c34	[125] 5.11.2	c35	c35
30	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
31	Via	[26] 20.42	m	m	[26] 20.42	m	m

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c1:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c2:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.						
c6:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						
c7:	IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c8:	IF A.4/14 THEN m ELSE o - - support of reliable transport.						
c10:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c11:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c12:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c13:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.						
c14:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.						
c15:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c16:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c17:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.						
c18:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c19:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c20:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c21:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c22:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 2).						
c23:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.						
c24:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.						
c25:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.						
c26:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.						
c27:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c28:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.						
c29:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c30:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						
c31:	IF A.3/1 AND A.4/74 THEN o ELSE n/a - - UE and SIP extension for the identification of services.						
c32:	IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.						
c33:	IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.						
c34:	IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.						
c35:	IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.						
c36:	IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).						
c37:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c38:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c39:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.						
c40:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.						
c41:	IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.						
c42:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.						
c43:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
c44:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						
c45:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.						
NOTE 1:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.						
NOTE 2:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].						

Prerequisite A.5/9A - - MESSAGE request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	permission document	[125] 5.4	c1	c1	[125] 5.4	c2	c2
2	application/vnd.3gpp.sms	[4D]	c3	c3	[4D]	c3	c3
3	message/cpim	[151]	c4	c4	[151]	c4	c4
4	message/imdn+xml	[157]	c5	c5	[157]	c5	c5
c1:	IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.						
c2:	IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.						
c3:	IF A.3A/61 OR A.3A/62 OR A.3A/63 THEN m ELSE o - - an SM-over-IP sender or an SM-over-IP receiver or an IP-SM-GW for SMS over IP.						
c4:	IF A.3A/71 AND A.4/85 THEN m ELSE n/a - - common presence and instant messaging (CPIM): message format.						
c5:	IF A.3A/71 AND A.4/86 THEN m ELSE n/a - - instant message disposition notification.						

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62BA: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/9B - - MESSAGE response for all remaining status-codes

Table A.62C: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
3	Content-Disposition	[26] 20.11	o (note 1)	o (note 1)	[26] 20.11	m (note 1)	m (note 1)
4	Content-Encoding	[26] 20.12	o (note 1)	o (note 1)	[26] 20.12	m (note 1)	m (note 1)
5	Content-Language	[26] 20.13	o (note 1)	o (note 1)	[26] 20.13	m (note 1)	m (note 1)
6	Content-Length	[26] 20.14	m (note 1)	m (note 1)	[26] 20.14	m (note 1)	m (note 1)
7	Content-Type	[26] 20.15	m (note 1)	m (note 1)	[26] 20.15	m (note 1)	m (note 1)
8	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9A	Expires	[26] 20.19	o	o	[26] 20.19	o	o
10	From	[26] 20.20	m	m	[26] 20.20	m	m
10A	Geolocation-Error	[89] 4.3	c14	c14	[89] 4.3	c14	c14
10B	History-Info	[66] 4.1	c13	c13	[66] 4.1	c13	c13
11	MIME-Version	[26] 20.24	o (note 1)	o (note 1)	[26] 20.24	m (note 1)	m (note 1)
12	Organization	[26] 20.25	o	o	[26] 20.25	o	o
12A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
12B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
12C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
12D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
12E	P-Debug-ID	[140]	o	c15	[140]	o	c16
12F	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
12G	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
12H	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
12I	Require	[26] 20.32	m	m	[26] 20.32	m	m
13	Server	[26] 20.35	o	o	[26] 20.35	o	o
13A	Session-ID	[162]	o	c17	[162]	o	c17
14	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
15	To	[26] 20.39	m	m	[26] 20.39	m	m
16	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
17	Via	[26] 20.42	m	m	[26] 20.42	m	m
18	Warning	[26] 20.43	o	o	[26] 20.43	o	o

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).
c13: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c14: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c15: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c16: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c17: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.

NOTE 1:	RFC 3428 [50] clause 7 states that all 2xx class responses to a MESSAGE request must not include any body, therefore for 2xx responses to the MESSAGE request the values on Sending side for "RFC status" and "Profile status" are "x", the values for Receiving side for "RFC status" and "Profile Status" are "n/a". RFC 3261 [26] subclause 7.4 states that all responses may contain bodies, therefore for all responses to the MESSAGE request other than 2xx responses, the values on Sending side for "RFC status" and "Profile status" are "o", the values for Receiving side for "RFC status" and "Profile Status" are "m".

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.62D: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept-Resource-Priority	[116] 3.2	c5	c5	[116] 3.2	c5	c5
1	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	Feature-Caps	[190]	c8	c8	[190]	c7	c7
6	Supported	[26] 20.37	o	o	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c4:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c5:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						
c7:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						
c8:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.62DA: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/103 - - Additional for 3xx or 485 (Ambiguous) response

Table A.62E: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62F: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.62G: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.62H: Void

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62I: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62J: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.62JA: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62K: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9B - - MESSAGE response

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

Table A.62L: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.62M: Void

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

Table A.62MA: Supported header fields within the MESSAGE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Permission-Missing	[125] 5.9.3	m	m	[125] 5.9.3	m	m

Prerequisite A.5/9B - - MESSAGE response

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

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

A.2.1.4.8 NOTIFY method

Prerequisite A.5/10 - - NOTIFY request

Table A.63: Supported header fields within the NOTIFY request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c19	c19	[56B] 9.2	c23	c23
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Call-Info	[26] 20.9	o	o	[26] 20.9	c25	c25
6B	Contact	[26] 20.10	m	m	[26] 20.10	m	m
7	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
9	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	Event	[28] 7.2.1	m	m	[28] 7.2.1	m	m
14A	Feature-Caps	[190]	c35	c35	[190]	c34	c34
15	From	[26] 20.20	m	m	[26] 20.20	m	m
15A	Geolocation	[89] 4.1	c24	c24	[89] 4.1	c24	c24
15B	Geolocation-Routing	[89] 4.2	c24	c24	[89] 4.2	c24	c24
15C	History-Info	[66] 4.1	c22	c22	[66] 4.1	c22	c22
15D	Max-Breadth	[117] 5.8	n/a	c26	[117] 5.8	c27	c27
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c32
17	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
17A	P-Access-Network-Info	[52] 4.4	c10	c11	[52] 4.4	c10	c12
17B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
17C	P-Charging-Function-Addresses	[52] 4.5	c14	c15	[52] 4.5	c14	c15
17D	P-Charging-Vector	[52] 4.6	c13	n/a	[52] 4.6	c13	n/a
17E	P-Debug-ID	[140]	o	c30	[140]	o	c31
17F	P-Preferred-Identity	[34] 9.2	c6	x	[34] 9.2	n/a	n/a
17G	Privacy	[33] 4.2	c7	n/a	[33] 4.2	c7	c7
18	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
19	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
19A	Reason	[34A] 2	c18	c18	[34A] 2	c18	c18
20	Record-Route	[26] 20.30	n/a	c32	[26] 20.30	c9	c9
20A	Referred-By	[59] 3	c20	c20	[59] 3	c21	c21
20B	Reject-Contact	[56B] 9.2	c19	c19	[56B] 9.2	c23	c23
20C	Request-Disposition	[56B] 9.1	c19	c19	[56B] 9.1	c23	c23
21	Require	[26] 20.32	m	m	[26] 20.32	m	m
22A	Resource-Priority	[116] 3.1	c29	c29	[116] 3.1	c29	c29
22B	Security-Client	[48] 2.3.1	c16	c16	[48] 2.3.1	n/a	n/a
22C	Security-Verify	[48] 2.3.1	c17	c17	[48] 2.3.1	n/a	n/a
22D	Session-ID	[162]	o	c33	[162]	o	c33
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	c32
23	Subscription-State	[28] 8.2.3	m	m	[28] 8.2.3	m	m
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
28	Via	[26] 20.42	m	m	[26] 20.42	m	m
29	Warning	[26] 20.43	o	o	[26] 20.43	o	o

c1:	IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c2:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9:	IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension.
c10:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c11:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c12:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c13:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c14:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c16:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note).
c17:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c18:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c19:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c20:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c21:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c22:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c23:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c24:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c25:	IF A.4/63 THEN m ELSE o - - subscriptions to request-contained resource lists in the session initiation protocol.
c26:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c27:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c29:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.
c30:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c31:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c32::	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c33:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c34:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c35:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.
NOTE:	Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/10 - - NOTIFY request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	sipfrag	[37] 2	c1	c1	[37]	c1	c1
2	event package (see NOTE)	[28]	m	m	[28]	m	m
c1:	IF A.4/15 THEN m ELSE o - - the REFER method extension						
NOTE:	The appropriate body specified for the supported event package (see table A.4A) is supported.						

Prerequisite A.5/11 - - NOTIFY response

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

Table A.64A: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/11 - - NOTIFY response for all remaining status-codes

Table A.65: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c12	c12	[89] 4.3	c12	c12
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c10	[52] 4.5	c9	c10
10D	P-Charging-Vector	[52] 4.6	c8	n/a	[52] 4.6	c8	n/a
10E	P-Debug-ID	[140]	o	c13	[140]	o	c14
10F	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10G	Privacy	[33] 4.2	c4	n/a	[33] 4.2	c4	c4
10H	Require	[26] 20.32	m	m	[26] 20.32	m	m
10I	Server	[26] 20.35	o	o	[26] 20.35	o	o
10J	Session-ID	[162]	o	c15	[162]	o	c15
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c4:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c5:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c6:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c7:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.						
c8:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).						
c12:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c13	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c14	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c15:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.66: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept-Resource-Priority	[116] 3.2	c6	c6	[116] 3.2	c6	c6
0B	Allow-Events	[28] 7.2.2	c4	c4	[28] 7.2.2	c5	c5

1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
1A	Contact	[26] 20.10	o	o	[26] 20.10	m	m
1B	Feature-Caps	[190]	c8	c8	[190]	c8	c8
2	Record-Route	[26] 20.30	c3	c3	[26] 20.30	c3	c3
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension.						
c4:	IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.						
c5:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.						
c6:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						
c8:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.66A: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/103 - - Additional for 3xx response

Table A.67: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	m	m	[26] 20.10	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.68: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.69: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.70: Void

Prerequisite A.5/11 - - NOTIFY response

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

Table A.71: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	c3	c3
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c3:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/11 - - NOTIFY response

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

Table A.72: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.72A: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						

Prerequisite A.5/11 - - NOTIFY response

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

Table A.73: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.73A: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.74: Void

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/35 - - Additional for 485 (Ambigious) response

Table A.74A: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o	o	[26] 20.10	m	m

Prerequisite A.5/11 - - NOTIFY response

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

Table A.75: Supported header fields within the NOTIFY response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	m	m

Prerequisite A.5/11 - - NOTIFY response

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

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

A.2.1.4.9 OPTIONS method

Prerequisite A.5/12 - - OPTIONS request

Table A.77: Supported header fields within the OPTIONS request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	m	m	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c21	c21	[56B] 9.2	c26	c26
2	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c24	c24	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7	c2	c2	[26] 20.7	c2	c2
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
8	Contact	[26] 20.10	o	o	[26] 20.10	o	o
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
15A	Feature-Caps	[190]	c42	c42	[190]	c41	c41
16	From	[26] 20.20	m	m	[26] 20.20	m	m
16A	Geolocation	[89] 4.1	c27	c27	[89] 4.1	c27	c27
16B	Geolocation-Routing	[89] 4.2	c27	c27	[89] 4.2	c27	c27
16C	History-Info	[66] 4.1	c25	c25	[66] 4.1	c25	c25
16D	Max-Breadth	[117] 5.8	n/a	c31	[117] 5.8	c32	c32
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c39
18	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
19	Organization	[26] 20.25	o	o	[26] 20.25	o	o
19A	P-Access-Network-Info	[52] 4.4	c11	c12	[52] 4.4	c11	c13
19B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
19C	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c30	c30
19D	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c9	c9
19E	P-Charging-Function-Addresses	[52] 4.5	c16	c17	[52] 4.5	c16	c17
19F	P-Charging-Vector	[52] 4.6	c14	c15	[52] 4.6	c14	c15
19G	P-Debug-ID	[140]	o	c35	[140]	o	c36
19H	P-Preferred-Identity	[34] 9.2	c6	c4	[34] 9.2	n/a	n/a
19I	P-Preferred-Service	[121] 4.2	c29	c28	[121] 4.2	n/a	n/a
19J	P-Private-Network-Indication	[134]	c34	c34	[134]	c34	c34
19K	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
19L	P-Served-User	[133] 6	c38	c38	[133] 6	c38	c38
19M	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
19N	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c10	n/a
19O	Privacy	[33] 4.2	c8	c8	[33] 4.2	c8	c8
20	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
21	Proxy-Require	[26] 20.29	o	o (note 1)	[26] 20.29	n/a	n/a
21A	Reason	[34A] 2	c20	c20	[34A] 2	c20	c20
22	Record-Route	[26] 20.30	n/a	c39	[26] 20.30	n/a	c39
22A	Recv-Info	[25] 5.2.3	c37	c37	[25] 5.2.3	c37	c37
22B	Referred-By	[59] 3	c22	c22	[59] 3	c23	c23
22C	Reject-Contact	[56B] 9.2	c21	c21	[56B] 9.2	c26	c26
22D	Request-Disposition	[56B] 9.1	c21	c21	[56B] 9.1	c26	c26
23	Require	[26] 20.32	m	m	[26] 20.32	m	m
23A	Resource-Priority	[116] 3.1	c33	c33	[116] 3.1	c33	c33
24	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
24A	Security-Client	[48] 2.3.1	c18	c18	[48] 2.3.1	n/a	n/a
24B	Security-Verify	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
24C	Session-ID	[162]	o	c40	[162]	o	c40

25	Supported	[26] 20.37	c6	c6	[26] 20.37	m	m
26	Timestamp	[26] 20.38	c7	c7	[26] 20.38	m	m
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c2: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c3: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c4: IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c5: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c8: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9: IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c10: IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c11: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c12: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c13: IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF.
c14: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c15: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c16: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c17: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18: IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 3).
c19: IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c20: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c21: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c22: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c23: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c24: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c25: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c26: IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c27: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c28: IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.
c29: IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.
c30: IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.
c31: IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13) THEN m ELSE IF A.3/1 AND NOT A.3C/1 - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c32: IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c33: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c34: IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).
c35: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c36: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c37: IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c38: IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.
c39: IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c40: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c41: IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c42: IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.

NOTE 1: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.
NOTE 2: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 3: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/12 - - OPTIONS request

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

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

Table A.79: Void

Prerequisite A.5/13 - - OPTIONS response

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

Table A.79A: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/13 - - OPTIONS response for all remaining status-codes

Table A.80: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c14	c14	[89] 4.3	c14	c14
9B	History-Info	[66] 4.1	c13	c13	[66] 4.1	c13	c13
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
11B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
11C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
11D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
11E	P-Debug-ID	[140]	o	c15	[140]	o	c16
11F	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
11G	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
11H	Recv-Info	[25] 5.2.3	c17	c17	[25] 5.2.3	c17	c17
11I	Require	[26] 20.32	m	m	[26] 20.32	m	m
11J	Server	[26] 20.35	o	o	[26] 20.35	o	o
11K	Session-ID	[162]	o	c18	[162]	o	c18
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller, or EATF.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/6 OR A.6/18 THEN m ELSE o - - 200 (OK), 405 (Method Not Allowed).
c13: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c14: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c15: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c16: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c17: IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c18: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.

NOTE: RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.81: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	m	m	[26] 20.1	m	m
1A	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	m	m	[26] 20.3	m	m
1C	Accept-Resource-Priority	[116] 3.2	c14	c14	[116] 3.2	c14	c14
2	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
3	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
5	Contact	[26] 20.10	o	o	[26] 20.10	o	o
6	Feature-Caps	[190]	c16	c16	[190]	c15	c15
7	Recv-Info	[25] 5.2.3	c6	c6	[25] 5.2.3	c6	c6
12	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c4:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c6:	IF A.4/13 THEN m ELSE n/a - - SIP INFO method and package framework.						
c14:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						
c15:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						
c16:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.						

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.81A: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.82: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
NOTE:	RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/13 - - OPTIONS response

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

Table A.83: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
10	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response.

Table A.84: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.85: Void

Prerequisite A.5/13 - - OPTIONS response

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

Table A.86: Supported header field s within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/13 - - OPTIONS response

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

Table A.87: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.87A: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						

Prerequisite A.5/13 - - OPTIONS response

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

Table A.88: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
7	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/13 - - OPTIONS response

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

Table A.88A: Supported header fields within the OPTIONS response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.89: Void

Prerequisite A.5/13 - - OPTIONS response

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

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

A.2.1.4.10 PRACK method

Prerequisite A.5/14 - - PRACK request

Table A.91: Supported header fields within the PRACK request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c15	c15	[56B] 9.2	c18	c18
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
9	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	From	[26] 20.20	m	m	[26] 20.20	m	m
14A	Max-Breadth	[117] 5.8	n/a	c21	[117] 5.8	c22	c22
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c34
16	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
16A	P-Access-Network-Info	[52] 4.4	c9	c10	[52] 4.4	c9	c11
16B	P-Charging-Function-Addresses	[52] 4.5	c13	c14	[52] 4.5	c13	c14
16C	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c12	n/a
16D	P-Debug-ID	[140]	o	c19	[140]	o	c20
16E	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
17	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
18	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
19	RAck	[27] 7.2	m	m	[27] 7.2	m	m
19A	Reason	[34A] 2	c7	c7	[34A] 2	c7	c7
20	Record-Route	[26] 20.30	n/a	c34	[26] 20.30	n/a	c34
20A	Recv-Info	[25] 5.2.3	c35	c35	[25] 5.2.3	c35	c35
20B	Referred-By	[59] 3	c16	c16	[59] 3	c17	c17
20C	Reject-Contact	[56B] 9.2	c15	c15	[56B] 9.2	c18	c18
20D	Request-Disposition	[56B] 9.1	c15	c15	[56B] 9.1	c18	c18
21	Require	[26] 20.32	m	m	[26] 20.32	m	m
21A	Resource-Priority	[116] 3.1	c33	c33	[116] 3.1	c33	c33
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	c34
22A	Session-ID	[162]	o	c36	[162]	o	c36
23	Supported	[26] 20.37	o	o	[26] 20.37	m	m
24	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
25	To	[26] 20.39	m	m	[26] 20.39	m	m
26	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
27	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c2:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c7:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c8:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c10:	IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), AS or MSC server enhanced for ICS.
c11:	IF A.4/34 AND (A.3/2A OR A.3A/81 OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), MSC server enhanced for ICS, AS acting as terminating UA, AS acting as third-party call controller or EATF.
c12:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c13:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c14:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c15:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c16:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c17:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c18:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c19:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c20:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c21:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c22:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c33:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c34:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c35:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c36:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.

Prerequisite A.5/14 - - PRACK request

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

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

Table A.93: Void

Prerequisite A.5/15 - - PRACK response

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

Table A.93A: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/15 - - PRACK response for all remaining status-codes

Table A.94: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c9	c9	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c3	c4	[52] 4.4	c3	c5
10B	P-Charging-Function-Addresses	[52] 4.5	c7	c8	[52] 4.5	c7	c8
10C	P-Charging-Vector	[52] 4.6	c6	n/a	[52] 4.6	c6	n/a
10D	P-Debug-ID	[140]	o	c11	[140]	o	c12
10E	P-Early-Media	[109] 8	c10	c10	[109] 8	c10	c10
10F	Privacy	[33] 4.2	c2	n/a	[33] 4.2	c2	n/a
10G	Recv-Info	[25] 5.2.3	c13	c13	[25] 5.2.3	c13	c13
10H	Require	[26] 20.32	m	m	[26] 20.32	m	m
10I	Server	[26] 20.35	o	o	[26] 20.35	o	o
10J	Session-ID	[162]	o	c14	[162]	o	c14
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c3:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c4:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c5:	IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF.						
c6:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c7:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c8:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c9:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)						
c10:	IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.						
c11:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c12:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c13:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.						
c14:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.95: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept-Resource-Priority	[116] 3.2	c14	c14	[116] 3.2	c14	c14
0B	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
0C	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2

0D	P-Early-Media	[109] 8	c5	c5	[109] 8	c5	c5
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c4:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c5:	IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.						
c14:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.95A: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.96: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
NOTE:	RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.						

Prerequisite A.5/15 - - PRACK response

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

Table A.97: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response.

Table A.98: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.99: Void

Prerequisite A.5/15 - - PRACK response

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

Table A.100: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/15 - - PRACK response

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

Table A.101: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.101A: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						

Prerequisite A.5/15 - - PRACK response

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

Table A.102: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/15 - - PRACK response

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

Table A.102A: Supported header fields within the PRACK response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.103: Void

Prerequisite A.5/15 - - PRACK response

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

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

A.2.1.4.10A PUBLISH method

Prerequisite A.5/15A – PUBLISH request

Table A.104A: Supported header fields within the PUBLISH request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Contact	[56B] 9.2	c22	c22	[56B] 9.2	c28	c28
2	Allow	[26] 20.5	o	o	[26] 20.5	m	m
3	Allow-Events	[26] 7.2.2	c1	c1	[26] 7.2.2	c2	c2
4	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
5	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
6A	Contact	[26] 20.10	o	o	[26] 20.10	o	o
7	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
9	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	Event	[70] 4, 6	m	m	[70] 4, 6	m	m
15	Expires	[26] 20.19, [70] 4, 5, 6	o	o	[26] 20.19, [70] 4, 5, 6	m	m
15A	Feature-Caps	[190]	c41	c41	[190]	c40	c40
16	From	[26] 20.20	m	m	[26] 20.20	m	m
16A	Geolocation	[89] 4.1	c38	c38	[89] 4.1	c38	c38
16B	Geolocation-Routing	[89] 4.2	c38	c38	[89] 4.2	c38	c38
16C	History-Info	[66] 4.1	c27	c27	[66] 4.1	c27	c27
17	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
17A	Max-Breadth	[117] 5.8	n/a	c23	[117] 5.8	c24	c24
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c37
19	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
20	Organization	[26] 20.25	o	o	[26] 20.25	o	o
21	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
22	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c11	c11
22A	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c31	c31
23	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
24	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
25	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
25A	P-Debug-ID	[140]	o	c34	[140]	o	c35
26	P-Preferred-Identity	[34] 9.2	c11	c7	[34] 9.2	n/a	n/a
26A	P-Preferred-Service	[121] 4.2	c31	c30	[121] 4.2	n/a	n/a
26B	P-Private-Network-Indication	[134]	c33	c33	[134]	c33	c33
26C	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
26D	P-Served-User	[133] 6	c36	c36	[133] 6	c36	c36
26E	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
27	P-Visited-Network-ID	[52] 4.3	x (note 3)	x	[52] 4.3	c14	n/a
28	Priority	[26] 20.26	o	o	[26] 20.26	o	o
29	Privacy	[33] 4.2	c12	c12	[33] 4.2	c12	c12
30	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
31	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
32	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
33	Reject-Contact	[56B] 9.2	c22	c22	[56B] 9.2	c28	c28
33A	Referred-By	[59] 3	c25	c25	[59] 3	c26	c26
34	Request-Disposition	[56B] 9.1	c22	c22	[56B] 9.1	c28	c28
35	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
36	Require	[26] 20.32	m	m	[26] 20.32	m	m
36A	Resource-Priority	[116] 3.1	c29	c29	[116] 3.1	c29	c29
37	Route	[26] 20.34	m	m	[26] 20.34	n/a	c37

38	Security-Client	[48] 2.3.1	c9	c9	[48] 2.3.1	n/a	n/a
39	Security-Verify	[48] 2.3.1	c10	c10	[48] 2.3.1	n/a	n/a
39A	Session-ID	[162]	o	c39	[162]	o	c39
40	SIP-If-Match	[70] 11.3.2	o	o	[70] 11.3.2	m	m
41	Subject	[26] 20.36	o	o	[26] 20.36	o	o
42	Supported	[26] 20.37, [26] 7.1	o	o	[26] 20.37, [26] 7.1	m	m
43	Timestamp	[26] 20.38	c6	c6	[26] 20.38	m	m
44	To	[26] 20.39	m	m	[26] 20.39	m	m
45	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
46	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c2: IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c7: IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 1).
c10: IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c11: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c12: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c13: IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c14: IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c15: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c16: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c17: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c18: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c19: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c20: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c22: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c23: IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c24: IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c25: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c26: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c27: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c28: IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c29: IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.
c30: IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.
c31: IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.
c32: IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.
c33: IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).
c34: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c35: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c36: IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.
c37: IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c38: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c39: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c40: IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c41: IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network

NOTE 1: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. NOTE 2: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.

Prerequisite A.5/15A - - PUBLISH request

Table A.104B: Supported message bodies within the PUBLISH request

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

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104BA: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/15B - - PUBLISH response for all remaining status-codes

Table A.104C: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 24.9	o	o	[26] 24.9	m	m
3	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
4	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
5	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
10	From	[26] 20.20	m	m	[26] 20.20	m	m
10A	Geolocation-Error	[89] 4.3	c16	c16	[89] 4.3	c16	c16
10B	History-Info	[66] 4.1	c13	c13	[66] 4.1	c13	c13
11	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
12	Organization	[26] 20.25	o	o	[26] 20.25	o	o
13	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
14	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
15	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
16	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
16A	P-Debug-ID	[140]	o	c14	[140]	o	c15
17	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
18	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
19	Require	[26] 20.32	m	m	[26] 20.32	m	m
20	Server	[26] 20.35	o	o	[26] 20.35	o	o
20A	Session-ID	[162]	o	c17	[162]	o	c17
21	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
22	To	[26] 20.39	m	m	[26] 20.39	m	m
23	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
24	Via	[26] 20.42	m	m	[26] 20.42	m	m
25	Warning	[26] 20.43	o	o	[26] 20.43	o	o

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).
c13: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c14: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c15: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c16: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c17: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/7 - - Additional for 200 (OK) response

Table A.104D: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c3	c3	[116] 3.2	c3	c3
1A	Allow-Events	[28] 7.2.2	c4	c4	[28] 7.2.2	c5	c5
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	Expires	[26] 20.19, [70] 4, 5, 6	m	m	[26] 20.19, [70] 4, 5, 6	m	m
3A	Feature-Caps	[190]	c8	c8	[190]	c7	c7
4	SIP-Etag	[70] 11.3.1	m	m	[70] 11.3.1	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

c1: IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.
c2: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c3: IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.
c4: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c5: IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c7: IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c8: IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.104DA: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.104E: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Contact	[26] 20.10	o	o	[26] 20.10	m	m

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11OR A.6/12 – Additional for 401 (Unauthorized) response

Table A.104F: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.104G: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.104H: Void

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104I: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
5	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104J: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.104JA: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104K: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104L: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104M: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Min-Expires	[26] 20.23, [70] 5, 6	m	m	[26] 20.23, [70] 5, 6	m	m

Table A.104N: Void

Prerequisite A.5/15B - - PUBLISH response

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

Table A.104O: Supported header fields within the PUBLISH response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	m	m

Prerequisite A.5/15B - - PUBLISH response

Table A.104P: Supported message bodies within the PUBLISH response

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

A.2.1.4.11 REFER method

Prerequisite A.5/16 - - REFER request

Table A.105: Supported header fields within the REFER request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept	[26] 20.1	o	o	[26] 20.1	m	m
0B	Accept-Contact	[56B] 9.2	c22	c22	[56B] 9.2	c25	c25
0C	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
1A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
2	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2
3	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Contact	[26] 20.10	m	m	[26] 20.10	m	m
5A	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
5B	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
5C	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
10	Expires	[26] 20.19	o	o	[26] 20.19	o	o
10A	Feature-Caps	[190]	c46	c46	[190]	c45	c45
11	From	[26] 20.20	m	m	[26] 20.20	m	m
11A	Geolocation	[89] 4.1	c26	c26	[89] 4.1	c26	c26
11B	Geolocation-Routing	[89] 4.2	c26	c26	[89] 4.2	c26	c26
11C	History-Info	[66] 4.1	c24	c24	[66] 4.1	c24	c24
11D	Max-Breadth	[117] 5.8	n/a	c30	[117] 5.8	c31	c31
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c39
13	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
14	Organization	[26] 20.25	o	o	[26] 20.25	o	o
14A	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
14B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c8	c8
14C	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c29	c29
14D	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c10	c10
14E	P-Charging-Function-Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
14F	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
14G	P-Debug-ID	[140]	o	c37	[140]	o	c38
14H	P-Preferred-Identity	[34] 9.2	c8	c7	[34] 9.2	n/a	n/a
14I	P-Preferred-Service	[121] 4.2	c28	c27	[121] 4.2	n/a	n/a
14J	P-Private-Network-Indication	[134]	c36	c36	[134]	c36	c36
14K	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
14L	P-Served-User	[133] 6	c41	c41	[133] 6	c41	c41
14M	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
14N	P-Visited-Network-ID	[52] 4.3	x (note 1)	x	[52] 4.3	c11	n/a
14O	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
15	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
16	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
16A	Reason	[34A] 2	c21	c21	[34A] 2	c21	c21
17	Record-Route	[26] 20.30	n/a	c39	[26] 20.30	m	m
17A	Refer-Sub	[173] 4	c40	c40	[173] 4	c40	c40
18	Refer-To	[36] 3	m	m	[36] 3	m	m
18A	Referred-By	[59] 3	c23	c23	[59] 3	c23	c23
18B	Reject-Contact	[56B] 9.2	c22	c22	[56B] 9.2	c25	c25
18C	Request-Disposition	[56B] 9.1	c22	c22	[56B] 9.1	c25	c25
19	Require	[26] 20.32	m	m	[26] 20.32	m	m
19A	Resource-Priority	[116] 3.1	c33	c33	[116] 3.1	c33	c33
20	Route	[26] 20.34	m	m	[26] 20.34	n/a	c39
20A	Security-Client	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
20B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	n/a	n/a

20C	Session-ID	[162]	o	c42	[162]	o	c42
21	Supported	[26] 20.37, [26] 7.1	o	o	[26] 20.37, [26] 7.1	m	m
21A	Target-Dialog	[184] 7	c43	c43	[184] 7	c44	c44
22	Timestamp	[26] 20.38	c6	c6	[26] 20.38	m	m
23	To	[26] 20.39	m	m	[26] 20.39	m	m
23A	Trigger-Consent	[125] 5.11.2	c34	c34	[125] 5.11.2	c35	c35
24	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
25	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c2:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c7:	IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c11:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c13:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c14:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c19:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 2).
c20:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c21:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c22:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c23:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By Mechanism.
c24:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c25:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c26:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c27:	IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.
c28:	IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.
c29:	IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.
c30:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c31:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c33:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c34:	IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.
c35:	IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.
c36:	IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).
c37:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c38:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c39:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c40:	IF A.4/95 THEN m ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.
c41:	IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.
c42:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c43:	IF A.4/99 THEN o ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.
c44:	IF A.4/99 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.
c45:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c46:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.
NOTE 1:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 2:	Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/16 - - REFER request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	application/vnd.3gpp.mid-call+xml	[8M] D	n/a	o	[8M] D	n/a	o

Table A.107: Void

Prerequisite A.5/17 - - REFER response

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

Table A.107A: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/17 - - REFER response for all remaining status-codes

Table A.108: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Contact	[26] 20.10	c13	c13	[26] 20.10	m	m
1B	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
2	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
3	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
4	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
5	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
6	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
7	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
8	From	[26] 20.20	m	m	[26] 20.20	m	m
8A	Geolocation-Error	[89] 4.3	c15	c15	[89] 4.3	c15	c15
8B	History-Info	[66] 4.1	c14	c14	[66] 4.1	c14	c14
9	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10	Organization	[26] 20.25	o	o	[26] 20.25	o	o
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
10D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
10E	P-Debug-ID	[140]	o	c16	[140]	o	c17
10F	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10G	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
10H	Require	[26] 20.32	m	m	[26] 20.32	m	m
10I	Server	[26] 20.35	o	o	[26] 20.35	o	o
10J	Session-ID	[162]	o	c18	[162]	o	c18
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c4:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c5:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c6:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c7:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.						
c8:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c10:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c12:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)						
c13:	IF A.6/102 THEN m ELSE o - - 2xx response.						
c14:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c15:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c16:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c17:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c18:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.						

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.109: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept-Resource-Priority	[116] 3.2	c12	c12	[116] 3.2	c12	c12
1	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	Feature-Caps	[190]	c15	c15	[190]	c14	c14
5	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
6	Refer-Sub	[173] 4	c13	c13	[173] 4	c13	c13
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c4:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c12:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						
c13:	IF A.4/95 THEN m ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.						
c14:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						
c15:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.						

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.109A: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Table A.110: Void

Prerequisite A.5/17 - - REFER response

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

Table A.111: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.112: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.113: Void

Prerequisite A.5/17 - - REFER response

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

Table A.114: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/17 - - REFER response

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

Table A.115: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.115A: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						

Prerequisite A.5/17 - - REFER response

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

Table A.116: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/17 - - REFER response

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

Table A.116A: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Table A.117: Void

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

Table A.117A: Supported header fields within the REFER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Permission-Missing	[125] 5.9.3	m	m	[125] 5.9.3	m	m

Prerequisite A.5/17 - - REFER response

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

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

A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

Table A.119: Supported header fields within the REGISTER request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c27	c27	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7, [49]	c2	c29	[26] 20.7, [49]	m	c22
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
8	Contact	[26] 20.10	o	m	[26] 20.10	m	m
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	Expires	[26] 20.19	o	o	[26] 20.19	m	m
16A	Feature-Caps	[190]	c40	c40	[190]	c39	c39
17	From	[26] 20.20	m	m	[26] 20.20	m	m
17A	Geolocation	[89] 4.1	c31	c31	[89] 4.1	c31	c31
17B	Geolocation-Routing	[89] 4.2	c31	c31	[89] 4.2	c31	c31
17C	History-Info	[66] 4.1	c28	c28	[66] 4.1	c28	c28
17D	Max-Breadth	[117] 5.8	n/a	c35	[117] 5.8	c36	c36
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
20	Organization	[26] 20.25	o	o	[26] 20.25	o	o
20A	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
20B	P-Charging-Function-Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
20C	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
20D	P-Debug-ID	[140]	o	c33	[140]	o	c34
20E	P-User-Database	[82] 4	n/a	n/a	[82] 4	c30	c30
20F	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c10	c11
20G	Path	[35] 4	c4	c5	[35] 4	m	c6
20H	Privacy	[33] 4.2	c9	n/a	[33] 4.2	c9	n/a
21	Proxy-Authorization	[26] 20.28	c8	c8	[26] 20.28	n/a	n/a
22	Proxy-Require	[26] 20.29	o	o (note 1)	[26] 20.29	n/a	n/a
22A	Reason	[34A] 2	c23	c23	[34A] 2	c23	c23
22B	Recv-Info	[25] 5.2.3	c37	c37	[25] 5.2.3	c37	c37
22C	Referred-By	[59] 3	c25	c25	[59] 3	c26	c26
22D	Request-Disposition	[56B] 9.1	c24	c24	[56B] 9.1	n/a	n/a
23	Require	[26] 20.32	m	m	[26] 20.32	m	m
23A	Resource-Priority	[116] 3.1	c32	c32	[116] 3.1	c32	c32
24	Route	[26] 20.34	o	n/a	[26] 20.34	n/a	n/a
24A	Security-Client	[48] 2.3.1	c19	c20	[48] 2.3.1	n/a	n/a
24B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	c21	n/a
24C	Session-ID	[162]	o	c38	[162]	o	c38
25	Supported	[26] 20.37	o	c29	[26] 20.37	m	m
26	Timestamp	[26] 20.38	c7	c7	[26] 20.38	c7	c7
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c2:	IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.
c3:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c4:	IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c5:	IF A.4/24 THEN x ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c6:	IF A.3/4 THEN m ELSE n/a. - - S-CSCF.
c7:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c8:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c11:	IF A.4/33 THEN m ELSE n/a - - the P-Visited-Network-ID extension.
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c13:	IF A.4/34 AND (A.3/1 OR A.3/4) THEN o ELSE n/a - - the P-Access-Network-Info header extension and UE or S-CSCF.
c14:	IF A.4/34 AND (A.3/4 OR A.3/7A) THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF or AS acting as terminating UA.
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).
c19:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 3).
c20:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c21:	IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.
c22:	IF A.3/4 THEN m ELSE n/a - - S-CSCF.
c23:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c24:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c25:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c26:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c27:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c28:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c29:	IF (A.3/1 OR A.3A/81) THEN m ELSE o - - UE, MSC Server enhanced for ICS.
c30:	IF A.4/48 THEN m ELSE n/a - - the P-User-Database private header extension.
c31:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c32:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.
c33:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c34:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c35:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE n/a - - IF A.4/71 AND (A.3/9B OR A.3/9C) THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).
c36:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c37:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c38:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c39:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c40:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.
NOTE 1:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.
NOTE 2:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 3:	Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented.

Prerequisite A.5/18 - - REGISTER request

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	message/sip	[26] 27.5	n/a	c1	[26] 27.5	n/a	c2
2	3GPP IM CN subsystem XML body	subclause 7.6	n/a	c1	subclause 7.6	n/a	c2
c1: IF A.3/4 THEN o ELSE n/a - - S-CSCF. c2: IF A.3/7 THEN o ELSE n/a - - AS.							

Table A.121: Void

Prerequisite A.5/19 - - REGISTER response

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

Table A.121A: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. c2: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol. c3: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.							

Prerequisite A.5/19 - - REGISTER response for all remaining status-codes

Table A.122: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c8	c8	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c10	c10	[89] 4.3	c10	c10
9B	History-Info	[66] 4.1	c9	c9	[66] 4.1	c9	c9
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c3	n/a	[52] 4.4	c3	n/a
11B	P-Charging-Function-Addresses	[52] 4.5	c6	c7	[52] 4.5	c6	c7
11C	P-Charging-Vector	[52] 4.6	c4	c5	[52] 4.6	c4	c5
11D	P-Debug-ID	[140]	o	c11	[140]	o	c12
11E	Privacy	[33] 4.2	c2	n/a	[33] 4.2	c2	n/a
11F	Require	[26] 20.32	m	m	[26] 20.32	m	m
11G	Server	[26] 20.35	o	o	[26] 20.35	o	o
11H	Session-ID	[162]	o	c13	[162]	o	c13
12	Timestamp	[26] 20.38	c2	c2	[26] 20.38	m	m
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c3: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c4: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c5: IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).
c6: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c7: IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).
c8: IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).
c9: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c10: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c11: IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c12: IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c13: IF A.4/91 THEN m ELSE n/a - - the Session-ID header.

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.123: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	o	o
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
1C	Accept-Resource-Priority	[116] 3.2	c14	c14	[116] 3.2	c14	c14
2	Allow-Events	[28] 7.2.2	c12	c12	[28] 7.2.2	c13	c13
3	Authentication-Info	[26] 20.6	c6	c6	[26] 20.6	c7	c7
5	Contact	[26] 20.10	o	o	[26] 20.10	m	m
5A	Feature-Caps	[190]	c18	c18	[190]	c17	c17
5B	Flow-Timer	[92] 11	c15	c15	[92] 11	c15	c15
5C	P-Associated-URI	[52] 4.1	c8	c9	[52] 4.1	c10	c11
6	Path	[35] 4	c3	c3	[35] 4	c4	c4
7	Security-Server	Subclause 7.2A.7	n/a	x	Subclause 7.2A.7	n/a	c16
8	Service-Route	[38] 5	c5	c5	[38] 5	c5	c5
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m

c1: IF (A.3/4 AND A.4/2) THEN m ELSE n/a. - - S-CSCF acting as registrar.
c2: IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c3: IF A.4/24 THEN m ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c4: IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c5: IF A.4/28 THEN m ELSE n/a - - session initiation protocol extension header field for service route discovery during registration.
c6: IF A.4/8 THEN o ELSE n/a - - authentication between UA and registrar.
c7: IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.
c8: IF A.4/2 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and registrar.
c9: IF A.3/1 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and S-CSCF.
c10: IF A.4/31 THEN o ELSE n/a - - P-Assocated-URI header extension.
c11: IF A.4/31 AND A.3/1 THEN m ELSE n/a - - P-Assocated-URI header extension and UE.
c12: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c13: IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c14: IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.
c15: IF A.4/57 THEN m ELSE n/a - - managing client initiated connections in SIP.
c16: IF A.4/37A THEN m ELSE n/a - - mediasec header field parameter for marking security mechanisms related to media.
c17: IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c18: IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.123A: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.124: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m

Prerequisite A.5/19 - - REGISTER response

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

Table A.125: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	x	[26] 20.27	c1	x
6	Security-Server	[48] 2	x	x	[48] 2	n/a	c2
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/8 THEN m ELSE n/a - - support of authentication between UA and registrar.						
c2:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.126: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.127: Void

Prerequisite A.5/19 - - REGISTER response

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

Table A.128: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Proxy-Authenticate	[26] 20.27	c1	x	[26] 20.27	c1	x
9	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/8 THEN m ELSE n/a - - support of authentication between UA and registrar.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.129: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.129A: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.130: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/19 - - REGISTER response

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

Table A.130A: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	c2	c2	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						
c2:	IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.131: Supported header fields within the REGISTER response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m

Table A.132: Void

Prerequisite A.5/19 - - REGISTER response

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

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

A.2.1.4.13 SUBSCRIBE method

Prerequisite A.5/20 - - SUBSCRIBE request

Table A.134: Supported header fields within the SUBSCRIBE request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c22	c22	[56B] 9.2	c26	c26
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	o	o	[28] 7.2.2	m	m
5	Authorization	[26] 20.7	c3	c3	[26] 20.7	c3	c3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
6B	Contact	[26] 20.10	m	m	[26] 20.10	m	m
7	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
9	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
10	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
11	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
12	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
13	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
14	Event	[28] 7.2.1	m	m	[28] 7.2.1	m	m
15	Expires	[26] 20.19	o (note 1)	o (note 1)	[26] 20.19	m	m
15A	Feature-Caps	[190]	c46	c46	[190]	c45	c45
16	From	[26] 20.20	m	m	[26] 20.20	m	m
16A	Geolocation	[89] 4.1	c27	c27	[89] 4.1	c27	c27
16B	Geolocation-Routing	[89] 4.2	c27	c27	[89] 4.2	c27	c27
16C	History-Info	[66] 4.1	c25	c25	[66] 4.1	c25	c25
16D	Max-Breadth	[117] 5.8	n/a	c38	[117] 5.8	c39	c39
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c41
18	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
18A	Organization	[26] 20.25	o	o	[26] 20.25	o	o
18B	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
18C	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
18D	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c32	c32
18E	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c10	c10
18F	P-Charging-Function-Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
18G	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
18H	P-Debug-ID	[140]	o	c36	[140]	o	c37
18I	P-Preferred-Identity	[34] 9.2	c6	c7	[34] 9.2	n/a	n/a
18J	P-Preferred-Service	[121] 4.2	c31	c30	[121] 4.2	n/a	n/a
18K	P-Private-Network-Indication	[134]	c35	c35	[134]	c35	c35
18L	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
18M	P-Served-User	[133] 6	c40	c40	[133] 6	c40	c40
18N	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
18O	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c11	n/a
18P	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
19	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
20	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
20A	Reason	[34A] 2	c21	c21	[34A] 2	c21	c21
21	Record-Route	[26] 20.30	n/a	c41	[26] 20.30	m	m
21A	Referred-By	[59] 3	c23	c23	[59] 3	c24	c24
21B	Reject-Contact	[56B] 9.2	c22	c22	[56B] 9.2	c26	c26
21C	Request-Disposition	[56B] 9.1	c22	c22	[56B] 9.1	c26	c26
22	Require	[26] 20.32	m	m	[26] 20.32	m	m
22A	Resource-Priority	[116] 3.1	c29	c29	[116] 3.1	c29	c29
23	Route	[26] 20.34	m	m	[26] 20.34	n/a	c41
23A	Security-Client	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
23B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	n/a	n/a

23C	Session-ID	[162]	o	c42	[162]	o	c42
24	Supported	[26] 20.37	o	o	[26] 20.37	m	m
24A	Target-Dialog	[184] 7	c43	c43	[184] 7	c44	c44
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	To	[26] 20.39	m	m	[26] 20.39	m	m
26A	Trigger-Consent	[125] 5.11.2	c33	c33	[125] 5.11.2	c34	c34
27	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
28	Via	[26] 20.42	m	m	[26] 20.42	m	m

c3:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c6:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7:	IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c11:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c13:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c14:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c19:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 3).
c20:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c21:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c22:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c23:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c24:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c25:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c26:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c27:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c29:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.
c30:	IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.
c31:	IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.
c32:	IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.
c33:	IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.
c34:	IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.
c35:	IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).
c36:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c37:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c38:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c39:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c40:	IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.
c41:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c42:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c43:	IF A.4/99 THEN o ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.
c44:	IF A.4/99 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.
c45:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c46:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.
NOTE 1:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.
NOTE 2:	The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 3:	Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/20 - - SUBSCRIBE request

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

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

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.135A: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/21 - - SUBSCRIBE response for all remaining status-codes

Table A.136: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c14	c14	[89] 4.3	c14	c14
9B	History-Info	[66] 4.1	c13	c13	[66] 4.1	c13	c13
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	Organization	[26] 20.25	o	o	[26] 20.25	o	o
10B	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
10C	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10D	P-Charging-Function-Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
10E	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
10F	P-Debug-ID	[140]	o	c15	[140]	o	c16
10G	P-Preferred-Identity	[34] 9.2	c3	x	[34] 9.2	n/a	n/a
10H	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
10I	Require	[26] 20.32	m	m	[26] 20.32	m	m
10J	Server	[26] 20.35	o	o	[26] 20.35	o	o
10K	Session-ID	[162]	o	c17	[162]	o	c17
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.						
c4:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c5:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c6:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c7:	IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.						
c8:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c10:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c12:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).						
c13:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c14:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c15:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c16:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c17:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.						

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.137: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept-Resource-Priority	[116] 3.2	c5	c5	[116] 3.2	c5	c5
0B	Allow-Events	[28] 7.2.2			[28] 7.2.2		
1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
1A	Contact	[26] 20.10	m	m	[26] 20.10	m	m
2	Expires	[26] 20.19	m	m	[26] 20.19	m	m
2A	Feature-Caps	[190]	c8	c8	[190]	c7	c7
3	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c5:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						
c7:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						
c8:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.						

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.137A: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.138: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Contact	[26] 20.10	m (note)	m	[26] 20.10	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than MANDATORY for a 485 response.						

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.139: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.140: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.141: Void

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.142: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.143: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
6	Server	[26] 20.35	o	o	[26] 20.35	o	o
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.143A: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.						

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.144: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.144A: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.145: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m

Table A.146: Void

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

Table A.146A: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Permission-Missing	[125] 5.9.3	m	m	[125] 5.9.3	m	m

Prerequisite A.5/21 - - SUBSCRIBE response

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

Table A.147: Supported header fields within the SUBSCRIBE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	m	m

Table A.148: Void

Prerequisite A.5/21 - - SUBSCRIBE response

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

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

A.2.1.4.14 UPDATE method

Prerequisite A.5/22 - - UPDATE request

Table A.150: Supported header fields within the UPDATE request

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c20	c20	[56B] 9.2	c24	c24
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
4	Allow	[26] 20.5	o	o	[26] 20.5	m	m
5	Allow-Events	[28] 7.2.2	c2	c2	[28] 7.2.2	c3	c3
6	Authorization	[26] 20.7	c4	c4	[26] 20.7	c4	c4
7	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
8	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
9	Contact	[26] 20.10	m	m	[26] 20.10	m	m
10	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
11	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
12	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
13	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
14	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
15	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
16	Date	[26] 20.17	c5	c5	[26] 20.17	m	m
16A	Feature-Caps	[190]	c37	c37	[190]	c36	c36
17	From	[26] 20.20	m	m	[26] 20.20	m	m
17A	Geolocation	[89] 4.1	c25	c25	[89] 4.1	c25	c25
17B	Geolocation-Routing	[89] 4.2	c25	c25	[89] 4.2	c25	c25
17C	Max-Breadth	[117] 5.8	n/a	c29	[117] 5.8	c30	c30
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	c31
19	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
19A	Min-SE	[58] 5	c21	c21	[58] 5	c21	c21
20	Organization	[26] 20.25	o	o	[26] 20.25	o	o
20A	P-Access-Network-Info	[52] 4.4	c11	c12	[52] 4.4	c11	c13
20B	P-Charging-Function-Addresses	[52] 4.5	c16	c17	[52] 4.5	c16	c17
20C	P-Charging-Vector	[52] 4.6	c14	c15	[52] 4.6	c14	c15
20D	P-Debug-ID	[140]	o	c27	[140]	o	c28
20E	P-Early-Media	[109] 8	c26	c26	[109] 8	c26	c26
20F	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
21	Proxy-Authorization	[26] 20.28	c10	c10	[26] 20.28	n/a	n/a
22	Proxy-Require	[26] 20.29	o	n/a	[26] 20.29	n/a	n/a
22A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
23	Record-Route	[26] 20.30	n/a	c31	[26] 20.30	n/a	c31
23A	Recv-Info	[25] 5.2.3	c34	c34	[25] 5.2.3	c34	c34
23B	Referred-By	[59] 3	c22	c22	[59] 3	c23	c23
23C	Reject-Contact	[56B] 9.2	c20	c20	[56B] 9.2	c24	c24
23D	Request-Disposition	[56B] 9.1	c20	c20	[56B] 9.1	c24	c24
24	Require	[26] 20.32	m	m	[26] 20.32	m	m
24A	Resource-Priority	[116] 3.1	c33	c33	[116] 3.1	c33	c33
25	Route	[26] 20.34	m	m	[26] 20.34	n/a	c31
25A	Security-Client	[48] 2.3.1	c18	c18	[48] 2.3.1	n/a	n/a
25B	Security-Verify	[48] 2.3.1	c19	c19	[48] 2.3.1	n/a	n/a
25C	Session-Expires	[58] 4	c21	c21	[58] 4	c21	c21
25D	Session-ID	[162]	o	c35	[162]	o	c35
26	Supported	[26] 20.37	o	o	[26] 20.37	m	m
27	Timestamp	[26] 20.38	c9	c9	[26] 20.38	m	m
28	To	[26] 20.39	m	m	[26] 20.39	m	m
29	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
30	Via	[26] 20.42	m	m	[26] 20.42	m	m

c2:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c3:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.
c4:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c5:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c6:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c8:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c10:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c11:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c12:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c13:	IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF.
c14:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c15:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c16:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c17:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c18:	IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note).
c19:	IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.
c20:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c21:	IF A.4/42 THEN m ELSE n/a - - the SIP session timer.
c22:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c23:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c24:	IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c25:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c26:	IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.
c27:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c28:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.
c29:	IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.
c30:	IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.
c31:	IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.
c33:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.
c34:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.
c35:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.
c36:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.
c37:	IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.
NOTE:	Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/22 - - UPDATE request

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

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

Prerequisite A.5/23 - - UPDATE response

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

Table A.151A: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
5A	P-Debug-ID	[140]	o	c2	[140]	o	c3
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c3:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						

Prerequisite A.5/23 - - UPDATE response for all remaining status-codes

Table A.152: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c11	c11	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
1B	Contact	[26] 20.10	o	o	[26] 20.10	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation-Error	[89] 4.3	c13	c13	[89] 4.3	c13	c13
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
10A	Organization	[26] 20.25	o	o	[26] 20.25	o	o
10B	P-Access-Network-Info	[52] 4.4	c4	c5	[52] 4.4	c4	c6
10C	P-Charging-Function-Addresses	[52] 4.5	c9	c10	[52] 4.5	c9	c10
10D	P-Charging-Vector	[52] 4.6	c7	c8	[52] 4.6	c7	c8
10E	P-Debug-ID	[140]	o	c14	[140]	o	c15
10F	Privacy	[33] 4.2	c3	n/a	[33] 4.2	c3	n/a
10G	Recv-Info	[25] 5.2.3	c16	c16	[25] 5.2.3	c16	c16
10H	Require	[26] 20.31	m	m	[26] 20.31	m	m
10I	Server	[26] 20.35	o	o	[26] 20.35	o	o
10J	Session-ID	[162]	o	c17	[162]	o	c17
11	Timestamp	[26] 20.38	c12	c12	[26] 20.38	c2	c2
12	To	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c4:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c5:	IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.						
c6:	IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF.						
c7:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c8:	IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.						
c9:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c10:	IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c11:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)						
c12:	IF A.4/6 THEN o ELSE n/a - - timestamping of requests.						
c13:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
c14:	IF A.4/80 THEN o ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c15:	IF A.4/80 THEN m ELSE n/a - - the P-Debug-ID header field for the session initiation protocol.						
c16:	IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.						
c17:	IF A.4/91 THEN m ELSE n/a - - the Session-ID header.						
NOTE:	For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.						

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.153: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Accept	[26] 20.1	o	o	[26] 20.1	m	m
0B	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
0C	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
0D	Accept-Resource-Priority	[116] 3.2	c14	c14	[116] 3.2	c14	c14
1	Allow-Events	[28] 7.2.2	c4	c4	[28] 7.2.2	c5	c5
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	Contact	[26] 20.10	m	m	[26] 20.10	m	m
3A	Feature-Caps	[190]	c16	c16	[190]	c16	c16
3B	P-Early-Media	[109] 8	c6	c6	[109] 8	c6	c6
4	Session-Expires	[58]	c3	c3	[58]	c3	c3
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/42 THEN m ELSE n/a - - the SIP session timer						
c4:	IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.						
c5:	IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.						
c6:	IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.						
c14:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						
c16:	IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.						

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.153A: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx, 485 (Ambiguous) response

Table A.154: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Contact	[26] 20.10	o	o	[26] 20.10	o	o

Prerequisite A.5/23 - - UPDATE response

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

Table A.154A: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.155: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.156: Void

Prerequisite A.5/23 - - UPDATE response

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

Table A.157: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
8	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/23 - - UPDATE response

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

Table A.158: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

Table A.158A: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept-Resource-Priority	[116] 3.2	c1	c1	[116] 3.2	c1	c1
c1:	IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.						

Prerequisite A.5/23 - - UPDATE response

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

Table A.159: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
7	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/23 - - UPDATE response

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

Table A.159A: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

Table A.159B: Supported header fields within the UPDATE response

Item	Header field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Min-SE	[58] 5	c1	c1	[58] 5	c1	c1
c1:	IF A.4/42 THEN m ELSE n/a - - the SIP session timer.						

Table A.160: Void

Prerequisite A.5/23 - - UPDATE response

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

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

Delete Section A.2.2 Proxy role

A.3 Profile definition for the Session Description Protocol as used in the present document

A.3.1 Introduction

Void.

A.3.2 User agent role

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

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

A.3.2.1 Major capabilities

Table A.317: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
	Extensions			
22	integration of resource management and SIP?	[30] [64]	o	c14
23	grouping of media lines?	[53]	c3	c3
24	mapping of media streams to resource reservation flows?	[54]	o	c1
25	SDP bandwidth modifiers for RTCP bandwidth?	[56]	o	o (NOTE 1)
26	TCP-based media transport in the session description protocol?	[83]	o	c2
27	interactive connectivity establishment?	[99]	o	c4
28	session description protocol format for binary floor control protocol streams?	[108]	o	o
29	extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF)?	[135]	o	c5
30	SDP capability negotiation?	[137]	o	c6
31	Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN)?	[155]	o	c7
32	miscellaneous capabilities negotiation in the Session Description Protocol (SDP)?	[156]	o	c7
33	transport independent bandwidth modifier for the Session Description Protocol?	[152]	o	c8
34	Secure Real-time Transport Protocol (SRTP)?	[169]	o	c15
35	MIKEY-TICKET?	[170]	o	c10
36	SDES?	[168]	o	c9
37	end-to-access-edge media security using SDES?	7.5.2	o	c16
38	SDP media capabilities negotiation?	[172]	o	c12
39	Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)?	[166]	o	c13
40	Message Session Relay Protocol?	[178]	o	c17
41	a SDP offer/answer mechanism to enable file transfer?	[185]	o	o
42	optimal media routeing	[11D]	n/a	c18
43	ECN for RTP over UDP	[188]	o	c19
44	T.38 FAX?	[202]	n/a	c20

c1:	IF A.3/1 THEN m ELSE n/a - - UE role.
c2:	IF A.3/9B AND A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 OR A.3/7 THEN o ELSE n/a - - IBCF (IMS-ALG), application gateway function (IMS-ALG), UE, MGCF, AS.
c3:	IF A.317/24 THEN m ELSE o - - mapping of media streams to resource reservation flows.
c4:	IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 THEN o ELSE n/a - - IBCF (IMS-ALG), application gateway function (IMS-ALG), UE, MGCF.
c5:	IF A.3A/50 OR A.3A/50A OR A.3/6 OR A.3/9B OR A.3A/89 THEN m ELSE o - - multimedia telephony service participant, multimedia telephony service application server, MGCF, IBCF (IMS-ALG), ATCF (UA).
c6:	IF A.3A/50 OR A.3A/50A OR A.3/6 OR A.3/9B OR A.3/13B OR A.3A/89 THEN m ELSE o - - multimedia telephony service participant, multimedia telephony service application server, MGCF, IBCF (IMS-ALG), application gateway function (IMS-ALG), ATCF (UA).
c7:	IF A.3A/82 OR A.3A/83 THEN m ELSE o - - ICS user agent, SCC application server.
c8:	IF A.317/25 AND (A.3/1 OR A.3/6 OR A.3A/89) THEN o ELSE n/a - - SDP bandwidth modifiers for RTCP bandwidth, UE, MGCF, ATCF (UA).
c9:	IF A.3D/301 OR A.3D/2A 20 THEN o m ELSE n/a - - end-to-access-edge media security using SDES, end-to-end media security using SDES.
c10:	IF A.3D/21 THEN m ELSE n/a - - end-to-end media security using KMS.
c12:	IF A.3A/82 OR A.3A/83 THEN m ELSE o - - ICS user agent, SCC application server.
c13:	IF IF A.3/7D OR A.3/8 THEN o else n/a - - AS performing 3rd party call control or MRFC.
c14:	IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.
c15:	IF A.3D/20 OR A.3D/21 OR A.3D/30 THEN m ELSE n/a - - end-to-end media security using SDES, end-to-end media security using KMS, end-to-access-edge media security using SDES.
c16:	If A.3D/30 THEN m ELSE n/a - - end-to-access-edge media security using SDES.
c17:	IF A.3A/33B OR A.3A/34 THEN m ELSE IF A.3A/8 OR A.3A/9 THEN o ELSE n/a - - session-mode messaging participant, session-mode messaging intermediate node, IBCF, MRFC.
c18:	IF A.3/2A OR A.3/6 OR A.3/7 OR A.3/9B OR A.3A/89 OR A.3/13B THEN o ELSE n/a - - P-CSCF (IMS-ALG), MGCF, AS, IBCF (IMS-ALG), ATCF (UA), application gateway function (IMS-ALG).
c19:	IF A.3/2A OR A.3/6 OR A.3/8 OR A.3/9B OR A.3A/81 OR A.3A/89 OR A.3/13B THEN o ELSE n/a - - P-CSCF (IMS-ALG), MGCF, MRFC, IBCF (IMS-ALG), MSC Server enhanced for ICS, ATCF (UA), application gateway function (IMS-ALG).
c20:	IF A.3/1 OR A.3/6 THEN o ELSE n/a - - UE, MGCF.
NOTE 1:	For "video" and "audio" media types that utilise RTP/RTCP, if the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then, it shall be specified. For other media types, it may be specified.

A.3.2.2 SDP types

Table A.318: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 5.1	m	m	[39] 5.1	m	m
2	o= (owner/creator and session identifier)	[39] 5.2	m	m	[39] 5.2	m	m
3	s= (session name)	[39] 5.3	m	m	[39] 5.3	m	m
4	i= (session information)	[39] 5.4	o	c2	[39] 5.4	m	c3
5	u= (URI of description)	[39] 5.5	o	c4	[39] 5.5	o	n/a
6	e= (email address)	[39] 5.6	o	c4	[39] 5.6	o	n/a
7	p= (phone number)	[39] 5.6	o	c4	[39] 5.6	o	n/a
8	c= (connection information)	[39] 5.7	c5	c5	[39] 5.7	m	m
9	b= (bandwidth information)	[39] 5.8	o	o (NOTE 1)	[39] 5.8	m	m
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 5.9	m	m	[39] 5.9	m	m
11	r= (zero or more repeat times)	[39] 5.10	o	c4	[39] 5.10	o	n/a
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 5.11	o	n/a	[39] 5.11	o	n/a
13	k= (encryption key)	[39] 5.12	x	x	[39] 5.12	n/a	n/a
14	a= (zero or more session attribute lines)	[39] 5.13	o	o	[39] 5.13	m	m
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 5.14	m	m	[39] 5.14	m	m
16	i= (media title)	[39] 5.4	o	c2	[39] 5.4	o	c3
17	c= (connection information)	[39] 5.7	c1	c1	[39] 5.7	m	m
18	b= (bandwidth information)	[39] 5.8	o	o (NOTE 1)	[39] 5.8	m	m
19	k= (encryption key)	[39] 5.12	x	x	[39] 5.12	n/a	n/a
20	a= (zero or more media attribute lines)	[39] 5.13	o	o	[39] 5.13	m	m

c1: IF (A.318/15 AND NOT A.318/8) THEN m ELSE IF (A.318/15 AND A.318/8) THEN o ELSE n/a - - “c=” contained in session level description and SDP contains media descriptions.
c2: IF A.3/6 THEN x ELSE o - - MGCF.
c3: IF A.3/6 THEN n/a ELSE m - - MGCF.
c4: IF A.3/6 THEN x ELSE n/a - - MGCF.
c5: IF A.318/17 THEN o ELSE m - - "c=" contained in all media description.

NOTE 1: The UE may use b=TIAS and b=AS as described in RFC 3890 [152]. For "video" and "audio" media types that utilise RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level different than the default RTCP bandwidth as specified in RFC 3556 [56], then the UE shall include the “b=” media descriptors with the bandwidth modifiers “RS” and “RR”. For other media types, the UE may include the “b=” media descriptor with the bandwidth modifiers “RS” and “RR”.

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

Table A.319: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6	c8	c8	[39] 6	c9	c9
2	keywords (a=keywds)	[39] 6	c8	c8	[39] 6	c9	c9
3	name and version of tool (a=tool)	[39] 6	c8	c8	[39] 6	c9	c9
4	packet time (a=ptime)	[39] 6	c10	c10	[39] 6	c11	c11
5	maximum packet time (a=maxptime)	[39] 6 (NOTE 1)	c10	c10	[39] 6 (NOTE 1)	c11	c11
6	receive-only mode (a=recvonly)	[39] 6	o	o	[39] 6	m	m
7	send and receive mode (a=sendrecv)	[39] 6	o	o	[39] 6	m	m
8	send-only mode (a=sendonly)	[39] 6	o	o	[39] 6	m	m
8A	Inactive mode (a=inactive)	[39] 6	o	o	[39] 6	m	m
9	whiteboard orientation (a=orient)	[39] 6	c10	c10	[39] 6	c11	c11
10	conference type (a=type)	[39] 6	c8	c8	[39] 6	c9	c9
11	character set (a=charset)	[39] 6	c8	c8	[39] 6	c9	c9
12	language tag (a=sdplang)	[39] 6	o	o	[39] 6	m	m
13	language tag (a=lang)	[39] 6	o	o	[39] 6	m	m
14	frame rate (a=framerate)	[39] 6	c10	c10	[39] 6	c11	c11
15	quality (a=quality)	[39] 6	c10	c10	[39] 6	c11	c11
16	format specific parameters (a=fmtp)	[39] 6	c10	c10	[39] 6	c11	c11
17	rtpmap attribute (a=rtpmap)	[39] 6	c10	c10	[39] 6	c11	c11
18	current-status attribute (a=curr)	[30] 5	c1	c1	[30] 5	c2	c2
19	desired-status attribute (a=des)	[30] 5	c1	c1	[30] 5	c2	c2
20	confirm-status attribute (a=conf)	[30] 5	c1	c1	[30] 5	c2	c2
21	media stream identification attribute (a=mid)	[53] 3	c3	c3	[53] 3	c4	c4
22	group attribute (a=group)	[53] 4	c5	c5	[53] 3	c6	c6
23	setup attribute (a=setup)	[83] 4	c7	c7	[83] 4	c7	c7
24	connection attribute (a=connection)	[83] 5	c7	c7	[83] 5	c7	c7
25	IP addresses (a=candidate)	[99]	c12	c12	[99]	c13	c13
26	floor control server determination (a=floorctrl)	[108] 4	c14	c14	[108] 4	c14	c14
27	conference id (a=confid)	[108] 5	c14	c14	[108] 5	c14	c14
28	user id (a=userid)	[108] 5	c14	c14	[108] 5	c14	c14
29	association between streams and floors (a=floorid)	[108] 6	c14	c14	[108] 6	c14	c14
30	RTCP feedback capability attribute (a=rtcp-fb)	[135] 4.2	c15	c15	[135] 4.2	c15	c15
31	extension of the rtcp-fb attribute (a=rtcp-fb)	[136] 7.1, [188] 6.2	c15	c15	[136] 7.1	c15	c15
32	supported capability negotiation extensions (a=csup)	[137] 3.3.1	c16	c16	[137] 3.3.1	c16	c16
33	required capability negotiation extensions (a=creq)	[137] 3.3.2	c16	c16	[137] 3.3.2	c16	c16
34	attribute capability (a=acap)	[137] 3.4.1	c16	c16	[137] 3.4.1	c16	c16
35	transport protocol capability (a=tcap)	[137] 3.4.2	c16	c16	[137] 3.4.2	c16	c16
36	potential configuration (a=pcfg)	[137] 3.5.1 [172]	c16	c16	[137] 3.5.1 [172]	c16	c16

		3.3.6			3.3.6		
37	actual configuration (a=acfg)	[137] 3.5.2	c16	c16	[137] 3.5.2	c16	c16
38	connection data capability (a=ccap)	[156] 5.1	c17	c17	[156] 5.1	c18	c18
39	maximum packet rate (a=maxprate)	[152] 6.3	c19	c19	[152] 6.3	c19	c19
40	crypto attribute (a=crypto)	[168]	c20	c20	[168]	c20	c20
41	key management attribute (a=key-mgmt)	[167]	c21	c21	[167]	c21	c21
42	3GPP_e2ae-security-indicator (a=3ge2ae)	7.5.2	c22	c22	7.5.2	c22	c22
43	media capability (a=mcap)	[172] 3.3.1	c23	c23	[172] 3.3.1	c23	c23
44	media format capability (a=mfcap)	[172] 3.3.2	c23	c23	[172] 3.3.2	c23	c23
45	media-specific capability (a=mscap)	[172] 3.3.3	c23	c23	[172] 3.3.3	c23	c23
46	latent configuration (a=lcfg)	[172] 3.3.5	c24	c24	[172] 3.3.5	c24	c24
47	session capability (a=sescap)	[172] 3.3.8	c24	c24	[172] 3.3.8	c24	c24
48	msrp path (a=path)	[178]	c25	c25	[178]	c25	c25
49	file selector (a=file-selector)	[185] 6	c27	c27	[185] 6	c28	c28
50	file transfer identifier (a= file-transfer-id)	[185] 6	c26	c26	[185] 6	c28	c28
51	file disposition (a=file-disposition)	[185] 6	c26	c26	[185] 6	c28	c28
52	file date (a=file-date)	[185] 6	c26	c26	[185] 6	c28	c28
53	file icon (a=file-icon	[185] 6	c26	c26	[185] 6	c28	c28
54	file range (a=file-range)	[185] 6	c26	c26	[185] 6	c28	c28
55	optimal media routeing visited realm (a=visited-realm)	7.5.3	c29	c29	7.5.3	c29	c29
56	optimal media routeing secondary realm (a=secondary-realm)	7.5.3	c29	c29	7.5.3	c29	c29
57	optimal media routeing media level checksum (a=omr-m-cksum)	7.5.3	c29	c29	7.5.3	c29	c29
58	optimal media routeing session level checksum (a=omr-s-cksum)	7.5.3	c29	c29	7.5.3	c29	c29
59	optimal media routeing codecs (a=omr-codecs)	7.5.3	c29	c29	7.5.3	c29	c29
60	optimal media routeing media attributes (a=omr-m-att)	7.5.3	c29	c29	7.5.3	c29	c29
61	optimal media routeing session attributes (a=omr-s-att)	7.5.3	c29	c29	7.5.3	c29	c29
62	optimal media routeing media bandwidth (a=omr-m-bw)	7.5.3	c29	c29	7.5.3	c29	c29
63	optimal media routeing session bandwidth (a=omr-s-bw)	7.5.3	c29	c29	7.5.3	c29	c29
64	ecn-attribute (a=ecn-capable-rtp)	[188]	c30	c30	[188]	c30	c30
65	T38 FAX Protocol version (a=T38FaxVersion)	[202]	n/a	c31	[202]	n/a	c31
66	T38 FAX Maximum Bit Rate (a=T38MaxBitRate)	[202]	n/a	c31	[202]	n/a	c31
67	T38 FAX Rate Management (a=T38FaxRateManagement)	[202]	n/a	c31	[202]	n/a	c31
68	T38 FAX Maximum Buffer Size (a=T38FaxMaxBuffer)	[202]	n/a	c31	[202]	n/a	c31
69	T38 FAX Maximum Datagram Size (a=T38FaxMaxDatagram)	[202]	n/a	c31	[202]	n/a	c31

70	T38 FAX maximum IFP frame size (a=T38FaxMaxIFP)	[202]	n/a	c32	[202]	n/a	c32
71	T38 FAX UDP Error Correction Scheme (a=T38FaxUdpEC)	[202]	n/a	c32	[202]	n/a	c32
72	T38 FAX UDP Error Correction Depth (a=T38FaxUdpECDepth)	[202]	n/a	c32	[202]	n/a	c32
73	T38 FAX UDP FEC Maximum Span (a=T38FaxUdpFECMaxSpan)	[202]	n/a	c32	[202]	n/a	c32
74	T38 FAX Modem Type (a=T38ModemType)	[202]	n/a	c32	[202]	n/a	c32
75	T38 FAX Vendor Info (a=T38VendorInfo)	[202]	n/a	c32	[202]	n/a	c32

c1: IF A.317/22 AND A.318/20 THEN o ELSE n/a - - integration of resource management and SIP, media level attribute name "a=".
c2: IF A.317/22 AND A.318/20 THEN m ELSE n/a - - integration of resource management and SIP, media level attribute name "a=".
c3: IF A.317/23 AND A.318/20 THEN o ELSE n/a - - grouping of media lines, media level attribute name "a=".
c4: IF A.317/23 AND A.318/20 THEN m ELSE n/a - - grouping of media lines, media level attribute name "a=".
c5: IF A.317/23 AND A.318/14 THEN o ELSE n/a - - grouping of media lines, session level attribute name "a=".
c6: IF A.317/23 AND A.318/14 THEN m ELSE n/a - - grouping of media lines, session level attribute name "a=".
c7: IF A.317/26 AND A.318/20 THEN m ELSE n/a - - TCP-based media transport in the session description protocol, media level attribute name "a=".
c8: IF A.318/14 THEN o ELSE x - - session level attribute name "a=".
c9: IF A.318/14 THEN m ELSE n/a - - session level attribute name "a=".
c10: IF A.318/20 THEN o ELSE x - - media level attribute name "a=".
c11: IF A.318/20 THEN m ELSE n/a - - media level attribute name "a=".
c12: IF A.317/27 AND A.318/20 THEN o ELSE n/a - - candidate IP addresses, media level attribute name "a=".
c13: IF A.317/27 AND A.318/20 THEN m ELSE n/a - - candidate IP addresses, media level attribute name "a=".
c14: IF A.317/28 AND A.318/20 THEN m ELSE n/a - - session description protocol format for binary floor control protocol streams, media level attribute name "a=".
c15: IF (A.317/29 AND A.318/20) THEN m ELSE n/a - - extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF), media level attribute name "a=".
c16: IF A.317/30 AND A.318/20 THEN m ELSE n/a - - SDP capability negotiation, media level attribute name "a=".
c17: IF A.317/32 AND A.318/20 THEN o ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".
c18: IF A.317/32 AND A.318/20 THEN m ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".
c19: IF A.317/33 AND (A.318/14 OR A.318/20) THEN o ELSE n/a - - bandwidth modifier packet rate parameter, media or session level attribute name "a=".
c20: IF A.317/34 AND A.317/36 AND 318/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using SDES, media level attribute name "a=".
c21: IF A.317/34 AND A.317/35 AND 318/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using KMS, media level attribute name "a=".
c22: IF A.317/37 THEN m ELSE n/a - - end to access edge media security.
c23: IF A.317/38 THEN m ELSE n/a - - SDP media capabilities negotiation.
c24: IF A.317/38 AND A.318/14 THEN m ELSE n/a - - SDP media capabilities negotiation, session level attribute name "a=".
c25: IF A.317/40 AND A.318/20 THEN m ELSE n/a - - message session relay protocol, media level attribute name "a=".
c26: IF A.317/41 AND A.318/20 THEN o ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".
c27: IF A.317/41 AND A.318/20 AND (A.3A/31 OR A.3A/33) THEN m ELSE IF A.317/41 AND A.318/20 AND NOT (A.3A/31 OR A.3A/33) THEN o ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=", messaging application server, messaging participant.
c28: IF A.317/41 AND A.318/20 THEN m ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".
c29: IF A.317/42 AND A.318/20 THEN o ELSE n/a - - optimal media routeing, media level attribute name "a=".
c30: IF A.317/43 THEN m ELSE n/a - - ECN for RTP over UDP, media level attribute name "a=".
c31: IF A.317/44 AND A.318/20 THEN m ELSE n/a - - T.38 FAX, media level attribute name "a=".
c32: IF A.317/44 AND A.318/20 THEN o ELSE n/a - - T.38 FAX, media level attribute name "a=".

NOTE 1: Further specification of the usage of this attribute is defined by specifications relating to individual codecs.

A.3.2.3 Void

Table A.320: Void

Table A.321: Void

Table A.322: Void

Table A.323: Void

Table A.324: Void

Table A.325: Void

Table A.326: Void

Table A.327: Void

A.3.2.4 Void

Table A.327A: Void

Delete Section A.3.3 Proxy role

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

~~*Prerequisite: A.2/2 – proxy role*~~

A.4 Profile definition for other message bodies as used in the present document

Void.

Delete Annex B (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IM CN subsystem

Delete Annex C (normative): UICC and USIM Aspects for access to the IM CN subsystem

Delete Annex D (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem

Annex E (normative): IP-Connectivity Access Network specific concepts when using xDSL, Fiber or Ethernet to access IM CN subsystem

E.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is xDSL, Fiber or Ethernet.

NOTE: Fixed-broadband access in this Annex refers to xDSL, Fiber and Ethernet accesses.

E.2 Fixed broadband aspects when connected to the IM CN subsystem

E.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the fixed-broadband access network to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the IP Edge node, defined in ETSI ES 282 001 [138]in support of this communication are outside the scope of this document and specified elsewhere.

From the UEs perspective, it is assumed that one or more IP-CAN bearer(s) are provided, in the form of connection(s) managed by the layer 2 (e.g. DSL modem supporting the UE).

In the first instance, it is assumed that the IP-CAN bearer(s) is (are) statically provisioned between the UE and the IP Edge node, defined in ETSI ES 282 001 [138], according to the user's subscription.

It is out of the scope of the current Release to specify whether a single IP-CAN bearer is used to convey both signalling and media flows, or whether several PVC connections are used to isolate various types of IP flows (signalling flows, conversational media, non conversational media…).

The end-to-end characteristics of the fixed-broadband IP-CAN bearer depend on the type of access network, and on network configuration. The description of the network PVC termination (e.g., located in the DSLAM, in the BRAS…) is out of the scope of this annex.

E.2.2 Procedures at the UE

E.2.2.1 Activation and P-CSCF discovery

Fixed-broadband bearer(s) is (are) statically provisioned in the current Release.

Unless a static IP address is allocated to the UE, prior to communication with the IM CN subsystem, the UE shall perform a Network Attachment procedure depending on the used fixed-broadband access type. When using a fixed-broadband access, both IPv4 and IPv6 UEs may access the IM CN subsystem. The UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or a DNS Server IPv6 address(es) via RFC 3315 [40].

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1. In case the DHCP server provides several P-CSCF addresses or FQDNs to the UE, the UE shall select the P-CSCF address or FQDN as indicated in RFC 3319 [41]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

II. The UE selects a P-CSCF from the list in the IMS management object as specified in 3GPP TS 24.167 [8G].

The UE shall use method II to select a P-CSCF if the IMS management object contains the P-CSCF list. Otherwise, the UE shall use method I to select a P-CSCF.

E.2.2.1A Modification of a fixed-broadband connection used for SIP signalling

Not applicable.

E.2.2.1B Re-establishment of a fixed-broadband connection used for SIP signalling

Not applicable.

E.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to keep-alive requests the UE shall acquire a different P-CSCF address using any of the methods described in the subclause E.2.2.1 and perform an initial registration as specified in subclause 5.1.

E.2.2.2 Void

E.2.2.3 Void

E.2.2.4 Void

E.2.2.5 Fixed-broadband bearer(s) for media

E.2.2.5.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same fixed-broadband bearer.

E.2.2.5.1A Activation or modification of fixed-broadband bearers for media by the UE

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), and if several fixed-broadband bearers are available to the UE for the session, the media stream(s) may be sent on separate fixed-broadband bearers according to the indication of grouping. The UE may freely group media streams to fixed-broadband bearers in case no indication of grouping is received from the P-CSCF.

If the UE receives media grouping attributes in accordance with RFC 3524 [54] that it cannot provide within the available fixed-broadband bearer(s), then the UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header field from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header field when a SIP session is initiated, the UE shall reuse the existing fixed-broadband bearer(s) and ignore the media authorization token.

E.2.2.5.1B Activation or modification of fixed-broadband bearers for media by the network

Not applicable.

E.2.2.5.1C Deactivation of fixed-broadband bearers for media

Not applicable.

E.2.2.5.2 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

E.2.2.5.3 Unsuccessful situations

Not applicable.

E.2.2.6 Emergency service

If attached to network via fixed-broadband access technology, the UE shall always consider being attached to its home operator's network for the purpose of emergency calls.

NOTE: In fixed-broadband the UE is unable to receive any indication from the network, that would allow the UE to determine, whether it is currently attached to its home operator's network or to a different network, so the UE assumes itself always attached to the home operator's network when connected via fixed-broadband access technology.

E.2A Usage of SDP

E.2A.0 General

Not applicable.

E.2A.1 Impact on SDP offer / answer of activation or modification of xDSL bearer for media by the network

Not applicable.

E.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

E.2A.3 Emergency service

No additional procedures defined.

E.3 Application usage of SIP

E.3.1 Procedures at the UE

E.3.1.1 P-Access-Network-Info header field

The UE may, but need not, include the P-Access-Network-Info header field where indicated in subclause 5.1.

E.3.1.2 Availability for calls

Not applicable.

E.3.1.2A Availability for SMS

Void.

E.3.1.3 Authorization header field

When using SIP digest or SIP digest without TLS, the UE need not include an Authorization header field on sending a REGISTER request, as defined in subclause 5.1.1.2.1.

NOTE: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters. Therefore, the public user identity used for registration in this case cannot be shared across multiple UEs. Deployment scenarios that require public user identities to be shared across multiple UEs that don't include an private user identity in the initial REGISTER request can be supported as follows:

- Assign each sharing UE a unique public user identity to be used for registration,

- Assign the shared public user identitiess to the implicit registration set of the unique registering public user identities assigned to each sharing UE.

Delete Section E.3.2 Procedures at the P-CSCF

Delete *Section E.3.3 Procedures at the S-CSCF*

Delete *Section* E.4 3GPP specific encoding for SIP header field extensions

Delete *Section* E.5 Use of circuit-switched domain

Annex F (normative): Additional procedures in support for hosted NAT

NOTE: This subclause describes the mechanism for support of the hosted NAT scenario. This does not preclude other mechanisms but they are out of the scope of this annex.

F.1 Scope

This annex describes the UE and P-CSCF procedures in support of hosted NAT. In this scenario, both the media flows and the SIP signalling both traverse a NA(P)T device located in the customer premises domain. The term "hosted NAT" is used to address this function.

When receiving an initial SIP REGISTER request without integrity protection, the P-CSCF can, determine whether to perform the hosted NAT procedures for the user identified by the REGISTER request by comparing the address information in the top-most SIP Via header field with the IP level address information from where the request was received. The P-CSCF will use the hosted NAT procedure only when the address information do not match.

NOTE: There is no need for the P-CSCF to resolve a domain name in the Via header field when UDP encapsulated tunnel mode for IPsec is used. The resolution of a domain name in the Via header field is not required by RFC 3261 [26].

In order to provide hosted NAT traversal for SIP REGISTER requests without integrity protection and the associated responses, the P-CSCF makes use of the "received" and "rport" header field parameters as described in RFC 3261 [26] and RFC 3581 [56A]. The hosted NAT traversal for protected SIP messages is provided by applying UDP encapsulation to IPSec packets in accordance with RFC 3948 [63A].

Alternativly to the procedures defined in subclause F.2 which are employed to support the hosted NAT scenario where the security solution is based on UDP encapsulated IPSec as defined in 3GPP TS 33.203 [19], subclause F.4 provides procedures for NAT traversal for security solutions that are not defined in 3GPP TS 33.203 [19]. Use of such security solutions is outside the scope of this document.

F.2 Application usage of SIP

F.2.1 UE usage of SIP

F.2.1.1 General

This subclause describes the UE SIP procedures for supporting hosted NAT scenarios. The description enhances the procedures specified in subclause 5.1.

The UE shall support the symmetric response routeing mechanism according to RFC 3581 [56A].

F.2.1.2 Registration and authentication

F.2.1.2.1 General

The text in subclause 5.1.1.1 applies without changes

F.2.1.2.1A Parameters contained in the ISIM

The text in subclause 5.1.1.1A applies without changes

F.2.1.2.1B Parameters provisioned to a UE without ISIM or USIM

The text in subclause 5.1.1.1B applies without changes.

F.2.1.2.2 Initial registration

The procedures described in subclause 5.1.1.2.1 apply with the additional procedures described in the present subclause.

NOTE 1: In accordance with the definitions given in subclause 3.1 the IP address acquired initially by the UE in a hosted NAT scenario is the UE private IP address.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.2.1 with the exceptions of subitems c) and d) which are modified as follows

The UE shall populate:

c) a Contact header field according to the following rules: if the REGISTER request is sent without integrity protection, the Contact header field shall be set to include SIP URI(s) containing the private IP address of the UE in the hostport parameter or FQDN. If the UE supports GRUU, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the REGISTER request is integrity protected, the UE shall include the public IP address or FQDNin the hostport parameter. The UE shall only use a FQDN in a protected REGISTER request, if it is ensured that the FQDN resolves to the public IP address of the NAT. If the UE supports GRUU, the UE shall include a "+sip.instance" header field parameter containing the instance ID. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

NOTE 2: The UE will learn its public IP address from the "received" header field parameter in the topmost Via header field in the 401 (Unauthorized) response to the unprotected REGISTER request.

d) a Via header field according to the following rules: if the REGISTER request is sent without integrity protection, the Via header field shall be set to include the private IP address or FQDN of the UE in the sent-by field. If the REGISTER request is integrity protected, the UE shall include the public IP address or FQDN in the sent-by field. The UE shall only use a FQDN in a protected REGISTER request, if it is ensured that the FQDN resolves to the public IP address of the NAT. Unless the UE has been configured to not send keep-alives, it shall include a

"keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, the registration, as described in RFC 6223 [143];

NOTE 3: If the UE specifies a FQDN in the host parameter in the Contact header field and in the sent-by field in the Via header field of an unprotected REGISTER request, this FQDN will not be subject to any processing by the P-CSCF or other entities within the IM CN subsystem. The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

If IMS AKA is used as a security mechanism, on sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as defined in subclause 5.1.1.2.2, with the exceptions of subitems c), and d) which are modified as follows:

d) the Security-Client header field set to specify the security mechanisms the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the IPSec layer algorithms for integrity protection and for encryption as defined in 3GPP TS 33.203 [19], and shall announce support for them according to the procedures defined in RFC 3329 [48]. In addition to transport mode the UE shall support UDP encapsulated tunnel mode as per RFC 3948 [63A] and shall announce support for both modes as described in TS 33.203 [19];

When a 401 (Unauthorized) response to a REGISTER is received and this response is received without integrity protection, the procedures described in subclause 5.1.1.2.1 apply with the following additions:

The UE shall compare the values in the "received" header field parameter and "rport" header field parameter with the corresponding values in the sent-by parameter in the topmost Via header field to detect if the UE is behind a NAT. If the comparison indicates that the respective values are the same, the UE concludes that it is not behind a NAT.

- If the UE is not behind a NAT, the UE shall proceed with the procedures described in subclause 5.1 of the main body of this specification;

- If the UE is behind a NAT, the UE shall verify using the Security-Server header field that mode "UDP-enc-tun" is selected. If the verification succeeds the UE shall store the IP address contained in the "received" header field parameter as the UE public IP address. If the verification does not succeed the UE shall abort the registration.

In addition, when a 401 (Unauthorized) response to a REGISTER is received (with or without integrity protection) the UE shall behave as described in subclause F.2.1.2.5.

When the UE, that is behind a NAT, receives a 400 (Bad Request) response with 301 Warning header field indicating "incompatible network address format" to the unprotected REGISTER request, the UE shall randomly select new values for the protected server port and the protected client port, and perform new initiate registration procedure by sending an unprotected REGISTER request containing the new values in the Security-Client header field.

Editor's Note: [GINI CR#3968] The impact of bulk number registration procedures according to RFC 6140 [191] on the additional procedures in support for hosted NAT is FFS.

F.2.1.2.3 Initial subscription to the registration-state event package

The procedures described in subclause 5.1.1.3 apply with the additional procedures described in subclause F.2.1.4.1.

F.2.1.2.4 User-initiated re-registration

The procedures described in subclause 5.1.1.4.1 apply with the additional procedures described in the present subclause.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as indicated in subclause 5.1.1.4.1 with the exception of subitems c) and d) which are modified as follows.

The UE shall populate:

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the public IP address of the UE or FQDN, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP

address of the NAT. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continous support to send keep-alives, as described in RFC 6223 [143];

NOTE 1: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

When the UE, that is behind a NAT, receives a 400 (Bad Request) response with 301 Warning header field indicating "incompatible network address format" to the REGISTER request that does not contain a challenge response, the UE shall randomly select a new value for the protected client port, and send the REGISTER request containing the new values in the Security-Client header field.

NOTE 2: The protected server port stays fixed for a UE until all public user identities of the UE have been de-registered.

Editor's Note: [GINI CR#3968] The impact of bulk number registration procedures according to RFC 6140 [191] on the additional procedures in support for hosted NAT is FFS.

F.2.1.2.5 Authentication

Delete Section F.2.1.2.5.1IMS AKA - general

Delete Section F.2.1.2.5.2Void

Delete Section F.2.1.2.5.3IMS AKA abnormal cases

F.2.1.2.5.4 SIP digest – general

Not applicable.

F.2.1.2.5.5 SIP digest – abnormal procedures

Not applicable.

F.2.1.2.5.6 SIP digest with TLS – general

Not applicable.

F.2.1.2.5.7 SIP digest with TLS – abnormal procedures

Not applicable.

F.2.1.2.5.8 Abnormal procedures for all security mechanisms

The text in subclause 5.1.1.5.8 applies without changes.

F.2.1.2.5A Network-initiated re-authentication

The text in subclause 5.1.1.5A applies without changes.

F.2.1.2.5B Change of IPv6 address due to privacy

The text in subclause 5.1.1.5B applies without changes.

F.2.1.2.6 User-initiated deregistration

The procedures of subclause 5.1.1.6.1 apply with with the additional procedures described in the present subclause.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.6 with the exception of subitems d) and e) which are modified as follows.

The UE shall populate:

c) a Contact header field set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN; and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

NOTE 1: In case of hosted NAT traversal only the UE public IP addresses are bound to security associations.

NOTE 2: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

Editor's Note: [GINI CR#3968] The impact of bulk number registration procedures according to RFC 6140 [191] on the additional procedures in support for hosted NAT is FFS.

F.2.1.2.7 Network-initiated deregistration

The procedures of subclause 5.1.1.7 apply with with the additional procedures described in the present subclause.

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated"; or

- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause F.2.1.2.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

F.2.1.3 Subscription and notification

The text in subclause 5.1.2 applies without changes.

F.2.1.4 Generic procedures applicable to all methods excluding the REGISTER method

F.2.1.4.1 UE originating case

The procedures described in subclause 5.1.2A.1 apply with the additional procedures described in the present subclause.

When the UE sends any request, the requirements in subclause 5.1.2A.1 are replaced by the following requirements. The UE shall include:

- a Via header field set to include the public IP address of the UE or FQDN and the protected server port in the sent-by field. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of

the NAT; and if this is a request for a new dialog, and the request includes a Contact header field, then the UE should populate the Contact header field as follows:

1) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93]; or

2) if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then insert the temporary GRUU ("temp-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93].

If this is a request within an existing dialog, and the request includes a Contact header field, and the contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

If the UE did not insert a GRUU in the Contact header field, then the UE shall include the public IP address of the UE or FQDN and the protected server port in the hostport parameter in any Contact header field that is otherwise included. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

NOTE: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

The UE shall discard any SIP response that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause F.2.1.2.4.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause F.2.1.2.3.

F.2.1.4.2 UE terminating case

The procedures described in subclause 5.1.2A.2 apply with the additional procedures described in the present subclause.

When the UE sends any response, the requirements in subclause 5.1.2A.1 are replaced by the following requirement.

If the response includes a Contact header field, and the response is not sent within an existing dialog, then the UE should populate the Contact header field as follows:

1) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does not indicate privacy of the P-Asserted-Identity, then insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93]; and

2) if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93].

If the UE did not insert a GRUU in the Contact header field, then the UE shall:

- include the public IP address of the UE or FQDN and the protected server port in the hostport parameter in any Contact header field that is otherwise included. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

NOTE: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause F.2.1.2.

Delete Section F.2.2 P-CSCF usage of SIP

Delete Section F.2.3 S-CSCF usage of SIP

F.3 Void

Delete Section F.4 P-CSCF usage of SIP in case UDP encapsulated IPsec is not employed

F.5 NAT traversal for media flows

To allow the IMS access gateway to perform address latching, for a given UDP-based media stream, the UE shall use the same port number for sending and receiving packets.

To allow early media flows, the UE shall send keepalive messages for each UDP-based media stream as soon as an SDP offer or answer is received in order to allow the IMS access gateway to perform address latching before the call is established.

To keep NAT bindings and firewall pinholes open for the UDP-based media streams, and enable the IMS access gateway to perform address latching, the UE shall send keepalive messages for each media stream as defined in subclause K.5.2.1.

Annex G (informative):
Void

Delete Section Annex H (normative):
IP-Connectivity Access Network specific concepts when using DOCSIS to access IM CN subsystem

Delete Section Annex I (normative):
Additional routeing capabilities in support of transit, roaming and interconnection traffics in IM CN subsystem

Annex J (normative):
Void

Annex K (normative):
Additional procedures in support of UE managed NAT traversal

K.1 Scope

This annex describes the UE, P-CSCF, and S-CSCF procedures in support of UE managed NAT traversal. For ICE, the IBCF procedures are also described. In this scenario, both the media flows and the SIP signalling both traverse a NA(P)T device located in the customer premises domain. The term "hosted NAT" is used to address this function. This annex does not consider the case where the NAT is behind the P-CSCF as different NAT traversal procedures are necessary for this architectural scenario.

The procedures described in this subclause of this annex rely on the UE to manage the NAT traversal process. As part of the UE management process, the UE can learn whether it is behind a NAT or not, and choose whether the proceedures in this annex are applied or not.

The protection of SIP messages is provided by applying either UDP encapsulation to IPSec packets in accordance with RFC 3948 [63A] and as defined in 3GPP TS 33.203 [19] or by utilizing TLS as defined in 3GPP TS 33.203 [19].

NOTE 1: This annex describes the mechanism for support of UE managed NAT traversal scenario defined in 3GPP TS 23.228 [7]. This does not preclude other mechanisms but they are out of the scope of this annex.

NOTE 2: It is recognized that outbound can be useful for capabilities beyond NAT traversal (e.g. multiple registrations) however this annex does not consider such capabilities at this time. Such capabilites can require additional information elements in the REGISTER request so that the P-CSCF and S-CSCF can distinguish whether to apply procedures as of annex F or annex K.

K.2 Application usage of SIP

K.2.1 Procedures at the UE

K.2.1.1 General

This subclause describes the UE SIP procedures for supporting a UE managed hosted NAT traversal approach. The description enhances the procedures specified in subclause 5.1.

K.2.1.2 Registration and authentication

K.2.1.2.1 General

The text in subclause 5.1.1.1 applies without changes.

K.2.1.2.1A Parameters contained in the ISIM

The text in subclause 5.1.1.1A applies without changes.

K.2.1.2.1B Parameters provisioned to a UE without ISIM or USIM

The text in subclause 5.1.1.1B applies without changes.

K.2.1.2.2 Initial registration

K.2.1.2.2.1 General

The procedures described in subclause 5.1.1.2.1 apply with the additional procedures described in the present subclause.

NOTE 1: In accordance with the definitions given in subclause 3.1 the IP address acquired initially by the UE in a hosted NAT scenario is the UE private IP address.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subitems a) through j) of subclause 5.1.1.2 with the exceptions of subitems c) and d) which are modified as follows.

The UE shall populate:

c) a Contact header field according to the following rules: the Contact header field shall be set to include SIP URI(s) containing the private IP address or FQDN of the UE in the hostport parameter. The UE shall also include an instance ID ("+sip.instance" header field parameter) and "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for theIMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the private IP address or FQDN of the UE in the sent-by field. For TCP, the response is received on the TCP connection on which the request was sent. For UDP, the UE shall include the "rport" header field parameter as defined in RFC 3581 [56A].

NOTE 2: The UE will learn its public IP address from the "received" header field parameter in the topmost Via header field in the 401 (Unauthorized) response to the unprotected REGISTER request.

NOTE 3: If the UE specifies a FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field of an unprotected REGISTER request, this FQDN will not be subject to any processing by the P-CSCF or other IMS entities.

When a 401 (Unauthorized) response to a REGISTER request is received with integrity protection the UE shall behave as described in subclause K.2.1.2.5.

When a 401 (Unauthorized) response to a REGISTER request is received and this response is received without integrity protection, the procedures described in subclause 5.1.1.2 apply with the following additions:

The UE shall compare the values in the "received" header field parameter and "rport" header field parameter with the corresponding values in the sent-by parameter in the topmost Via header field to detect if the UE is behind a NAT. If the comparison indicates that the respective values are the same, the UE concludes that it is not behind a NAT.

- if the UE is not behind a NAT the UE shall proceed with the procedures described in subclause 5.1;
- if the UE is behind a NAT the UE shall verify using the Security-Server header field that either the mechanism-name "tls" or "ipsec-3gpp" and the mode "UDP-enc-tun" is selected. If the verification succeeds the UE shall behave as described in subclause K.2.1.2.5 and store the IP address contained in the "received" header field parameter as the UE's public IP address. If the verification does not succeed the UE shall abort the registration.

On receiving the 200 (OK) response to the REGISTER request, the procedures described in subclause 5.1.1.2 apply with the following additions:

The UE shall determine the P-CSCFs ability to support the keep-alive procedures as described in RFC 5626 [92] by checking whether the "outbound" option-tag is present in the Require header field:

- if no "outbound" option-tag is present, the UE may use some other explicit indication in order to find out whether the P-CSCF supports the outbound edge proxy functionality. Such indication may be acomplished either through UE local configuration means or the UE can examine the 200 (OK) response to its REGISTER request for Path header fields, and if such are present check whether the bottommost Path header field contains the "ob" SIP URI parameter. If the UE determines that the P-CSCF supports the outbound edge proxy functionality, the UE can use the keep-alive techniques defined in subclause K.2.1.5 and RFC 5626 [92] towards the P-CSCF; or
- if an "outbound" option-tag is present, the UE shall initiate keep-alive mechanisms as defined in subclause K.2.1.5 and RFC 5626 [92] towards the P-CSCF.

NOTE 4: Presence of the "outbound" option-tag in the Require header field indicates that both the P-CSCF and S-CSCF fully support the outbound procedures. The number of subsequent outbound registrations for the same private user identity but with a different reg-id value is based on operator policy.

Delet Section ~~*K.2.1.2.2.2 Initial registration using IMS AKA*~~

K.2.1.2.2.3 Initial registration using SIP digest without TLS

The procedures described in subclause 5.1.1.2.3 apply without modification.

K.2.1.2.2.4 Initial registration using SIP digest with TLS

The procedures described in subclause 5.1.1.2.4 apply without modification.

K.2.1.2.2.5 Initial registration using NASS-IMS bundled authentication

The procedures described in subclause 5.1.1.2.5 apply without modification.

K.2.1.2.3 Initial subscription to the registration-state event package

The procedures described in subclause 5.1.1.3 apply with the additional procedures described in subclause K.2.1.4.1.

K.2.1.2.4 User-initiated re-registration

K.2.1.2.4.1 General

The procedures described in subclause 5.1.1.4 apply with the additional procedures described in the present subclause.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as indicated in subclause 5.1.1.4.1 with the exception of subitems c) and d) which are modified as follows.

The UE shall populate:

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the private IP address of the UE or FQDN, its instance ID ("+sip.instance" header field parameter) along with the same "reg-id" header field parameter used for the initial, successful, registration for the given P-CSCF public identity combination as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62]; and

d) a Via header field according to the following rules:

- For UDP, the UE shall include the public IP address or FQDN in the sent-by field. The UE shall also include the "rport" header field parameter as defined in RFC 3581 [56A]. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; or

- For TCP, the UE shall include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

When the timer F expires at the UE, the UE shall:

1) stop processing of all ongoing dialogs and transactions associated with that, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs); and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE shall follow the procedures in RFC 5626 [92] to form a new flow to replace the failed one. When registering to create a new flow to replace the failed one, procedures in subclause 5.1.1.2 apply.

NOTE: These actions can also be triggered as a result of the failure of a STUN keep-alive. It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g., based on ICMP messages.

If failed registration attempts occur in the process of creating a new flow, the flow recovery procedures defined in RFC 5626 [92] shall apply.

Delete Section K.2.1.2.4.2 IMS AKA as a security mechanism

K.2.1.2.4.3 SIP Digest without TLS as a security mechanism

The procedures described in subclause 5.1.1.4.3 apply without modification.

K.2.1.2.4.4 SIP Digest with TLS as a security mechanism

The procedures described in subclause 5.1.1.4.4 apply without modification.

K.2.1.2.4.5 NASS-IMS bundled authentication as a security mechanism

The procedures described in subclause 5.1.1.4.5 apply without modification.

K.2.1.2.5 Authentication

Delete Section K.2.1.2.5.1 IMS AKA – general

~~*K.2.1.2.5.2 Void*~~

Delete Section K.2.1.2.5.3 IMS AKA abnormal cases

K.2.1.2.5.4 SIP digest without TLS – general

The text in subclause 5.1.1.5.4 applies without changes.

K.2.1.2.5.5 SIP digest without TLS – abnormal procedures

The procedures of subclause 5.1.1.5.5 apply with the additional procedures described in the present subclause.

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed. If performing SIP digest with TLS, the UE should send an initial REGISTER according to the procedure specified in subclause K.2.1.2.2 if the UE considers the TLS session to be no longer active at the P-CSCF.

K.2.1.2.5.6 SIP digest with TLS – general

The text in subclause 5.1.1.5.6 applies without changes.

K.2.1.2.5.7 SIP digest with TLS – abnormal procedures

The text in subclause 5.1.1.5.7 applies without changes.

K.2.1.2.5.8 NASS-IMS bundled authentication – general

The text in subclause 5.1.1.5.8 applies without changes.

K.2.1.2.5.9 NASS-IMS bundled authentication – abnormal procedures

The text in subclause 5.1.1.5.9 applies without changes.

K.2.1.2.5.10 Abnormal procedures for all security mechanisms

The text in subclause 5.1.1.5.10 applies without changes.

K.2.1.2.5A Network initiated re-authentication

The procedures of subclause 5.1.1.5A apply with the additional procedures described in the present subclause.

On starting the re-authentication procedure sending a REGISTER request that does not contain a challenge response, the UE shall behave as of subclause 5.1.1.5A with the exception of subitem 2) which is is modified as follows.

The UE shall:

2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a re-registration as described in subclause K.2.1.2.4, if required.

K.2.1.2.5B Change of IPv6 address due to privacy

The text in subclause 5.1.1.5B applies without changes.

K.2.1.2.6 User-initiated deregistration

K.2.1.2.6.1 General

The procedures of subclause 5.1.1.6.1 apply with the additional procedures described in the present subclause.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.6.1 with the exception of subitems c) and d) which are modified as follows.

The UE shall populate:

c) a Contact header field set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, its instance ID ("+sip.instance" header field parameter) along with the same "reg-id" header field parameter used for the initial, successful, registration for the given P-CSCF public identity combination as described in RFC 5626 [92];. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

d) a Via header field according to the following rules:

- For UDP, the UE shall include the public IP address or FQDN. The UE shall also include the "rport" header field parameter as defined in RFC 3581 [56A]. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; or

- For TCP, the UE shall include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

NOTE: In case of hosted NAT traversal only the UE public IP addresses are bound to security associations or TLS session.

Delete Section K.2.1.2.6.2 IMS AKA as a security mechanism

K.2.1.2.6.3 SIP digest as a security mechanism

The text in subclause 5.1.1.6.3 applies without changes.

K.2.1.2.6.4 SIP digest with TLS as a security mechanism

The text in subclause 5.1.1.6.4 applies without changes.

K.2.1.2.6.5 Initial registration using NASS-IMS bundled authentication

The text in subclause 5.1.1.6.5 applies without changes.

K.2.1.2.7 Network-initiated deregistration

The procedures of subclause 5.1.1.7 apply with the additional procedures described in the present subclause.

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated"; or

- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

The UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause K.2.1.2.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

K.2.1.3 Subscription and notification

The text in subclause 5.1.2 applies without changes.

K.2.1.4 Generic procedures applicable to all methods excluding the REGISTER method

K.2.1.4.1 UE-originating case

The procedures described in subclause 5.1.2A.1 apply with the additional procedures described in the present subclause.

When the UE sends any request, the requirements in subclause 5.1.2A.1 are extended by the following requirements. The UE shall include:

- a Via header field according to the following rules:

  - For UDP, the UE shall include the public IP address or FQDN and the protected server port value in the sent-by field. The UE shall also include the "rport" header field parameter as defined in RFC 3581 [56A]. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; or

- For TCP, the UE shall include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; and

- if the request contains a Contact header field, include a Contact header field according to the following rules:

  - if this is a request for a new or existing dialog, and the UE did insert a GRUU in the Contact header field, then the UE shall also include its instance ID ("+sip.instance" header field parameter), and an "ob" SIP URI parameter as described in RFC 5626 [92]; or

  - if this is a request for a new or existing dialog, and the UE did not insert a GRUU in the Contact header field, then the UE shall include the public IP address of the UE or FQDN and the protected server port value bound to the security association or TLS session in the hostport parameter along with its instance ID ("+sip.instance" header field parameter), and an "ob" SIP URI parameter as described in RFC 5626 [92]. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

NOTE: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

Where a security association or TLS session exists, the UE shall discard any SIP response that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause K.2.1.2.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause K.2.1.2.4.

K.2.1.4.2 UE-terminating case

The procedures described in subclause 5.1.2A.2 apply with the additional procedures described in the present subclause.

When the UE sends any response, the requirements in subclause 5.1.2A.2 are extended by the following requirement. If the UE did not include a GRUU in the Contact header field, then the UE shall:

- include the public IP address of the UE or FQDN and the protected server port value bound to the security association or TLS session in the hostport parameter in any Contact header field that is otherwise included. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause K.2.1.2.

K.2.1.5 Maintaining flows and detecting flow failures

STUN Binding Requests are used by the UE as a keep-alive mechanism to maintain NAT bindings for signalling flows over connectionless transport (for dialogs outside a registration as well as within a registration) as well as to determine whether a flow (as described in RFC 5626 [92]) is still valid (e.g. a NAT reboot could cause the transport parameters to change). As such, the UE acts as a STUN client and shall follow the requirements defined by RFC 5389 [100]. Further, when using UDP encapsulated IPsec, the keep-alive capabilities defined within should not be used.

CRLF as defined in RFC 5626 [92] is used by the UE as a keep-alive mechanism to maintain NAT bindings for signalling flows over connection oriented transports (for dialogs outside a registration as well as within a registration) as well as to determine whether a flow (as described in RFC 5626 [92]) is still valid (e.g. a NAT reboot could cause the transport parameters to change). As such, the UE shall follow the requirements defined by RFC 5626 [92].

If the UE determines that the flow to a given P-CSCF is no longer valid (the UE does not receive a STUN reply (or CRLF) or the reply indicates a new public IP Address) the UE shall consider the flow and any associated security associations invalid and perform the initial registration procedures defined in subclause K.2.1.2.2.

When a NAT is not present, it may not be desirable to send keep-alive requests (i.e. given battery considerations for wireless UEs). As such, if a UE can reliably determine that a NAT is not present (i.e. by comparing the "received" and "rport" header field parameters in the Via header field in the response to the initial un-protected REGISTER request with the locally assigned IP Address and Port) then the UE may not perform the keep-alive procedures.

Delete Section K.2.1.6 Emergency services

NOTE: The implementation of the emergency service is Deutsche Telekom specific.

Delete Section K.2.2 Procedures at the P-CSCF

~~*K.2.3*~~ Void

K.2.4 Void

K.3 Application usage of SDP

K.3.1 UE usage of SDP

The procedures as of subclause 6.1 apply.

~~*K.3.2 P-CSCF usage of SDP*~~

The procedures as of subclause 6.2 apply.

K.4 Void

K.5 Application usage of ICE

K.5.1 Introduction

The following subclauses describe the usage of the Interactive Connectivity Establishment (ICE) procedures as documented in RFC 5245 [99]

K.5.2 UE usage of ICE

K.5.2.1 General

NAT bindings also need to be kept alive for media. RFC 5245 [99] provides requirements for STUN based keepalive mechanisms. UEs that do not implement the ICE procedures as defined in RFC 5245 [99] should implement the keepalive procedures defined in RFC 5245 [99]. In the case where keepalives are required and the other end does not support ICE (such that STUN cannot be used for a keepalive) or the UE can not discover STUN or TURN servers to gather candidates, the UE shall send an empty (no payload) RTP packet with a payload type of 20 as a keepalive as long as the other end has not negotiated the use of this value. If this value has already been negotiated, then some other unused static payload type from table 5 of RFC 3551 [55A] shall be used. When sending an empty RTP packet, the UE shall continue using the sequence number (SSRC) and timestamp as the negotiated RTP steam.

K.5.2.2 Call initiation – UE-origination case

The UE should support the agent requirements for ICE as defined by RFC 5245 [99] when sending the initial INVITE request. RFC 5245 [99] provides procedures for:

1) Gathering candidate addresses for RTP and RTCP prior to sending the INVITE;

2) Encoding the candidate addresses in the SDP that is included with the INVITE;

3) Acting as a STUN server to receive binding requests from the remote client when it does connectivity checks;

4) Performing connectivity checks on received candidate addresses for RTP and RTCP;

5) Determining and possibly selecting a better active address based on the requirements in RFC 5245 [99];

6) Subsequent offer/answer exchanges; and

7) Sending media.

When supporting the ICE procedures, the UE shall also support the STUN agent requirements as described in RFC 5389 [100] in order to gather STUN addresses, the TURN client requirements as described in RFC 5766 [101] in order to gather TURN Server addresses and the STUN Server requirements defined in RFC 5245 [99] as well as the requirements for STUN Servers defined in RFC 5389 [100] for responding to connectivity checks.

RFC 5245 [99] provides an algorithm for determining the priority of a particular candidate. The following additional requirements are provided to the UE:

1) The type preference assigned for each type of candidate from least to highest should be: Relayed Transport Address, STUN address, local address; and

2) If the UE has a dual IPv4/IPv6 stack, IPv6 addresses may be assigned a higher local preference than IPv4 addresses based on the operator's policy.

RFC 5245 [99] provides guidance on choosing the in-use candidate and recommends that a UE choose relayed candidates as the in-use address. The following additional requirements are provided to the UE:

1) If a TURN server is available, the Relayed Transport Address should be used as the initial active transport address (i.e. as advertised in the m/c lines of the SDP); and

2) If a TURN server is not available, an address obtained via STUN should be used as the initial active transport address.

Regardless of whether the UE supports the above procedures, the UE shall, upon receipt of an SDP answer with candidate addresses, perform connectivity checks on the candidate addresses as described in RFC 5245 [99]. In order to perform connectivity checks, the UE shall act as a STUN client as defined in RFC 5389 [100]. Further, the UE shall also follow the procedures in RFC 5245 [99] when sending media.

K.5.2.3 Call termination – UE-termination case

The UE should support agent requirements for ICE as defined by RFC 5245 [99] when receiving an initial INVITE request. RFC 5245 [99] provides procedures for:

1) Gathering candidate addresses for RTP and RTCP prior to sending the answer as described in RFC 5245 [99];

2) Encoding the candidate addresses in the SDP answer as described in RFC 5245 [99];

3) Acting as a STUN server to receive binding requests from the remote client when it does connectivity checks;

4) Performing connectivity checks on received candidate addresses for RTP and RTCP;

5) Determining and possibly selecting a better active address based on the requirements in RFC 5245 [99];

6) Subsequent offer/answer exchanges; and

7) Sending media.

When supporting the ICE procedures, the UE shall also support the STUN agent requirements as described in RFC 5389 [100] in order to gather STUN addresses, the TURN client requirements as described in RFC 5766 [101] in order to gather TURN Server addresses and the STUN Server requirements defined in RFC 5245 [99] as well as the requirements for STUN Servers defined in RFC 5389 [100] for responding to connectivity checks.

RFC 5245 [99] provides an algorithm for determining the priority of a given candidate. The additional requirements for the UE:

1) The priority of candidate addresses from least to highest should be: Relayed Transport Address, STUN address, local address; and

2) If the UE has a dual IPv4/IPv6 stack, IPv6 addresses MAY be placed at a higher priority than IPV4 addresses based on the operator's policy.

RFC 5245 [99] provides guidance on choosing the in-use candidate and recommends that a UE choose relayed candidates as the in-use address. The following additional requirements are provided to the UE:

1) If a TURN server is available, the Relayed Transport Address should be used as the initial active transport address (i.e. as advertised in the m/c lines of the SDP); and

2) If a TURN server is not available, an address obtained via STUN should be used as the initial active transport address.

Regardless of whether the UE supports the above procedures, the UE shall, upon receipt of an SDP offer with candidate addresses, perform connectivity checks on the candidate addresses as described in RFC 5245 [99]. In order to perform connectivity checks, the UE shall act as a STUN client as defined in RFC 5389 [100]. Further, the UE shall also follow the procedures in RFC 5245 [99] when sending media.

When receiving an SDP offer which does not indicate support for ICE, the UE aborts the ICE procedures and reverts to RFC 3264 [27B] offer/answer procedures; per RFC 5245 [99]. However, if the terminating UE is behind a NA(P)T device this may result in the inability to pass media for the session as the terminating UE will respond with its locally assigned IP address which is unreachable. In order to ensure successful media exchange, the terminating UE shall provide either a STUN derived IP address and port or a TURN provided IP address and port in the m/c lines of the SDP answer. If the provided address and port is a TURN address and port, the policy charging and control framework will be unable to establish proper filter criteria as the address is that of the TURN server and not that of the UE or NAT in front of the UE; see RFC 5245 [99] subclause B.3 for further details. To rectify this issue, the terminating UE shall also include a candidate attribute as described in RFC 5245 [99] identifying the server reflexive IP address and port (i.e. the IP address and port on the public side of the NAT) used when a TURN provided address and port is provided in the m/c line of the SDP answer.

Delete Section K.5.3 P-CSCF support of ICE

K.5.4 **Void**

Delete Section Annex L (normative): IP-Connectivity Access Network specific concepts when using EPS to access IM CN subsystem

Delete Annex M (normative): IP-Connectivity Access Network specific concepts when using cdma2000® packet data subsystem to access IM CN subsystem

Delete Annex N (Normative): Functions to support overlap signalling

Delete Section Annex O (normative): IP-Connectivity Access Network specific concepts when using the EPC via cdma2000® HRPD to access IM CN subsystem

Annex P (Informative): Definition for DTMF info package

P.1 Scope

This annex defines an info package (see RFC 6086 [25]) for sending Dual Tone Multi Frequency (DTMF) tones using SIP INFO requests.

P.2 DTMF info package

P.2.1 General

This subclause contains the information required for the IANA registration of an info package.

Editor's note: MCC needs to register the DTMF info package with IANA once this annex has been incorporated into 3GPP TS 24.229.

P.2.2 Overall description

DTMF tones are normally sent when a user presses a button on the terminal. Each tone, identified by a unique frequency, represents a number (0-9) or a special character. The DTMF info package is used to transport that value.

The DTMF info package can be used to transport a single DTMF tone, or a series of tones. If a series of tones is transported in a single SIP INFO request, it is not possible to indicate the duration between each tone in the series.

The DTMF info package is not defined for a specific application. Any application, where sending of DTMF tones using the SIP INFO method is required, can used the DTMF info package.

P.2.3 Applicability

The info package mechanism for transporting DTMF tones has been chosen because it allows SIP entities that do not have access to the user plane (where DTMF tones can also be transported) to send and receive tones. The mechanism also allows the tones to be sent inside an existing dialog, using the same signalling path as other SIP messages within the dialog, rather than having to establish a separate dialog (DTMF tones can also be transported using subscription event packages).

P.2.4 Info package name

The name of the DTMF info package is: infoDtmf

P.2.5 Info package parameters

No parameters are defined for the DTMF info package.

P.2.6 SIP option tags

No SIP option tags are defined for the DTMF info package.

P.2.7 INFO message body parts

P.2.7.1 General

The DTMF digits are carried in the Overlap digit message body, defined in annex G of 3GPP TS 29.163 [11B].

P.2.7.2 MIME type

The MIME type value for the message body is "application/x-session-info", defined in annex G of 3GPP TS 29.163 [11B].

P.2.7.3 Content disposition

The Content Disposition value for the message body, when associated with the DTMF info package, is "info-package" (see RFC 6086 [25]).

P.2.8 Info package usage restrictions

No usage restrictions are defined for the DTMF info package.

If SIP entities support multiple mechanisms for sending DTMF tones they need to ensure, using negotiation mechanisms, that each entity is aware of which mechanism is used.

P.2.9 Rate of INFO requests

No maximum rate or minimum rate is defined for sending INFO requests associated with the DTMF info package.

When DTMF tones are triggered by user interaction, the DTMF tones are normally generated when the user pushes a button. Specific applications can decide upon which rate DTMF tones are generated. However, the DTMF info package does not provide a feedback mechanism to indicate to the sender that the rate of DTMF tones is too slow or fast.

P.2.10 Info package security considerations

No additional security mechanism is defined for the DTMF info package.

The security of the DTMF info package is based on the generic security mechanism provided for the underlaying SIP signalling.

P.2.11 Implementation details and examples

Examples of the DTMF info package usage can be found in the following specification:

- 3GPP TS 24.182 [8Q]: "Customized Alerting Tones; Protocol specification".

Delete Annex Q (normative):
IP-Connectivity Access Network specific concepts when using the cdma2000® 1x Femtocell Network to access IM CN subsystemDelete Section Annex R (normative):
IP-Connectivity Access Network specific concepts when using the EPC via WLAN to access IM CN subsystem

Delete Section Annex S (normative):
IP-Connectivity Access Network specific concepts when using DVB-RCS2 to access IM CN subsystem

Annex T (informative):
Change history

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					Version 0.0.0 Editor's internal draft			
					Version 0.0.1 Editor's internal draft			
					Version 0.0.2 Editor's internal draft			
		N1-001060			Version 0.0.3 Submitted to CN1 SIP adhoc #1			
19/10/00		N1-001109			Version 0.0.4 Reflecting results of initial CN1 discussion			
19/10/00		N1-001115			Version 0.0.5 Reflecting output of CN1 SIP adhoc#1 discussion			
09/11/00					Version 0.0.6 Revision to include latest template and styles			
		N1-010092			Version 0.0.7 Reflecting updates of some IETF drafts			
14/02/01		N1-010269			Version 0.0.8 Revision to include temporary annex B incorporating valuable source material			
18/03/01		N1-010378 rev			Version 0.1.0 incorporating results of CN1 discussion at CN1 #16			
12/04/01		N1-010737			Version 0.2.0 incorporating results of CN1 discussions at SIP adhoc #4			
11/06/01		N1-010935			Version 0.3.0 incorporating results of CN1 discussions at CN1 #16			
23/07/01		N1-011103			Version 0.4.0 incorporating results of CN1 discussions at CN1 #18 (agreed documents N1-011028, N1-011050, N1-011055, N1-011056)			
12/09/01		N1-011385			Version 0.5.0 incorporating results of CN1 discussions at CN1 #19 (agreed documents N1-011109, N1-011152, N1-011195, N1-011312, N1-011319, N1-011343)			
04/10/01		N1-011470			Version 0.6.0 incorporating results of CN1 discussions at CN1 #19bis (agreed documents N1-011346, N1-011373, N1-011389, N1-011390, N1-011392, N1-011393, N1-011394, N1-011408, N1-011410, N1-011426)			
19/10/01		N1-011643			Version 0.7.0 incorporating results of CN1 discussions at CN1 #20 (agreed documents N1-011477, N1-011479, N1-011498, N1-011523, N1-011548, N1-			

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					011585, N1-011586, N1-011592, N1-011611, N1-011629)			
16/11/01		N1-011821			Version 0.8.0 incorporating results of CN1 discussions at CN1 #20bis (agreed documents N1-011685, N1-011690, N1-011741, N1-011743, N1-011759, N1-011760, N1-011761, N1-011765c, N1-011767, N1-011769, N1-011770, N1-011771, N1-011774, N1-011777, N1-011779, N1-011780) N1-011712 was agreed but determined to have no impact on the specification at this time.			
30/11/01		N1-020010			Version 1.0.0 incorporating results of CN1 discussions at CN1 #21 (agreed documents N1-011828, N1-011829, N1-011836, N1-011899 [revision marks not used on moved text - additional change from chairman's report incorporated], implementation of subclause 3.1 editor's note based on discussion of N1-011900 [chairman's report], N1-011905, N1-011984, N1-011985, N1-011986, N1-011988, N1-011989, N1-012012 [excluding points 2 and 16], N1-012013, N1-012014 [excluding point 1], N1-012015, N1-012021, N1-012022, N1-012025, N1-012031, N1-012045, N1-012056, N1-012057) CN1 agreed for presentation for information to CN plenary.			
18/01/02		N1-020189			Version 1.1.0 incorporating results of CN1 discussions at CN1 SIP ad-hoc (agreed documents N1-020015, N1-020053, N1-020064, N1-020101, N1-020123, N1-020124, N1-020142, N1-020146, N1-020147, N1-020148, N1-020151, N1-020157, N1-020159, N1-020165). Also N1-012000 (agreed at previous meeting) required, subclause 5.2.6 to be deleted and this change has been enacted			
01/02/02		N1-020459			Version 1.2.0 incorporating results of CN1 discussions at CN1 #22 (agreed documents N1-020198, N1-020396, N1-020398, N1-020399, N1-020408, N1-020417, N1-020418, N1-020419, N1-020421, N1-020422, N1-020436, N1-020437, N1-020449)			
01/02/02		N1-020569			Version 1.2.1 issues to correct cut and paste error in incorporation of Annex B into main document. Affected subclause 5.1.1.3. Change to clause 7 title that was incorrectly applied to subclause 7.2 also corrected.			
22/02/02					Advanced to version 2.0.0 based on agreement of N1-020515. Version 2.0.0 incorporating results of CN1 discussions at CN1 #22bis (agreed documents N1-020466, N1-020468, N1-020469, N1-020472, N1-020473, N1-020500, N1-020504, N1-020507, N1-020511, N1-020512, N1-020521, N1-020583, N1-020584, N1-020602, N1-020603, N1-020604, N1-020611, N1-020612, N1-020613, N1-020614, N1-020615, N1-020617, N1-020623, N1-020624, N1-020625, N1-020626, N1-020627, N1-020642, N1-020643, N1-020646, N1-020649, N1-020656, N1-020659, N1-020668, N1-020669, N1-020670, N1-020671). In addition N1-020409, agreed at CN1#22 but missed from the previous version, was also implemented.			

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					References have been resequenced.			
02/03/02					Editorial clean-up by ETSI/MCC.	2.0.0	2.0.1	
11/03/02	TSG CN#15	NP-020049			The draft was approved, and 3GPP TS 24.229 was then to be issued in Rel-5 under formal change control.	2.0.1	5.0.0	
2002-06	NP-16	NP-020230	004	1	S-CSCF Actions on Authentication Failure	5.0.0	5.1.0	N1-020903
2002-06	NP-16	NP-020230	005	2	Disallow Parallel Registrations	5.0.0	5.1.0	N1-020959
2002-06	NP-16	NP-020230	007	1	Hiding	5.0.0	5.1.0	N1-020910
2002-06	NP-16	NP-020312	008	8	Support for services for unregistered users	5.0.0	5.1.0	
2002-06			009	1	Not implemented nor implementable. In the meeting report CN1#24 under doc N1-021513 it is shown that CR095r2 supercedes 009r1 if 095r2 was to be approved in CN#16 (but unfortunately 009r1 was also approved in the the CN#16 draft minutes).			N1-020921
2002-06	NP-16	NP-020231	019		MGCF procedure clarification	5.0.0	5.1.0	N1-020788
2002-06	NP-16	NP-020231	020	2	MGCF procedure error cases	5.0.0	5.1.0	N1-020960
2002-06	NP-16	NP-020231	022	1	Abbreviations clean up	5.0.0	5.1.0	N1-020949
2002-06	NP-16	NP-020231	023		Clarification of SIP usage outside IM CN subsystem	5.0.0	5.1.0	N1-020792
2002-06	NP-16	NP-020314	024	3	Replacement of COMET by UPDATE	5.0.0	5.1.0	
2002-06	NP-16	NP-020231	025	3	Incorporation of current RFC numbers	5.0.0	5.1.0	N1-021091
2002-06	NP-16	NP-020231	026	1	Clarification of B2BUA usage in roles	5.0.0	5.1.0	N1-020941
2002-06	NP-16	NP-020231	028	4	Determination of MO / MT requests in I-CSCF(THIG)	5.0.0	5.1.0	N1-021248
2002-06	NP-16	NP-020231	030	2	P-CSCF release of an existing session	5.0.0	5.1.0	N1-021006
2002-06	NP-16	NP-020232	031	1	S-CSCF release of an existing session	5.0.0	5.1.0	N1-020939
2002-06	NP-16	NP-020232	033	3	SDP procedure at the UE	5.0.0	5.1.0	N1-020971
2002-06	NP-16	NP-020232	035	1	AS Procedures corrections	5.0.0	5.1.0	N1-020934
2002-06	NP-16	NP-020232	036	8	Corrections to SIP Compression	5.0.0	5.1.0	N1-021499
2002-06	NP-16	NP-020232	037	1	Enhancement of S-CSCF and I-CSCF Routing Procedures for interworking with external networks	5.0.0	5.1.0	N1-020928
2002-06	NP-16	NP-020232	041	2	Delivery of IMS security parameters from S-CSCF to the P-CSCF by using proprietary auth-param	5.0.0	5.1.0	N1-021003
2002-06	NP-16	NP-020232	045		Cleanup of request / response terminology - clause 5	5.0.0	5.1.0	N1-020835
2002-06	NP-16	NP-020232	046		Cleanup of request / response terminology - clause 6	5.0.0	5.1.0	N1-020836
2002-06	NP-16	NP-020232	047	2	Simplification of profile tables	5.0.0	5.1.0	N1-021059
2002-06	NP-16	NP-020232	049		Forking options	5.0.0	5.1.0	N1-020839
2002-06	NP-16	NP-020315	050	1	Media-Authorization header corrections	5.0.0	5.1.0	
2002-06	NP-16	NP-020233	051	1	Clause 5.4 editorials (S-CSCF)	5.0.0	5.1.0	N1-020950
2002-06	NP-16	NP-020233	053	2	Integrity protection signalling from the P-CSCF to the S-CSCF	5.0.0	5.1.0	N1-021007
2002-06	NP-16	NP-020233	054		Representing IM CN subsystem functional entities in profile table roles	5.0.0	5.1.0	N1-020847
2002-06	NP-16	NP-020233	055		Clause 4 editorials	5.0.0	5.1.0	N1-020848
2002-06	NP-16	NP-020233	056		Clause 5.8 editorials (MRFC)	5.0.0	5.1.0	N1-020849

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2002-06	NP-16	NP-020233	057	1	Annex A editorials, including precondition additions	5.0.0	5.1.0	N1-021001
2002-06	NP-16	NP-020233	058	2	Representing the registrar as a UA	5.0.0	5.1.0	N1-021054
2002-06	NP-16	NP-020233	059		Additional definitions	5.0.0	5.1.0	N1-020852
2002-06	NP-16	NP-020312	060	11	Restructuring of S-CSCF Registration Sections	5.0.0	5.1.0	
2002-06	NP-16	NP-020234	061	2	Determination of MOC / MTC at P-CSCF and S-CSCF	5.0.0	5.1.0	N1-021060
2002-06	NP-16	NP-020234	062		Correction to the terminating procedures	5.0.0	5.1.0	N1-020927
2002-06	NP-16	NP-020234	063		Loose Routing for Network Initiated Call Release Procedures	5.0.0	5.1.0	N1-020940
2002-06	NP-16	NP-020234	064		Incorporation of previously agreed corrections to clause 5.2.5.2 (N1-020416)	5.0.0	5.1.0	N1-021004
2002-06	NP-16	NP-020234	065		Clause 7.2 editorial corrections	5.0.0	5.1.0	N1-021005
2002-06	NP-16	NP-020234	067	2	S-CSCF routing of MO calls	5.0.0	5.1.0	N1-021097
2002-06	NP-16	NP-020234	068	1	I-CSCF routeing of dialog requests	5.0.0	5.1.0	N1-021078
2002-06	NP-16	NP-020234	069	2	Definition of the Tokanised-by parameter	5.0.0	5.1.0	N1-021096
2002-06	NP-16	NP-020235	070	3	SDP procedures at UE	5.0.0	5.1.0	N1-021453
2002-06	NP-16	NP-020235	073	2	Updates to the procedures involving the iFCs, following the Oulu iFC changes	5.0.0	5.1.0	N1-021440
2002-06	NP-16	NP-020235	074	1	Addition of DHCPv6 references to 24.229	5.0.0	5.1.0	N1-021086
2002-06	NP-16	NP-020235	075	1	Clarification to URL and address assignments	5.0.0	5.1.0	N1-021083
2002-06	NP-16	NP-020235	079	3	Downloading the implicitely registered public user identities from the S-CSCF to P-CSCF	5.0.0	5.1.0	N1-021510
2002-06	NP-16	NP-020235	080	3	Clarification of GPRS aspects	5.0.0	5.1.0	N1-021486
2002-06	NP-16	NP-020235	081	2	Introduction of Subscription Locator Function Interrogation at I-CSCF in 24.229	5.0.0	5.1.0	N1-021469
2002-06	NP-16	NP-020235	082	1	Introduction of Visited_Network_ID p-header	5.0.0	5.1.0	N1-021433
2002-06	NP-16	NP-020236	084	1	MRFC register addresses	5.0.0	5.1.0	N1-021434
2002-06	NP-16	NP-020236	085	1	MRFC INVITE interface editor's notes	5.0.0	5.1.0	N1-021470
2002-06	NP-16	NP-020236	086	1	MRFC OPTIONS interface editor's notes	5.0.0	5.1.0	N1-021471
2002-06	NP-16	NP-020236	087		MRFC PRACK & INFO editor's notes	5.0.0	5.1.0	N1-021159
2002-06	NP-16	NP-020236	088	1	MGCF OPTIONS interface editor's notes	5.0.0	5.1.0	N1-021472
2002-06	NP-16	NP-020236	089		MGCF reINVITE editor's notes	5.0.0	5.1.0	N1-021161
2002-06	NP-16	NP-020237	090		3PCC AS editor's notes	5.0.0	5.1.0	N1-021162
2002-06	NP-16	NP-020237	091		AS acting as terminating UA editor's notes	5.0.0	5.1.0	N1-021163
2002-06	NP-16	NP-020237	092	1	AS acting as originating UA editor's notes	5.0.0	5.1.0	N1-021466
2002-06	NP-16	NP-020237	093	2	Charging overview clause	5.0.0	5.1.0	N1-021512
2002-06	NP-16	NP-020237	094	1	Procedures for original-dialog-id P-header	5.0.0	5.1.0	N1-021456
2002-06	NP-16	NP-020237	095	2	Procedures for charging-vector P-header	5.0.0	5.1.0	N1-021513
2002-06	NP-16	NP-020237	096	1	Procedures for charging-function-addresses P-header	5.0.0	5.1.0	N1-021458
2002-06	NP-16	NP-020237	097	1	SDP types	5.0.0	5.1.0	N1-021467
2002-06	NP-16	NP-020237	100		Removal of State from profile tables	5.0.0	5.1.0	N1-021173

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2002-06	NP-16	NP-020238	101		Editor's note cleanup - clause 3	5.0.0	5.1.0	N1-021174
2002-06	NP-16	NP-020238	102		Editor's note cleanup - clause 4	5.0.0	5.1.0	N1-021175
2002-06	NP-16	NP-020238	103		Editor's note cleanup - clause 5.1 and deletion of void subclauses	5.0.0	5.1.0	N1-021176
2002-06	NP-16	NP-020238	104	1	Editor's note cleanup - clause 5.2 and deletion of void subclauses	5.0.0	5.1.0	N1-021487
2002-06	NP-16	NP-020238	105		Editor's note cleanup - clause 5.3	5.0.0	5.1.0	N1-021178
2002-06	NP-16	NP-020238	106		Editor's note cleanup - clause 5.4 and deletion of void subclauses	5.0.0	5.1.0	N1-021179
2002-06	NP-16	NP-020238	107		Editor's note cleanup - clause 5.5 and deletion of void subclauses	5.0.0	5.1.0	N1-021180
2002-06	NP-16	NP-020238	110		Editor's note cleanup - clause 6	5.0.0	5.1.0	N1-021183
2002-06	NP-16	NP-020238	111		Editor's note cleanup - clause 9	5.0.0	5.1.0	N1-021184
2002-06	NP-16	NP-020239	113	1	SIP Default Timers	5.0.0	5.1.0	N1-021465
2002-06	NP-16	NP-020239	114	1	Correction of the subscription to the registration event package	5.0.0	5.1.0	N1-021436
2002-06	NP-16	NP-020239	115	1	Support for ISIMless UICC	5.0.0	5.1.0	N1-021441
2002-06	NP-16	NP-020239	119	1	SIP procedures at UE	5.0.0	5.1.0	N1-021452
2002-06	NP-16	NP-020239	121	2	New requirements in the P-CSCF	5.0.0	5.1.0	N1-021509
2002-06	NP-16	NP-020239	122		SDP procedures at MGCF	5.0.0	5.1.0	N1-021264
2002-06	NP-16	NP-020239	124	1	S-CSCF allocation	5.0.0	5.1.0	N1-021443
2002-06	NP-16	NP-020240	129	1	Introduction of P-Access-Network-Info header	5.0.0	5.1.0	N1-021498
2002-06	NP-16	NP-020240	130	2	Usage of Path and P-Service Route	5.0.0	5.1.0	N1-021508
2002-06	NP-16	NP-020240	133		Removal of Referred-By header from specification	5.0.0	5.1.0	N1-021354
2002-06	NP-16	NP-020240	134		Handling of Record-Route header in profile tables	5.0.0	5.1.0	N1-021357
2002-06	NP-16	NP-020312	135	1	Asserted identities and privacy	5.0.0	5.1.0	
2002-06	NP-16	NP-020240	136		Removal of caller preferences from specification	5.0.0	5.1.0	N1-021359
2002-06	NP-16	NP-020240	137		Substitution of REFER references	5.0.0	5.1.0	N1-021360
2002-06	NP-16	NP-020240	138		Removal of session timer from specification	5.0.0	5.1.0	N1-021361
2002-09	NP-17	NP-020489	141	2	Adding MESSAGE to 24.229	5.1.0	5.2.0	
2002-09	NP-17	NP-020375	142		Public user identity to use for third party register	5.1.0	5.2.0	N1-021563
2002-09	NP-17	NP-020375	143	1	Replace P-Original-Dialog-ID header with unique data in Route header	5.1.0	5.2.0	N1-021797
2002-09	NP-17	NP-020375	145		Synchronize text with latest I-D for P-headers for charging	5.1.0	5.2.0	N1-021569
2002-09	NP-17	NP-020488	146	2	Service profiles and implicitly registered public user identities	5.1.0	5.2.0	
2002-09	NP-17	NP-020376	147		S-CSCF decides when to include	5.1.0	5.2.0	N1-021571
2002-09	NP-17	NP-020376	148		Clean up XML in clause 7.6	5.1.0	5.2.0	N1-021572
2002-09	NP-17	NP-020376	149		Fix clause 5.2.7.4 header	5.1.0	5.2.0	N1-021573
2002-09	NP-17	NP-020376	150		Removal of forward reference to non P-CSCF procedures	5.1.0	5.2.0	N1-021589
2002-09	NP-17	NP-020376	151		Deregistration of public user identities	5.1.0	5.2.0	N1-021590
2002-09	NP-17	NP-020376	152		Reauthentication trigger via other means	5.1.0	5.2.0	N1-021591
2002-09	NP-17	NP-020487	153	3	Registration with integrity protection	5.1.0	5.2.0	

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2002-09	NP-17	NP-020485	154	2	Explicit listing of need to route response messages	5.1.0	5.2.0	
2002-09	NP-17	NP-020377	157	1	Include IP address in ICID	5.1.0	5.2.0	N1-021816
2002-09	NP-17	NP-020377	158		Reference updates	5.1.0	5.2.0	N1-021604
2002-09	NP-17	NP-020377	159		Abbreviation updates	5.1.0	5.2.0	N1-021605
2002-09	NP-17	NP-020377	163	1	Clarifications of allocation of IP address	5.1.0	5.2.0	N1-021817
2002-09	NP-17	NP-020377	171	1	Verifications at the P-CSCF for subsequent request	5.1.0	5.2.0	N1-021802
2002-09	NP-17	NP-020377	174	1	Clarification of IMS signalling flag	5.1.0	5.2.0	N1-021781
2002-09	NP-17	NP-020377	176	1	Definition of a general-purpose PDP context for IMS	5.1.0	5.2.0	N1-021783
2002-09	NP-17	NP-020372	177	2	Request for DNS IPv6 server address	5.1.0	5.2.0	N1-021833
2002-09	NP-17	NP-020378	178		Error cases for PDP context modification	5.1.0	5.2.0	N1-021679
2002-09	NP-17	NP-020378	183	1	Incorporation of draft-ietf-sip-sec-agree-04.txt	5.1.0	5.2.0	N1-021791
2002-09	NP-17	NP-020378	185	1	User Initiated De-registration	5.1.0	5.2.0	N1-021787
2002-09	NP-17	NP-020378	186	1	Mobile initiated de-registration	5.1.0	5.2.0	N1-021788
2002-09	NP-17	NP-020378	187	1	CallID of REGISTER requests	5.1.0	5.2.0	N1-021786
2002-09	NP-17	NP-020378	188	1	Correction to the I-CSCF routing procedures	5.1.0	5.2.0	N1-021803
2002-09	NP-17	NP-020378	189	1	Registration procedures at P-CSCF	5.1.0	5.2.0	N1-021793
2002-09	NP-17	NP-020378	192	1	Corrections related to the P-Access-Network-Info header	5.1.0	5.2.0	N1-021827
2002-09	NP-17	NP-020378	194	1	Chapter to decribe the registration event	5.1.0	5.2.0	N1-021794
2002-09	NP-17	NP-020484	196		Definition of abbreviation IMS	5.1.0	5.2.0	
2002-12	NP-18	NP-020558	140	4	Support of non-IMS forking	5.2.0	5.3.0	N1-022446
2002-12	NP-18	NP-020565	144	2	Identification of supported IETF drafts within this release	5.2.0	5.3.0	N1-022114
2002-12	NP-18	NP-020558	161	3	Clarifications and editorials to SIP profile	5.2.0	5.3.0	N1-022412
2002-12	NP-18	NP-020558	175	5	Clarifications of the binding and media grouping	5.2.0	5.3.0	N1-022494
2002-12	NP-18	NP-020558	179	2	Support of originating requests from Application Servers	5.2.0	5.3.0	N1-022106
2002-12	NP-18	NP-020558	197		Wrong references in 4.1	5.2.0	5.3.0	N1-021902
2002-12	NP-18	NP-020558	198		Alignment of the MGCF procedures to RFC 3312	5.2.0	5.3.0	N1-021903
2002-12	NP-18	NP-020558	199	1	Service Route Header and Path Header interactions	5.2.0	5.3.0	N1-022080
2002-12	NP-18	NP-020558	202		Addition of clause 6 though clause 9 references to conformance clause	5.2.0	5.3.0	N1-021919
2002-12	NP-18	NP-020558	203	1	URL and address assignments	5.2.0	5.3.0	N1-022115
2002-12	NP-18	NP-020559	204	3	Fix gprs-charging-info definition and descriptions	5.2.0	5.3.0	N1-022426
2002-12	NP-18	NP-020559	206		Alignment of the SDP attributes related to QoS integration with IETF	5.2.0	5.3.0	N1-021930
2002-12	NP-18	NP-020559	207	1	Update of the 3GPP-generated SIP P-headers document references	5.2.0	5.3.0	N1-022116

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2002-12	NP-18	NP-020559	208	1	Handling of INVITE requests that do not contain SDP	5.2.0	5.3.0	N1-022098
2002-12	NP-18	NP-020559	209	2	UE Registration	5.2.0	5.3.0	N1-022471
2002-12	NP-18	NP-020559	211	1	Usage of private user identity during registration	5.2.0	5.3.0	N1-022083
2002-12	NP-18	NP-020559	212	1	P-CSCF subscription to the users registration-state event	5.2.0	5.3.0	N1-022084
2002-12	NP-18	NP-020559	213	2	Handling of MT call by the P-CSCF	5.2.0	5.3.0	N1-022154
2002-12	NP-18	NP-020559	215		P-CSCF acting as a UA	5.2.0	5.3.0	N1-021939
2002-12	NP-18	NP-020559	216	1	S-CSCF handling of protected registrations	5.2.0	5.3.0	N1-022085
2002-12	NP-18	NP-020560	217	1	S-CSCF handling of subscription to the users registration-state event	5.2.0	5.3.0	N1-022086
2002-12	NP-18	NP-020560	218	1	Determination of MO or MT in I-CSCF	5.2.0	5.3.0	N1-022102
2002-12	NP-18	NP-020560	220		Definition of the NAI and RTCP abbreviations	5.2.0	5.3.0	N1-021944
2002-12	NP-18	NP-020560	222	4	Go related error codes in the UE	5.2.0	5.3.0	N1-022495
2002-12	NP-18	NP-020560	223	1	Clarifications on CCF/ECF addresses	5.2.0	5.3.0	N1-022120
2002-12	NP-18	NP-020560	225	2	Clarifications on dedicated PDP Context for IMS signalling	5.2.0	5.3.0	N1-022156
2002-12	NP-18	NP-020560	228	3	Clarifications on the use of charging correlation information	5.2.0	5.3.0	N1-022425
2002-12	NP-18	NP-020560	232	1	Expires information in REGISTER response	5.2.0	5.3.0	N1-022095
2002-12	NP-18	NP-020560	235	2	Indication of successful establishment of Dedicated Signalling PDP context to the UE	5.2.0	5.3.0	N1-022129
2002-12	NP-18	NP-020560	237		P-CSCF sending 100 (Trying) Response for reINVITE	5.2.0	5.3.0	N1-021998
2002-12	NP-18	NP-020561	239	1	Correction on P-Asserted-Id, P-Preferred-Id, Remote-Party-ID	5.2.0	5.3.0	N1-022100
2002-12	NP-18	NP-020561	240	1	Clarifications to subclause 9.2.5	5.2.0	5.3.0	N1-022137
2002-12	NP-18	NP-020561	242		ENUM translation	5.2.0	5.3.0	N1-022020
2002-12	NP-18	NP-020561	243	1	AS routing	5.2.0	5.3.0	N1-022107
2002-12	NP-18	NP-020561	245	1	Warning header	5.2.0	5.3.0	N1-022108
2002-12	NP-18	NP-020561	246	3	S-CSCF procedure tidyup	5.2.0	5.3.0	N1-022497
2002-12	NP-18	NP-020561	247	1	P-CSCF procedure tidyup	5.2.0	5.3.0	N1-022125
2002-12	NP-18	NP-020561	248	2	UE procedure tidyup	5.2.0	5.3.0	N1-022472
2002-12	NP-18	NP-020561	249	3	MESSAGE corrections part 1	5.2.0	5.3.0	N1-022455
2002-12	NP-18	NP-020561	250	2	MESSAGE corrections part 2	5.2.0	5.3.0	N1-022456
2002-12	NP-18	NP-020562	251	2	Security association clarifications	5.2.0	5.3.0	N1-022440
2002-12	NP-18	NP-020562	252	1	The use of security association by the UE	5.2.0	5.3.0	N1-022433
2002-12	NP-18	NP-020562	253	1	UE integrity protected re-registration	5.2.0	5.3.0	N1-022434

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2002-12	NP-18	NP-020562	255	3	Handling of default public user identities by the P-CSCF	5.2.0	5.3.0	N1-022496
2002-12	NP-18	NP-020562	263		Fixing ioi descriptions	5.2.0	5.3.0	N1-022266
2002-12	NP-18	NP-020562	264	1	Fix descriptions for ECF/CCF addresses	5.2.0	5.3.0	N1-022447
2002-12	NP-18	NP-020562	266	2	Alignment with draft-ietf-sipping-reg-event-00 and clarification on network initiated deregistration	5.2.0	5.3.0	N1-022493
2002-12	NP-18	NP-020563	267	1	Correction to network initiated re-authentication procedure	5.2.0	5.3.0	N1-022449
2002-12	NP-18	NP-020563	268	1	Registration Expires Timer Default Setting	5.2.0	5.3.0	N1-022439
2002-12	NP-18	NP-020563	269	1	Clarification on Sh interface for charging purposes	5.2.0	5.3.0	N1-022465
2002-12	NP-18	NP-020563	270	2	Clarifications on the scope	5.2.0	5.3.0	N1-022500
2002-12	NP-18	NP-020563	273	1	Add charging info for SUBSCRIBE	5.2.0	5.3.0	N1-022467
2002-12	NP-18	NP-020563	274	1	Profile revisions for RFC 3261 headers	5.2.0	5.3.0	N1-022413
2002-12	NP-18	NP-020563	275		Consistency changes for SDP procedures at MGCF	5.2.0	5.3.0	N1-022345
2002-12	NP-18	NP-020563	276		Proxy support of PRACK	5.2.0	5.3.0	N1-022350
2002-12	NP-18	NP-020563	277		Clarification of transparent handling of parameters in profile	5.2.0	5.3.0	N1-022351
2002-12	NP-18	NP-020564	279	1	Meaning of refresh request	5.2.0	5.3.0	N1-022444
2002-12	NP-18	NP-020564	280		Removal of Caller Preferences dependency	5.2.0	5.3.0	N1-022362
2002-12	NP-18	NP-020564	281	1	P-Access-Network-Info clarifications	5.2.0	5.3.0	N1-022445
2002-12	NP-18	NP-020564	282		Clarification on use of the From header by the UE	5.2.0	5.3.0	N1-022370
2002-12	NP-18	NP-020634	283	2	Support of comp=sigcomp parameter	5.2.0	5.3.0	
2002-12	NP-18	NP-020668	284	4	SDP media policy rejection	5.2.0	5.3.0	
2002-12	NP-18	NP-020567	285	1	Fallback for compression failure	5.2.0	5.3.0	N1-022481
2002-12	NP-18	NP-020564	287	1	SA related procedures	5.2.0	5.3.0	N1-022459
2002-12	NP-18	NP-020568	290	1	Emergency Service correction	5.2.0	5.3.0	N1-022461
2002-12	NP-18	NP-020663	278	4	P-CSCF does not strip away headers	5.2.0	5.3.0	N1-022499
2002-12	NP-18	NP-020557	289		PCF to PDF	5.2.0	5.3.0	N1-022387
2003-03	NP-19	NP-030049	291		Minor correction and consistency changes to general part of profile	5.3.0	5.4.0	N1-030012
2003-03	NP-19	NP-030049	292		SIP profile minor correction and consistency changes	5.3.0	5.4.0	N1-030013
2003-03	NP-19	NP-030049	293	1	Network asserted identity procedure corrections for the UE	5.3.0	5.4.0	N1-030261
2003-03	NP-19	NP-030049	294	1	Asserted identity inclusion in SIP profile	5.3.0	5.4.0	N1-030300
2003-03	NP-19	NP-030049	296		Profile references relating to registration	5.3.0	5.4.0	N1-030023
2003-03	NP-19	NP-030049	297	2	Reference corrections	5.3.0	5.4.0	N1-030301

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2003-03	NP-19	NP-030050	300	1	488 message with a subset of allowed media parameters	5.3.0	5.4.0	N1-030245
2003-03	NP-19	NP-030050	301	1	Handling of Emergency Numbers in P-CSCF	5.3.0	5.4.0	N1-030239
2003-03	NP-19	NP-030050	302	2	Correction of the registration state event package	5.3.0	5.4.0	N1-030268
2003-03	NP-19	NP-030050	305	2	User initiated de-registration at P-CSCF	5.3.0	5.4.0	N1-030295
2003-03	NP-19	NP-030050	306	2	Network-initiated deregistration at UE, P-CSCF, and S-CSCF	5.3.0	5.4.0	N1-030296
2003-03	NP-19	NP-030050	307	2	UE deregistration during established dialogs	5.3.0	5.4.0	N1-030297
2003-03	NP-19	NP-030050	308	2	S-CSCF handling of deregistration during established dialogs	5.3.0	5.4.0	N1-030298
2003-03	NP-19	NP-030050	309	1	S-CSCF handling of established dialogs upon deregistration	5.3.0	5.4.0	N1-030233
2003-03	NP-19	NP-030050	310	2	S-CSCF handling of established dialogs upon registration-lifetime expiration	5.3.0	5.4.0	N1-030299
2003-03	NP-19	NP-030051	311	1	P-CSCF handling of established dialogs upon registration-lifetime expiration	5.3.0	5.4.0	N1-030235
2003-03	NP-19	NP-030051	312	1	Correction of Authentication procedure	5.3.0	5.4.0	N1-030240
2003-03	NP-19	NP-030051	313		Mixed Path header and Service-Route operation	5.3.0	5.4.0	N1-030127
2003-03	NP-19	NP-030051	315	2	Clarifications on updating the authorization token	5.3.0	5.4.0	N1-030255
2003-03	NP-19	NP-030051	318	2	Consideration of P-CSCF/PDF	5.3.0	5.4.0	N1-030307
2003-03	NP-19	NP-030051	319	2	Clarification on GPRS charging information	5.3.0	5.4.0	N1-030308
2003-03	NP-19	NP-030051	323	1	P-Access-Network-Info procedure corrections for the UE	5.3.0	5.4.0	N1-030250
2003-03	NP-19	NP-030051	324	1	P-Access-Network-Info procedure corrections for the S-CSCF	5.3.0	5.4.0	N1-030251
2003-03	NP-19	NP-030051	326	1	Updating user agent related profile tables	5.3.0	5.4.0	N1-030260
2003-03	NP-19	NP-030052	327	2	Cleanup and clarification to the registration and authentication procedure	5.3.0	5.4.0	N1-030282
2003-03	NP-19	NP-030052	328	1	Corrections to the reg event package	5.3.0	5.4.0	N1-030230
2003-03	NP-19	NP-030052	330	2	Clarifications for setting up separate PDP contexts in case of SBLP	5.3.0	5.4.0	N1-030288
2003-03	NP-19	NP-030052	331	2	Handling of the P-Media-Autohorization header	5.3.0	5.4.0	N1-030289
2003-03	NP-19	NP-030052	333	3	Removal of P-Asserted-Identity from clause 7 of 24.229	5.3.0	5.4.0	N1-030310
2003-03	NP-19	NP-030052	334		P-CSCF general procedure corrections	5.3.0	5.4.0	N1-030182
2003-03	NP-19	NP-030052	335	2	Usage of Contact in UE's registration procedure	5.3.0	5.4.0	N1-030281
2003-03	NP-19	NP-030052	337		Usage of P-Asserted-Identity for responses	5.3.0	5.4.0	N1-030193
2003-03	NP-19	NP-030052	339	2	Authorization for registration event	5.3.0	5.4.0	N1-030285

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					package			

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2003-03	NP-19	NP-030052	341	1	P-CSCF subscription to reg event	5.3.0	5.4.0	N1-030284
2003-06	NP-20	NP-030275	295	4	Security agreement inclusion in SIP profile	5.4.0	5.5.0	N1-030939
2003-06	NP-20	NP-030275	322	5	3GPP P-header inclusion in SIP profile	5.4.0	5.5.0	N1-030938
2003-06	NP-20	NP-030275	332	5	Change of IP address for the UE	5.4.0	5.5.0	N1-030923
2003-06	NP-20	NP-030275	342		Removal of the requirement for UE re-authentication initiated by HSS	5.4.0	5.5.0	N1-030349
2003-06	NP-20	NP-030275	343	2	UE behaviour on reception of 420 (Bad Extension) message	5.4.0	5.5.0	N1-030552
2003-06	NP-20	NP-030275	347	2	Handling of DTMF	5.4.0	5.5.0	N1-030551
2003-06	NP-20	NP-030276	348	1	Format of Tel URL in P-Asserted-Id	5.4.0	5.5.0	N1-030510
2003-06	NP-20	NP-030276	349		Delete Note on header stripping/SDP manipulation	5.4.0	5.5.0	N1-030387
2003-06	NP-20	NP-030276	354	1	Clarifications on using DNS procedures	5.4.0	5.5.0	N1-030520
2003-06	NP-20	NP-030276	356	4	Addition of procedures at the AS for SDP	5.4.0	5.5.0	N1-030942
2003-06	NP-20	NP-030276	357	1	Usage of P-Associated-URI	5.4.0	5.5.0	N1-030499
2003-06	NP-20	NP-030276	359	1	Network-initiated deregistration at UE and P-CSCF	5.4.0	5.5.0	N1-030501
2003-06	NP-20	NP-030276	360	2	Barred identities	5.4.0	5.5.0	N1-030550
2003-06	NP-20	NP-030276	365	1	PDP contex subject to SBLP cannot be reused by other IMS sessions	5.4.0	5.5.0	N1-030513
2003-06	NP-20	NP-030276	368	1	User authentication failure cleanups	5.4.0	5.5.0	N1-030506
2003-06	NP-20	NP-030277	369	3	S-CSCF behavior correction to enable call forwarding	5.4.0	5.5.0	N1-030931
2003-06	NP-20	NP-030277	370	1	SUBSCRIBE request information stored at the P-CSCF and S-CSCF	5.4.0	5.5.0	N1-030521
2003-06	NP-20	NP-030277	371	1	Profile Tables - Transparency	5.4.0	5.5.0	N1-030858
2003-06	NP-20	NP-030277	375	1	Profile Tables - Major Capability Corrections	5.4.0	5.5.0	N1-030860
2003-06	NP-20	NP-030277	376	2	Profile Tables - Deletion of Elements not used in 24.229	5.4.0	5.5.0	N1-030921
2003-06	NP-20	NP-030277	377	1	Use of the QoS parameter 'signalling information' for a signalling PDP context	5.4.0	5.5.0	N1-030840
2003-06	NP-20	NP-030277	378	2	Deregistration of a PUID (not the last one)	5.4.0	5.5.0	N1-030919
2003-06	NP-20	NP-030277	379	2	'Last registered public user identity' terminology change	5.4.0	5.5.0	N1-030920
2003-06	NP-20	NP-030277	380	1	Check Integrity Protection for P-Access-Network-Info header	5.4.0	5.5.0	N1-030881
2003-06	NP-20	NP-030278	381	1	PCSCF setting of Integrity protection indicator and checking of Security Verify header	5.4.0	5.5.0	N1-030882
2003-06	NP-20	NP-030278	383	1	Consistent treatment of register and de-register	5.4.0	5.5.0	N1-030884
2003-06	NP-20	NP-030278	384	1	Optionality of sending CK is removed	5.4.0	5.5.0	N1-030885
2003-06	NP-20	NP-030278	385	1	Addition of note and Correction of References regarding security	5.4.0	5.5.0	N1-030886

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					associations and registration			

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2003-06	NP-20	NP-030278	387	1	Subscription/Registration refresh time	5.4.0	5.5.0	N1-030887
2003-06	NP-20	NP-030278	388	1	Corrections to use of IK	5.4.0	5.5.0	N1-030863
2003-06	NP-20	NP-030278	390		Mobile-originating case at UE	5.4.0	5.5.0	N1-030647
2003-06	NP-20	NP-030278	394	2	Re-authentication procedure.	5.4.0	5.5.0	N1-030917
2003-06	NP-20	NP-030278	395		Replacement of SIP URL with SIP URI	5.4.0	5.5.0	N1-030652
2003-06	NP-20	NP-030279	397	2	Notification about registration state	5.4.0	5.5.0	N1-030926
2003-06	NP-20	NP-030279	402	1	Handling of P-Asserted ID in MGCF	5.4.0	5.5.0	N1-030848
2003-06	NP-20	NP-030279	404	1	S-CSCF initiated release of calls to circiut switched network	5.4.0	5.5.0	N1-030873
2003-06	NP-20	NP-030279	405	2	Supported Integrity algorithms	5.4.0	5.5.0	N1-030927
2003-06	NP-20	NP-030279	407	1	RFC 3524, Single Reservation Flows	5.4.0	5.5.0	N1-030851
2003-06	NP-20	NP-030279	410	1	Clarification of the S-CSCF's handling of the P-access-network-info header	5.4.0	5.5.0	N1-030868
2003-06	NP-20	NP-030279	411	2	Port numbers in the RR header entries	5.4.0	5.5.0	N1-030941
2003-06	NP-20	NP-030279	412	2	Registration abnormal cases	5.4.0	5.5.0	N1-030928
2003-06	NP-20	NP-030280	415		Minor correction to section 5.4.5.1.2	5.4.0	5.5.0	N1-030720
2003-06	NP-20	NP-030280	417	1	Introduction of RTCP bandwidth	5.4.0	5.5.0	N1-030872
2003-06	NP-20	NP-030280	418	1	Registratin Event - Shortend	5.4.0	5.5.0	N1-030844
2003-06	NP-20	NP-030280	419	1	HSS / S-CSCF text relating to user deregistration	5.4.0	5.5.0	N1-030845
2003-06	NP-20	NP-030280	421		Handling of unknown methods at the P-CSCF	5.4.0	5.5.0	N1-030743
2003-06	NP-20	NP-030280	422	1	Definitions and abbreviations update	5.4.0	5.5.0	N1-030870
2003-06	NP-20	NP-030280	423		Removal of hanging paragraph	5.4.0	5.5.0	N1-030752
2003-06	NP-20	NP-030280	424		Access network charging information	5.4.0	5.5.0	N1-030753
2003-06	NP-20	NP-030280	425	1	UE procedure tidyup	5.4.0	5.5.0	N1-030871
2003-06	NP-20	NP-030281	426		P-CSCF procedure tidyup	5.4.0	5.5.0	N1-030755
2003-06	NP-20	NP-030281	427		I-CSCF procedure tidyup	5.4.0	5.5.0	N1-030756
2003-06	NP-20	NP-030281	428		S-CSCF procedure tidyup	5.4.0	5.5.0	N1-030757
2003-06	NP-20	NP-030281	429		BGCF procedure tidyup	5.4.0	5.5.0	N1-030758
2003-06	NP-20	NP-030281	430		AS procedure tidyup	5.4.0	5.5.0	N1-030759
2003-06	NP-20	NP-030281	431		MRFC procedure tidyup	5.4.0	5.5.0	N1-030760
2003-06	NP-20	NP-030281	434	1	SDP procedure tidyup	5.4.0	5.5.0	N1-030852
2003-06	NP-20	NP-030281	438	2	Profile Tables – Further Corrections	5.4.0	5.5.0	N1-030935
2003-06	NP-20	NP-030281	439	3	AS's subscription for the registration state event package	5.4.0	5.5.0	N1-030940
2003-06	NP-20	NP-030281	440		Temporary Public User Identity in re- and de-REGISTER requests	5.4.0	5.5.0	N1-030792
2003-09	NP-21	NP-030412	444	2	All non-REGISTER requests must be integrity protected	5.5.0	5.6.0	N1-031328

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2003-09	NP-21	NP-030412	445		Download of all service profiles linked to PUID being registered and implicitly registered	5.5.0	5.6.0	N1-031010
2003-09	NP-21	NP-030412	448	3	Authentication at UE	5.5.0	5.6.0	N1-031326
2003-09	NP-21	NP-030412	449	1	Nework authentication failure at the UE	5.5.0	5.6.0	N1-031242
2003-09	NP-21	NP-030412	451	3	Handling of security association	5.5.0	5.6.0	N1-031327
2003-09	NP-21	NP-030412	452	1	Re-authentication timer at S-CSCF	5.5.0	5.6.0	N1-031274
2003-09	NP-21	NP-030412	455	2	Authentication failure at S-CSCF	5.5.0	5.6.0	N1-031285
2003-09	NP-21	NP-030413	456	2	Subscription termination sent by the S-CSCF	5.5.0	5.6.0	N1-031276
2003-09	NP-21	NP-030413	457		Subscription termination at the P-CSCF	5.5.0	5.6.0	N1-031032
2003-09	NP-21	NP-030413	458		Network -initiated deregistration at P-CSCF	5.5.0	5.6.0	N1-031033
2003-09	NP-21	NP-030349	459	2	Notification about registration status at AS	5.5.0	5.6.0	
2003-09	NP-21	NP-030413	461	1	Service profile	5.5.0	5.6.0	N1-031233
2003-09	NP-21	NP-030413	466	1	Requirements on Preconditions	5.5.0	5.6.0	N1-031246
2003-09	NP-21	NP-030413	467	1	Call forwarding cleanup	5.5.0	5.6.0	N1-031238
2003-09	NP-21	NP-030413	468		Update of references	5.5.0	5.6.0	N1-031094
2003-09	NP-21	NP-030414	470	1	Adding P-Asserted-Identity headers to NE initiated subscriptions	5.5.0	5.6.0	N1-031314
2003-09	NP-21	NP-030414	479	1	Replace USIM by ISIM for user identity storage	5.5.0	5.6.0	N1-031247
2003-09	NP-21	NP-030414	481	1	24.229 R5 CR: Corrections to Profile Tables	5.5.0	5.6.0	N1-031248
2003-09	NP-21	NP-030414	482		24.229 R5 CR: Setting of SUBSCRIBE exipiration time	5.5.0	5.6.0	N1-031140
2003-09	NP-21	NP-030414	483	3	24.229 R5 CR: Alignment of IMS Compression with RFC 3486	5.5.0	5.6.0	N1-031335
2003-09	NP-21	NP-030418	465	1	Alignment with TS for policy control over Gq interface	5.6.0	6.0.0	N1-031267
2003-09	NP-21	NP-030418	472	1	I-CSCF procedures for openness	5.6.0	6.0.0	N1-031304
2003-09	NP-21	NP-030433	473	3	Registration from multiple terminals and forking	5.6.0	6.0.0	
2003-09	NP-21	NP-030419	480	3	Access Independent IMS	5.6.0	6.0.0	N1-031333
2003-12	NP-22	NP-030482	487	1	Registration amendments in profile	6.0.0	6.1.0	N1-031627
2003-12	NP-22	NP-030482	489		Privacy considerations for the UE	6.0.0	6.1.0	N1-031351
2003-12	NP-22	NP-030476	493		INVITE dialog amendments in profile	6.0.0	6.1.0	N1-031359
2003-12	NP-22	NP-030482	494		Correction of I-CSCF handling of multiple private user identities with same public user identity	6.0.0	6.1.0	N1-031375
2003-12	NP-22	NP-030476	496	1	P-Asserted-Identity in SUBSCRIBE requests	6.0.0	6.1.0	N1-031632
2003-12	NP-22	NP-030482	497		Addition of reference to Gq interface	6.0.0	6.1.0	N1-031378

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2003-12	NP-22	NP-030476	503	2	Update of HSS information at deregistration	6.0.0	6.1.0	N1-031720
2003-12	NP-22	NP-030482	507		Unavailable definitions	6.0.0	6.1.0	N1-031392
2003-12	NP-22	NP-030476	509		Reference corrections	6.0.0	6.1.0	N1-031394
2003-12	NP-22	NP-030484	510	1	UICC related changes for IMS commonality and interoperability	6.0.0	6.1.0	N1-031682
2003-12	NP-22	NP-030484	511		Interoperability and commonality; definition of scope	6.0.0	6.1.0	N1-031427
2003-12	NP-22	NP-030484	512		Interoperability and commonality; addition of terminology	6.0.0	6.1.0	N1-031428
2003-12	NP-22	NP-030484	513		Interoperability and commonality; media grouping	6.0.0	6.1.0	N1-031429
2003-12	NP-22	NP-030484	515		Interoperability and commonality; charging information	6.0.0	6.1.0	N1-031431
2003-12	NP-22	NP-030482	518	1	Profile support of RFC 3326: The Reason Header Field for the Session Initiation Protocol	6.0.0	6.1.0	N1-031681
2003-12	NP-22	NP-030482	519		Profile support of RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing	6.0.0	6.1.0	N1-031439
2003-12	NP-22	NP-030484	522	1	Clause 9 restructuring	6.0.0	6.1.0	N1-031684
2003-12	NP-22	NP-030477	524	2	Correct use of RAND during re-synchronisation failures	6.0.0	6.1.0	N1-031712
2003-12	NP-22	NP-030478	526	1	Correction to description or RES/XRES usage	6.0.0	6.1.0	N1-031617
2003-12	NP-22	NP-030483	529		Corrections on charging specification number	6.0.0	6.1.0	N1-031469
2003-12	NP-22	NP-030581	531	3	Corrections on ICID for REGISTER	6.0.0	6.1.0	
2003-12	NP-22	NP-030478	543	1	Correction of user initiated re-registration	6.0.0	6.1.0	N1-031619
2003-12	NP-22	NP-030483	551	1	IMS trust domain in Rel 6	6.0.0	6.1.0	N1-031622
2003-12	NP-22	NP-030478	556	1	P-CSCF and UE handling of Security Associations	6.0.0	6.1.0	N1-031624
2003-12	NP-22	NP-030483	560	2	SDP offer handling in SIP responses in S-CSCF and P-CSCF	6.0.0	6.1.0	N1-031727
2003-12	NP-22	NP-030483	564	1	SIP compression	6.0.0	6.1.0	N1-031705
2003-12	NP-22	NP-030478	566		Sending challenge	6.0.0	6.1.0	N1-031580
2003-12	NP-22	NP-030480	568	2	Reg-await-auth timer value	6.0.0	6.1.0	N1-031716
2003-12	NP-22	NP-030480	571	1	Network initiated deregistration	6.0.0	6.1.0	N1-031707
2003-12	NP-22	NP-030483	572		Text harmonisation with 3GPP2	6.0.0	6.1.0	N1-031589
2003-12	NP-22	NP-030483	573	1	Procedures in the absence of UICC	6.0.0	6.1.0	N1-031680
2003-12	NP-22	NP-030483	575	1	P-Access-Network-Info changes	6.0.0	6.1.0	N1-031683
2004-03	NP-23	NP-040027	488	3	Completion of major capabilities table in respect of privacy	6.1.0	6.2.0	N1-040406
2004-03	NP-23	NP-040027	499	5	P-CSCF integrity protection	6.1.0	6.2.0	N1-040500

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2004-03	NP-23	NP-040032	578	1	UE requesting no-fork	6.1.0	6.2.0	N1-040184
2004-03	NP-23	NP-040032	579	1	Inclusion of caller preferences into profile	6.1.0	6.2.0	N1-040284
2004-03	NP-23	NP-040027	586	1	Network-initiated re-authentication	6.1.0	6.2.0	N1-040391
2004-03	NP-23	NP-040032	588	1	Re-authentication - Abnormal cases	6.1.0	6.2.0	N1-040393
2004-03	NP-23	NP-040027	592	1	Integrity protected correction	6.1.0	6.2.0	N1-040398
2004-03	NP-23	NP-040032	596	1	Sec-agree parameter in "Proxy-Require" header	6.1.0	6.2.0	N1-040400
2004-03	NP-23	NP-040027	600	2	Handling of record-route in target refresh and subsequent request	6.1.0	6.2.0	N1-040481
2004-03	NP-23	NP-040035	603		Cleanup for IP-CAN and GPRS	6.1.0	6.2.0	N1-040304
2004-03	NP-23	NP-040032	604		Forking in S-CSCF	6.1.0	6.2.0	N1-040325
2004-03	NP-23	NP-040108	605	3	Determination of S-CSCF role	6.1.0	6.2.0	
2004-03	NP-23	NP-040134	608	3	Unprotected deregistration	6.1.0	6.2.0	
2004-03	NP-23	NP-040029	610		Sending authentication challenge	6.1.0	6.2.0	N1-040331
2004-03	NP-23	NP-040033	613		Reference to PDF operation	6.1.0	6.2.0	N1-040334
2004-03	NP-23	NP-040029	615	1	Support of MESSAGE (Profile Tables)	6.1.0	6.2.0	N1-040466
2004-03	NP-23	NP-040033	616	2	Introduction of PSI Routing to 24.229	6.1.0	6.2.0	N1-040487
2004-03	NP-23	NP-040033	617	1	P-CSCF Re-selection	6.1.0	6.2.0	N1-040463
2004-03	NP-23	NP-040033	618		I-CSCF does not re-select S-CSCF during re-registration	6.1.0	6.2.0	N1-040344
2004-03	NP-23	NP-040033	620	1	Handling of media authorization token due to messaging	6.1.0	6.2.0	N1-040430
2004-06	NP-24	NP-040191	621	2	Forking requests terminating at the served user	6.2.0	6.3.0	N1-040739
2004-06	NP-24	NP-040191	624	1	Abbreviations	6.2.0	6.3.0	N1-040691
2004-06	NP-24	NP-040191	625	5	Removal of restriction for multiple SIP sessions on a single PDP context	6.2.0	6.3.0	N1-041053
2004-06	NP-24	NP-040191	626	3	Record route in S-CSCF	6.2.0	6.3.0	N1-041061
2004-06	NP-24	NP-040189	627	3	Correction of reception of media authorization token	6.2.0	6.3.0	N1-040994
2004-06	NP-24	NP-040191	628	3	Introduction of PSI Routing to 24.229	6.2.0	6.3.0	N1-041059
2004-06	NP-24	NP-040198	629	2	Addition of PRESNC material	6.2.0	6.3.0	N1-040996

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2004-06	NP-24	NP-040189	631	1	Missing statements regarding P-Charging-Function-Addresses header	6.2.0	6.3.0	N1-040987
2004-06	NP-24	NP-040191	634	1	Multiple registrations	6.2.0	6.3.0	N1-041054
2004-06	NP-24	NP-040192	635	1	Network-initiated deregistration	6.2.0	6.3.0	N1-041055
2004-06	NP-24	NP-040192	636		Network-initiated re-authentication	6.2.0	6.3.0	N1-040778
2004-06	NP-24	NP-040192	637	1	Mobile-initiated deregistration	6.2.0	6.3.0	N1-041056
2004-06	NP-24	NP-040192	638	1	Notification about registration state	6.2.0	6.3.0	N1-041057
2004-06	NP-24	NP-040189	642	3	Syntax of the extension to the P-Charging-Vector header field	6.2.0	6.3.0	N1-041100
2004-06	NP-24	NP-040192	643	2	Session Timer	6.2.0	6.3.0	N1-041095
2004-06	NP-24	NP-040193	644	3	Session initiation without preconditions	6.2.0	6.3.0	N1-041096
2004-06	NP-24	NP-040192	645	1	IMS Conferencing: Inclusion of Profile Tables to TS 24.229	6.2.0	6.3.0	N1-041015
2004-06	NP-24	NP-040189	649	1	Revisions due to published version of draft-ietf-sipping-reg-event	6.2.0	6.3.0	N1-040992
2004-06	NP-24	NP-040198	652		Creation of separate event package table for UA role	6.2.0	6.3.0	N1-041066
2004-09	NP-25	NP-040380	658		Correction of User identity verification at the AS	6.3.0	6.4.0	N1-041344
2004-09	NP-25	NP-040381	666	1	NOTIFY requests	6.3.0	6.4.0	N1-041586
2004-09	NP-25	NP-040381	654	4	Callee capabilities and Registration	6.3.0	6.4.0	N1-041315
2004-09	NP-25	NP-040381	668	2	Network deregistration	6.3.0	6.4.0	N1-041614
2004-09	NP-25	NP-040381	682	1	SDP parameters received by the S-CSCF and the P-CSCF in the 200 OK message	6.3.0	6.4.0	N1-041592
2004-09	NP-25	NP-040381	661	1	Call Release	6.3.0	6.4.0	N1-041589
2004-09	NP-25	NP-040381	659		Multiple public ID registration	6.3.0	6.4.0	N1-041350
2004-09	NP-25	NP-040381	660		Standalone transactions	6.3.0	6.4.0	N1-041351
2004-09	NP-25	NP-040381	663		Unprotected REGISTER	6.3.0	6.4.0	N1-041354
2004-09	NP-25	NP-040381	662	1	Session timer	6.3.0	6.4.0	N1-041590
2004-09	NP-25	NP-040381	665		Contact in SUBSCRIBE request	6.3.0	6.4.0	N1-041372
2004-09	NP-25	NP-040381	650	2	Support of draft-ietf-sip-replaces	6.3.0	6.4.0	N1-041391
2004-09	NP-25	NP-040381	657	1	Support of draft-ietf-sip-join	6.3.0	6.4.0	N1-041393
2004-09	NP-25	NP-040381	656	1	Support of draft-ietf-sip-referredby	6.3.0	6.4.0	N1-041263
2004-09	NP-25	NP-040381	678		Support of TLS	6.3.0	6.4.0	N1-041462
2004-09	NP-25	NP-040381	688	2	Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules	6.3.0	6.4.0	N1-041641
2004-09	NP-25	NP-040382	692	2	Ipv6 IPv4 interworking	6.3.0	6.4.0	N1-041630
2004-09	NP-25	NP-040383	689	2	Addition of session set-up not requiring preconditions and reliable transport of provisional responses.	6.3.0	6.4.0	N1-041632
2004-09	NP-25	NP-040385	697		Missing value for the event attribute within the <contact> element of NOTIFY body	6.3.0	6.4.0	N1-041540

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2004-09	NP-25	NP-040385	698		HSS initiated deregistration	6.3.0	6.4.0	N1-041549
2004-09	NP-25	NP-040385	673		Syntax correction for the P-Charging-Vector header	6.3.0	6.4.0	N1-041434
2004-09	NP-25	NP-040385	699	1	Network initiated deregistration upon UE roaming and registration to a new network	6.3.0	6.4.0	N1-041629
2004-12	NP-26	NP-040506	651	4	Downloading the user profile based on User-Data-Request-Type	6.4.0	6.5.0	N1-042031
2004-12	NP-26	NP-040506	703	2	SDP Encryption	6.4.0	6.5.0	N1-042095
2004-12	NP-26	NP-040506	704	1	RTCP streams	6.4.0	6.5.0	N1-042019
2004-12	NP-26	NP-040506	709		Contact in 200(OK) response	6.4.0	6.5.0	N1-041725
2004-12	NP-26	NP-040506	710	1	P-Access-Network-Info header	6.4.0	6.5.0	N1-042020
2004-12	NP-26	NP-040506	711	1	P-Called-Party-ID header	6.4.0	6.5.0	N1-041954
2004-12	NP-26	NP-040506	713	1	IMS-ALG routing	6.4.0	6.5.0	N1-042021
2004-12	NP-26	NP-040506	714	1	Public User Identity	6.4.0	6.5.0	N1-042022
2004-12	NP-26	NP-040506	715	1	"Pres" and "im" URIs	6.4.0	6.5.0	N1-042023
2004-12	NP-26	NP-040502	723	1	Correction Term IOI handling	6.4.0	6.5.0	N1-041956
2004-12	NP-26	NP-040502	725	1	Request handling in S-CSCF originating case	6.4.0	6.5.0	N1-041958
2004-12	NP-26	NP-040502	727	1	Request handling in S-CSCF - terminating case	6.4.0	6.5.0	N1-041960
2004-12	NP-26	NP-040506	728		SBLP and non-realtime PDP contexts	6.4.0	6.5.0	N1-041797
2004-12	NP-26	NP-040590	730	2	Reference updates	6.4.0	6.5.0	N1-042085
2004-12	NP-26	NP-040590	733	3	Support for extended SigComp	6.4.0	6.5.0	N1-042117
2004-12	NP-26	NP-040590	734	2	Correction to subclause 5.1.3 of TS 24,229	6.4.0	6.5.0	N1-042120
2004-12	NP-26	NP-040590	735	1	Correction to subclause 5.1.4.1.2.3 of TS 24,.229	6.4.0	6.5.0	N1-042084
2004-12	NP-26	NP-040502	738	1	Population of Via header when using REGISTER method	6.4.0	6.5.0	N1-041962
2004-12	NP-26	NP-040590	739		Tel-URI related reference updates	6.4.0	6.5.0	N1-041869
2004-12	NP-26	NP-040590	741	1	Throttling	6.4.0	6.5.0	N1-042086
2004-12	NP-26	NP-040590	742		Editorial correction resulting from CR665	6.4.0	6.5.0	N1-041881
2004-12	NP-26	NP-040590	743		Unprotected REGISTER corrections	6.4.0	6.5.0	N1-041882
2004-12	NP-26	NP-040590	744	1	Corrections to receiving SDP offer in 200 (OK) response	6.4.0	6.5.0	N1-042087
2004-12	NP-26	NP-040590	745	1	Privacy corrections	6.4.0	6.5.0	N1-042085
2004-12	NP-26	NP-040590	747	2	Syntax of the P-Charging-Vector	6.4.0	6.5.0	N1-042105
2004-12	NP-26	NP-040590	752	2	Unavailability of the access-network-charging-info when the session is established without SBLP	6.4.0	6.5.0	N1-042106
2004-12	NP-26	NP-040590	753	1	SIP messages carrying the access-network-charging-info for sessions without preconditions	6.4.0	6.5.0	N1-042089

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2004-12	NP-26	NP-040590	755	1	Network-initiated deregistration for multiple UEs sharing the same user public identity and for the old contact information of a roaming UE registered in a new network	6.4.0	6.5.0	N1-042090
2004-12	NP-26	NP-040502	765	1	Interaction between S-CSCF and HSS in Network initiated deregistration procedure	6.4.0	6.5.0	N1-041966
2004-12	NP-26	NP-040502	768	1	Downloading of user profile	6.4.0	6.5.0	N1-042103
2005-01					Fix Word problem	6.5.0	6.5.1	
2005-03	NP-27	NP-050069	839		Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration	5.11.1	5.12.0	N1-050220
2005-03	NP-27	NP-050069	785		Deregistration effect on active sessions	6.5.1	6.6.0	N1-050052
2005-03	NP-27	NP-050069	784		Deregistration effect on active sessions	5.11.1	5.12.0	N1-050051
2005-03	NP-27	NP-050069	809	1	IOI storage at MGCF	5.11.1	5.12.0	N1-050295
2005-03	NP-27	NP-050069	840		Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration	6.5.1	6.6.0	N1-050221
2005-03	NP-27	NP-050069	806	1	Use of original dialog identifier at AS	6.5.1	6.6.0	N1-050292
2005-03	NP-27	NP-050069	807	2	Checking Request-URI for terminating requests at the S-CSCF	5.11.1	5.12.0	N1-050401
2005-03	NP-27	NP-050069	805	1	Use of original dialog identifier at AS	5.11.1	5.12.0	N1-050291
2005-03	NP-27	NP-050069	808	2	Checking Request-URI for terminating requests at the S-CSCF	6.5.1	6.6.0	N1-050402
2005-03	NP-27	NP-050069	810	1	IOI storage at MGCF	6.5.1	6.6.0	N1-050296
2005-03	NP-27	NP-050073	794		RFC 3966	6.5.1	6.6.0	N1-050080
2005-03	NP-27	NP-050073	848	1	Removal of I-CSCF normative requirement on Cx interface	6.5.1	6.6.0	N1-050299
2005-03	NP-27	NP-050073	841		Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules	6.5.1	6.6.0	N1-050225
2005-03	NP-27	NP-050073	817		Editorial corrections	6.5.1	6.6.0	N1-050129
2005-03	NP-27	NP-050073	786	1	Cleanups resulting from CR changes for last version	6.5.1	6.6.0	N1-050324
2005-03	NP-27	NP-050073	821	1	Handling topmost Route header at the P-CSCF	6.5.1	6.6.0	N1-050297
2005-03	NP-27	NP-050073	790		Registration - Abnormal Case	6.5.1	6.6.0	N1-050076
2005-03	NP-27	NP-050074	832	1	Corrections to the tables for 'PUBLISH'	6.5.1	6.6.0	N1-050341
2005-03	NP-27	NP-050074	822	1	Corrections to the UE tables for 'major capabilities'	6.5.1	6.6.0	N1-050332
2005-03	NP-27	NP-050074	825	1	Corrections to the UE tables for 'ACK'	6.5.1	6.6.0	N1-050334
2005-03	NP-27	NP-050074	826	1	Corrections to the tables for 'CANCEL'	6.5.1	6.6.0	N1-050335
2005-03	NP-27	NP-050074	827	1	Corrections to the tables for 'INVITE'	6.5.1	6.6.0	N1-050336
2005-03	NP-27	NP-050074	828	1	Corrections to the tables for 'MESSAGE'	6.5.1	6.6.0	N1-050337
2005-03	NP-27	NP-050074	829	1	Corrections to the tables for 'NOTIFY'	6.5.1	6.6.0	N1-050338
2005-03	NP-27	NP-050074	830	1	Corrections to the tables for 'OPTIONS'	6.5.1	6.6.0	N1-050339

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2005-03	NP-27	NP-050074	834	1	Corrections to the tables for 'REGISTER'	6.5.1	6.6.0	N1-050343
2005-03	NP-27	NP-050074	831	1	Corrections to the tables for 'PRACK'	6.5.1	6.6.0	N1-050340
2005-03	NP-27	NP-050074	833	1	Corrections to the tables for 'REFER'	6.5.1	6.6.0	N1-050342
2005-03	NP-27	NP-050074	835	1	Corrections to the tables for 'SUBSCRIBE'	6.5.1	6.6.0	N1-050344
2005-03	NP-27	NP-050074	836	1	Corrections to the tables for 'UPDATE'	6.5.1	6.6.0	N1-050345
2005-03	NP-27	NP-050074	837	1	Corrections to the tables for SDP	6.5.1	6.6.0	N1-050346
2005-03	NP-27	NP-050074	824	1	Removal of the UE table for 'status codes'	6.5.1	6.6.0	N1-050351
2005-03	NP-27	NP-050074	823	1	Corrections to the tables for 'BYE'	6.5.1	6.6.0	N1-050333
2005-03	NP-27	NP-050075	846	2	Correction to the Registration procedure	6.5.1	6.6.0	N1-050413
2005-03	NP-27	NP-050075	850	1	Addition of IMS-ALF to profile tables	6.5.1	6.6.0	N1-050348
2005-03	NP-27	NP-050075	851	2	Press and im URIs in incoming requests	6.5.1	6.6.0	N1-050395
2005-03	NP-27	NP-050075	788	1	MO - Calls to IPv4 SIP terminals	6.5.1	6.6.0	N1-050387
2005-03	NP-27	NP-050075	818	3	Corrections to subclause 5.5 in TS 24.229	6.5.1	6.6.0	N1-050414
2005-03	NP-27	NP-050075	801	3	Default handling associated with the trigger at the S-CSCF	6.5.1	6.6.0	N1-050418
2005-03	NP-27	NP-050075	803	4	Default handling associated with the trigger for third party registration	6.5.1	6.6.0	N1-050421
2005-03	NP-27	NP-050078	795	1	Sip-profile package in major capabilities	6.5.1	6.6.0	N1-050306
2005-03	NP-27	NP-050127	849	2	Corrections to addition of session set-up not requiring preconditions and reliable transport of provisional responses	6.5.1	6.6.0	
2005-06	CP-28	CP-050059	879		Correction Reg-Await-Auth Timer	6.6.0	6.7.0	C1-050522
2005-06	CP-28	CP-050059	881		Security Association in P-CSCF	6.6.0	6.7.0	C1-050524
2005-06	CP-28	CP-050059	871	1	Port 5060	6.6.0	6.7.0	C1-050674
2005-06	CP-28	CP-050059	891	2	SIP headers storage for P-CSCF initiated session release	6.6.0	6.7.0	C1-050777
2005-06	CP-28	CP-050059	921	1	Correction of error in the specification of the extension to Authorization header	6.6.0	6.7.0	C1-050689
2005-06	CP-28	CP-050059	886	2	Handling of P-Associated URI header	6.6.0	6.7.0	C1-050783
2005-06	CP-28	CP-050059	907	2	Clarification to the procedures at the I-CSCF	6.6.0	6.7.0	C1-050785
2005-06	CP-28	CP-050061	894	1	Re-registration failure	6.6.0	6.7.0	C1-050709
2005-06	CP-28	CP-050061	892		Completion of status-code tables in SIP profile	6.6.0	6.7.0	C1-050571
2005-06	CP-28	CP-050061	865	1	Unsubscribe by P-CSCF	6.6.0	6.7.0	C1-050671
2005-06	CP-28	CP-050061	866	1	Protected initial registration	6.6.0	6.7.0	C1-050708
2005-06	CP-28	CP-050061	916	1	Clarify that S-CSCF shall support Supported and Require headers	6.6.0	6.7.0	C1-050684
2005-06	CP-28	CP-050061	862		Shared public user identities	6.6.0	6.7.0	C1-050599
2005-06	CP-28	CP-050061	860	1	P-CSCF - routing of REGISTER requests	6.6.0	6.7.0	C1-050701
2005-06	CP-28	CP-050061	870	1	Correction of table A.104A	6.6.0	6.7.0	C1-050711

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2005-06	CP-28	CP-050061	887	1	Contact address in REGISTER response	6.6.0	6.7.0	C1-050716
2005-06	CP-28	CP-050061	890	1	P-CSCF Record-Route processing for target refresh requests/responses	6.6.0	6.7.0	C1-050717
2005-06	CP-28	CP-050061	893	1	AS originated requests on behalf of PSI	6.6.0	6.7.0	C1-050719
2005-06	CP-28	CP-050061	896	1	Routing PSI at terminating side	6.6.0	6.7.0	C1-050720
2005-06	CP-28	CP-050061	856	2	Notification about registration state	6.6.0	6.7.0	C1-050789
2005-06	CP-28	CP-050061	861	3	Registration failure at UE	6.6.0	6.7.0	C1-050790
2005-06	CP-28	CP-050061	899	2	Correction of the references for the integration of resource management procedures	6.6.0	6.7.0	C1-050791
2005-06	CP-28	CP-050061	902	2	Clarification on P-CSCF-intiated call release	6.6.0	6.7.0	C1-050792
2005-06	CP-28	CP-050061	863	3	Error handling in UE in case of RFC 3524	6.6.0	6.7.0	C1-050793
2005-06	CP-28	CP-050061	895	3	UE registration failure because the selected S-CSCF is unreachable	6.6.0	6.7.0	C1-050802
2005-06	CP-28	CP-050061	787	6	MT- SDP offer with IPv4 address.	6.6.0	6.7.0	C1-050794
2005-06	CP-28	CP-050061	858	1	S-CSCF redirecting	6.6.0	6.7.0	C1-050700
2005-06	CP-28	CP-050064	872	2	I-WLAN information for IMS	6.6.0	6.7.0	C1-050729
2005-06	CP-28	CP-050074	901		MWI RFC3842	6.6.0	7.0.0	C1-050600
2005-06	CP-28	CP-050075	905	1	3xx response and non-SDP bodies handking by proxies	6.6.0	7.0.0	C1-050775
2005-09	CP-29	CP-050346	986		Modifications to 24.229 to allow multiple IPsec security association per IKE_Security association	7.0.0	7.1.0	
2005-09	CP-29	CP-050355	930	1	Correction Profile Table A.119	7.0.0	7.1.0	C1-051061
2005-09	CP-29	CP-050355	946		Public User identity in 3rd party REG	7.0.0	7.1.0	C1-050906
2005-09	CP-29	CP-050355	957	1	Removal of Access Network Charging Information by the S-CSCF	7.0.0	7.1.0	C1-051081
2005-09	CP-29	CP-050355	965		Optional ccf	7.0.0	7.1.0	C1-050986
2005-09	CP-29	CP-050355	969	1	Contact header in REGISTER requests	7.0.0	7.1.0	C1-051177
2005-09	CP-29	CP-050359	932		SigComp-Corrections	7.0.0	7.1.0	C1-050877
2005-09	CP-29	CP-050359	962	1	IETF reference corrections	7.0.0	7.1.0	C1-051074
2005-09	CP-29	CP-050359	968	1	AS procedure correction	7.0.0	7.1.0	C1-051085
2005-09	CP-29	CP-050367	924		Incorporation of draft-ietf-sip-history	7.0.0	7.1.0	C1-050838
2005-09	CP-29	CP-050367	938		Contact header	7.0.0	7.1.0	C1-050887
2005-09	CP-29	CP-050367	939	1	Reason header - loss of radio coverage	7.0.0	7.1.0	C1-051158
2005-09	CP-29	CP-050367	947	3	Changes to TS 24.229 to ease interworking with non precondition terminals	7.0.0	7.1.0	C1-051213
2005-09	CP-29	CP-050367	958	2	Contents of P-Associated-URI header in 200 (OK) response to REGISTER	7.0.0	7.1.0	C1-051206
2005-09	CP-29	CP-050367	960	3	Consideration on 3rd Party Service Provider in Trust Domain	7.0.0	7.1.0	C1-051208

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2005-09	CP-29	CP-050367	971	1	Correction of requirement to insert P-Asserted-Identity header	7.0.0	7.1.0	C1-051166
2005-09	CP-29	CP-050368	950	3	privacy and trust rules for History header	7.0.0	7.1.0	C1-051199
2005-10					missing word in subclause 5.4.1.2.2, bullet 10b) is added by MCC	7.1.0	7.1.1	
2005-12	CP-30	CP-050538	1049		Replace “originated” with “terminated”	7.1.1	7.2.0	C1-051479
2005-12	CP-30	CP-050538	1046	2	Mobile originating call related requests	7.1.1	7.2.0	C1-051668
2005-12	CP-30	CP-050538	1012	1	Correction to section 5.4.3.2 t of TS 24.229	7.1.1	7.2.0	C1-051563
2005-12	CP-30	CP-050538	1026		Handling of P-Charging-Function-Adress	7.1.1	7.2.0	C1-051424
2005-12	CP-30	CP-050538	1071		Correction Syntax P-Charging Vector	7.1.1	7.2.0	C1-051508
2005-12	CP-30	CP-050541	1002	1	Modification to the definition of Security Association	7.1.1	7.2.0	C1-051576
2005-12	CP-30	CP-050542	0982	3	Access Type of P-Access-Network-Info header	7.1.1	7.2.0	C1-051675
2005-12	CP-30	CP-050542	1059		Replace “served” by “Originating” UE	7.1.1	7.2.0	C1-051489
2005-12	CP-30	CP-050542	1017		Correction to subclause 5.7.5.1. of TS 24229	7.1.1	7.2.0	C1-051382
2005-12	CP-30	CP-050542	1073	2	Short Session Setup in IMS	7.1.1	7.2.0	C1-051656
2005-12	CP-30	CP-050542	1054		Adjusting section reference in section 6.3	7.1.1	7.2.0	C1-051484
2005-12	CP-30	CP-050542	1029	1	B2B UA AS handling	7.1.1	7.2.0	C1-041597
2005-12	CP-30	CP-050542	1062	2	Correction to 3rd party registration procedures for SESSION_TERMINATED default handling	7.1.1	7.2.0	C1-051672
2005-12	CP-30	CP-050542	0994		cdma2000	7.1.1	7.2.0	C1-051336
2005-12	CP-30	CP-050542	1043		Correction of a reference in some tables in Appendix A	7.1.1	7.2.0	C1-051473
2005-12	CP-30	CP-050542	1005	2	Refreshes of SUBSCRIBE to reg-event (Fix for Rel 7)	7.1.1	7.2.0	C1-051670
2005-12	CP-30	CP-050542	1065	1	Charging terms correction	7.1.1	7.2.0	C1-051618
2005-12	CP-30	CP-050548	1081		Change of originating and terminating terminal terminology	7.1.1	7.2.0	C1-051535
2005-12	CP-30	CP-050548	1069	2	IBCF	7.1.1	7.2.0	C1-051587
2005-12	CP-30	CP-050550	1055		Editorial Changes	7.1.1	7.2.0	C1-051485
2005-12	CP-30	CP-050550	0996	1	UE initiated deregistration	7.1.1	7.2.0	C1-051649
2005-12	CP-30	CP-050550	1027	1	Mobile originated Request for unregistered user	7.1.1	7.2.0	C1-051653
2005-12	CP-30	CP-050550	0990	1	Authentication related Clarification	7.1.1	7.2.0	C1-051560
2005-12	CP-30	CP-050550	1019	2	Receipt of SIP URI with user equal phone at I-CSCF	7.1.1	7.2.0	C1-051671
2005-12	CP-30	CP-050550	0995	2	Default public user ID	7.1.1	7.2.0	C1-051691
2005-12	CP-30	CP-050550	0997	1	P-Preferred-Identity header	7.1.1	7.2.0	C1-051650
2005-12	CP-30	CP-050550	1082	1	P-CSCF discovery	7.1.1	7.2.0	C1-051681

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2005-12	CP-30	CP-050677	1085	2	Incorporating of TR 24.819 fixed broadband access impacts into TS 24.229	7.1.1	7.2.0	
2006-03	CP-31	CP-060106	1187	-	Removal of Warning header non-compliance with RFC 3261	7.2.0	7.3.0	C1-060328
2006-03	CP-31	CP-060106	1117	1	IMS AKA - SQN resync clarifications	7.2.0	7.3.0	C1-060453
2006-03	CP-31	CP-060106	1114	1	IMS AKA - content of initial authentication header	7.2.0	7.3.0	C1-060450
2006-03	CP-31	CP-060106	1204	-	Syntax and operation for Security-Client, Security-Server and Security-Verify headers	7.2.0	7.3.0	C1-060387
2006-03	CP-31	CP-060107	1148	1	UE processing 305 (Use Proxy)	7.2.0	7.3.0	C1-060507
2006-03	CP-31	CP-060107	1164	1	Clarifications on P-CSCF discovery	7.2.0	7.3.0	C1-060459
2006-03	CP-31	CP-060107	1161	1	DHCPv6 options for Domain Name Servers	7.2.0	7.3.0	C1-060456
2006-03	CP-31	CP-060110	1136	1	SDP answer	7.2.0	7.3.0	C1-060472
2006-03	CP-31	CP-060110	1206	-	Inclusion of Ma reference point	7.2.0	7.3.0	C1-060392
2006-03	CP-31	CP-060110	1134	-	Preconditions required	7.2.0	7.3.0	C1-060192
2006-03	CP-31	CP-060110	1156	1	Tables Change in Appendix A	7.2.0	7.3.0	C1-060478
2006-03	CP-31	CP-060110	1132	1	P-Asserted-Identity	7.2.0	7.3.0	C1-060476
2006-03	CP-31	CP-060111	1219	-	Reference Update of TS24.229, Rel7	7.2.0	7.3.0	C1-060483
2006-03	CP-31	CP-060111	1119	2	IMS Short Session Setup - Clarifications	7.2.0	7.3.0	C1-060595
2006-03	CP-31	CP-060111	1189	3	Definition of principles for IOI exchange and storage	7.2.0	7.3.0	C1-060610
2006-03	CP-31	CP-060111	1129	2	Tel URI	7.2.0	7.3.0	C1-060593
2006-03	CP-31	CP-060117	1210	1	Coding of P-Access-Network-Info header for 3GPP2 IMS	7.2.0	7.3.0	C1-060494
2006-03	CP-31	CP-060118	1103	1	Editor's Note on xDSL bearer	7.2.0	7.3.0	C1-060119
2006-03	CP-31	CP-060118	1095	1	Reference to new annexes on NAT	7.2.0	7.3.0	C1-060116
2006-03	CP-31	CP-060118	1101	-	Replaces header in Profile Tables	7.2.0	7.3.0	C1-060051
2006-03	CP-31	CP-060118	1093	2	P-Access-Network-Info header absence for emergency call detection	7.2.0	7.3.0	C1-060339
2006-03	CP-31	CP-060118	1196	1	correction for the procedure of changing media data	7.2.0	7.3.0	C1-060518
2006-03	CP-31	CP-060118	1197	1	Editorial Changes	7.2.0	7.3.0	C1-060519
2006-03	CP-31	CP-060118	1092	3	Optionality of P-Access-Network-Info header	7.2.0	7.3.0	C1-060338
2006-03	CP-31	CP-060118	1086	1	Addition of TISPAN supported internet-drafts	7.2.0	7.3.0	C1-060337
2006-03	CP-31	CP-060118	1089	1	IBCF corrections	7.2.0	7.3.0	C1-060110
2006-03	CP-31	CP-060118	1106	4	Completion of IBCF routing procedures	7.2.0	7.3.0	C1-060498
2006-03	CP-31	CP-060118	1088	4	IBCF enhancements	7.2.0	7.3.0	C1-060603
2006-03	CP-31	CP-060119	1177	1	PacketCable Extensions to P-Charging-Vector header	7.2.0	7.3.0	C1-060512

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2006-03	CP-31	CP-060120	1098	4	Emergency service S-CSCF impact	7.2.0	7.3.0	C1-060601
2006-03	CP-31	CP-060120	1097	5	Emergency service - P-CSCF impact	7.2.0	7.3.0	C1-060600
2006-03	CP-31	CP-060120	1099	5	Emergency service - E-CSCF impact	7.2.0	7.3.0	C1-060599
2006-03	CP-31	CP-060120	1096	5	Emergency service - UE impact	7.2.0	7.3.0	C1-060602
2006-03	CP-31	CP-060121	1183	-	Transfer of Text from the Combinational Services TR 24.879 to TS 24.229	7.2.0	7.3.0	C1-060311
2006-03	CP-31	CP-060124	1138	2	Session termination by P-CSCF	7.2.0	7.3.0	C1-060605
2006-03	CP-31	CP-060124	1157	3	Support for RFC 4145	7.2.0	7.3.0	C1-060621
2006-03	CP-31	CP-060124	1184	3	Registration of multiple PUIs - CR	7.2.0	7.3.0	C1-060608
2006-03	CP-31	CP-060124	1137	1	Session termination by S-CSCF	7.2.0	7.3.0	C1-060533
2006-03	CP-31	CP-060124	1152	1	Editorial Changes	7.2.0	7.3.0	C1-060539
2006-03	CP-31	CP-060124	1107	1	Reference Update of TS24.229	7.2.0	7.3.0	C1-060123
2006-03	CP-31	CP-060124	1125	-	Pre-loaded Route header	7.2.0	7.3.0	C1-060183
2006-03	CP-31	CP-060142	1226	1	Transport of HSS address from I-CSCF to S-CSCF	7.2.0	7.3.0	-
2006-03	CP-31	CP-060153	1222	2	Mandationof RFC 4320 fixes for issues found with the Session Initiation Protocol's (SIP) Non-INVITE Transactions	7.2.0	7.3.0	-
2006-03	CP-31	CP-060176	1225	2	Support of call forwarding at the S-CSCF	7.2.0	7.3.0	-
2006-06	CP-32	CP-060232	1290	2	Realm Parameter Handling	7.3.0	7.4.0	
2006-06	CP-32	CP-060249	1242	3	SDP answer	7.3.0	7.4.0	
2006-06	CP-32	CP-060262	1309	2	Hiding correction	7.3.0	7.4.0	C1-061115
2006-06	CP-32	CP-060262	1306	2	3rd-party registration	7.3.0	7.4.0	C1-061098
2006-06	CP-32	CP-060262	1303	1	One private identity one contact	7.3.0	7.4.0	C1-061095
2006-06	CP-32	CP-060264	1274	2	Re-authentication during deregistration	7.3.0	7.4.0	C1-061113
2006-06	CP-32	CP-060265	1312		I-CSCF registration procedure correction	7.3.0	7.4.0	C1-060829
2006-06	CP-32	CP-060266	1265	1	IOI overview	7.3.0	7.4.0	C1-060997
2006-06	CP-32	CP-060266	1271	1	Introduction of signalling encryption	7.3.0	7.4.0	C1-060999
2006-06	CP-32	CP-060266	1348		UE behavior after timer F expiry	7.3.0	7.4.0	C1-060897
2006-06	CP-32	CP-060266	1236	2	P-Asserted-ID	7.3.0	7.4.0	C1-061119
2006-06	CP-32	CP-060266	1238	1	Via header in the initial registration	7.3.0	7.4.0	C1-060975
2006-06	CP-32	CP-060266	1327	1	Incorrect requirement on I-CSCF	7.3.0	7.4.0	C1-061079
2006-06	CP-32	CP-060270	1247	1	Emergency PUID	7.3.0	7.4.0	C1-061054
2006-06	CP-32	CP-060270	1266	1	Inclusion of draft-ietf-ecrit-service-urn	7.3.0	7.4.0	C1-061009
2006-06	CP-32	CP-060270	1229		Emergency service S-CSCF impact	7.3.0	7.4.0	C1-060642
2006-06	CP-32	CP-060270	1360		Inclusion of E-CSCF in subclause 3.1 and subclause 4.1	7.3.0	7.4.0	C1-060923
2006-06	CP-32	CP-060270	1249	2	Emergency call release	7.3.0	7.4.0	C1-061121
2006-06	CP-32	CP-060270	1338	1	Adding RDF in E-CSCF procedure	7.3.0	7.4.0	C1-061060

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2006-06	CP-32	CP-060270	1358	1	Priority handling for emergency calls at the E-CSCF	7.3.0	7.4.0	C1-061017
2006-06	CP-32	CP-060270	1357	1	Priority handling for emergency calls at the S-CSCF	7.3.0	7.4.0	C1-061015
2006-06	CP-32	CP-060270	1356	1	Priority handling for emergency calls at the P-CSCF	7.3.0	7.4.0	C1-061013
2006-06	CP-32	CP-060270	1354		Inclusion of session timer procedures at the E-CSCF	7.3.0	7.4.0	C1-060917
2006-06	CP-32	CP-060270	1340	2	TEL URI associated with emergency IMPU	7.3.0	7.4.0	C1-061120
2006-06	CP-32	CP-060270	1337	1	Getting local emergency numbers	7.3.0	7.4.0	C1-061010
2006-06	CP-32	CP-060270	1336	1	Some corrections in IMS emergency calls	7.3.0	7.4.0	C1-061059
2006-06	CP-32	CP-060271	1258	1	UDP encapsulation of IPSec	7.3.0	7.4.0	C1-061019
2006-06	CP-32	CP-060271	1318	1	Extensions to P-Access-Network-Info header for DOCSIS Access	7.3.0	7.4.0	C1-061025
2006-06	CP-32	CP-060271	1317	2	PRACK	7.3.0	7.4.0	C1-061026
2006-06	CP-32	CP-060271	1267	1	IBCF corrections	7.3.0	7.4.0	C1-061022
2006-06	CP-32	CP-060271	1259	1	IBCF initiated call release	7.3.0	7.4.0	C1-061021
2006-06	CP-32	CP-060271	1345	1	Correction of the reference document	7.3.0	7.4.0	C1-061082
2006-06	CP-32	CP-060274	1234	1	Final NOTIFY	7.3.0	7.4.0	C1-060989
2006-06	CP-32	CP-060274	1255		Full notification	7.3.0	7.4.0	C1-060686
2006-06	CP-32	CP-060274	1260		Reg event package parameters in notification	7.3.0	7.4.0	C1-060704
2006-06	CP-32	CP-060274	1261		Subscription refreshing	7.3.0	7.4.0	C1-060705
2006-06	CP-32	CP-060274	1217	2	Definition of B2BUA	7.3.0	7.4.0	C1-061074
2006-06	CP-32	CP-060274	1277	1	Usage of associated public user identities	7.3.0	7.4.0	C1-060964
2006-06	CP-32	CP-060274	1321		Verification by I-CSCF of trust domain origin for incoming requests	7.3.0	7.4.0	C1-060844
2006-06	CP-32	CP-060274	1322		Miscellaneous Correction	7.3.0	7.4.0	C1-060845
2006-06	CP-32	CP-060274	1328	1	Resilience to registration and authentication errors	7.3.0	7.4.0	C1-061080
2006-06	CP-32	CP-060274	1335	1	The Correction on the description for the information of registration status	7.3.0	7.4.0	C1-060986
2006-06	CP-32	CP-060274	1361		Reference updates	7.3.0	7.4.0	C1-060924
2006-06	CP-32	CP-060283	1366		Emergency service – UE impact	7.3.0	7.4.0	
2006-06	CP-32	CP-060284	1367		Emergency service- E-CSCF impact	7.3.0	7.4.0	
2006-06	CP-32	CP-060335	1232	3	Handling of P-Charging-Addresses	7.3.0	7.4.0	
2006-06	CP-32	CP-060345	1365	1	Registration of several unrelated public user identities	7.3.0	7.4.0	
2006-06	CP-32	CP-060352	1228	4	Emergency service P-CSCF-impact	7.3.0	7.4.0	C1-061134
2006-09	CP-33	CP-060452	1461	1	Correction of Realm Parameter Handling for S-CSCF procedures	7.4.0	7.5.0	C1-061732
2006-09	CP-33	CP-060452	1467		SDP reference revision	7.4.0	7.5.0	C1-061657

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2006-09	CP-33	CP-060452	1475	2	"Response" value in unprotected Register requests	7.4.0	7.5.0	C1-061845
2006-09	CP-33	CP-060463	1351	3	Treatment of emergency requests other than INVITE requests at the P-CSCF	7.4.0	7.5.0	C1-061357
2006-09	CP-33	CP-060463	1352	3	Treatment of emergency requests other than INVITE requests at the E-CSCF	7.4.0	7.5.0	C1-061358
2006-09	CP-33	CP-060463	1369	1	UE emergency deregistration	7.4.0	7.5.0	C1-061304
2006-09	CP-33	CP-060463	1370	1	Emergency subscription	7.4.0	7.5.0	C1-061305
2006-09	CP-33	CP-060463	1371	1	P-CSCF emergency subscription	7.4.0	7.5.0	C1-061306
2006-09	CP-33	CP-060463	1373	2	S-CSCF emergency registration	7.4.0	7.5.0	C1-061350
2006-09	CP-33	CP-060463	1374	2	Handling of Emergency registration in S-CSCF	7.4.0	7.5.0	C1-061349
2006-09	CP-33	CP-060463	1375	2	Handling of emergency registration at the UE	7.4.0	7.5.0	C1-061351
2006-09	CP-33	CP-060463	1379	4	Location handling E-CSCF	7.4.0	7.5.0	C1-061913
2006-09	CP-33	CP-060463	1380	1	Clarification of Emergency Session Setup without prior IMS Registration	7.4.0	7.5.0	C1-061311
2006-09	CP-33	CP-060463	1381	1	Clarifications to subclause 5.1.6.1	7.4.0	7.5.0	C1-061313
2006-09	CP-33	CP-060463	1383	1	Non-INVITE requests	7.4.0	7.5.0	C1-061314
2006-09	CP-33	CP-060463	1384	2	IP-CAN for emergency calls	7.4.0	7.5.0	C1-061355
2006-09	CP-33	CP-060463	1390	1	Adoption of terminology from draft-ietf-ecrit-requirements	7.4.0	7.5.0	C1-061315
2006-09	CP-33	CP-060463	1391	3	Minor corrections to EMC1 text from previous CRs	7.4.0	7.5.0	C1-061367
2006-09	CP-33	CP-060463	1414	2	Handling of loacation information at E-CSCF	7.4.0	7.5.0	C1-061860
2006-09	CP-33	CP-060463	1440	2	P-Asserted-Identity in P-CSCF handling	7.4.0	7.5.0	C1-061861
2006-09	CP-33	CP-060463	1443	4	Handling of PSAP address mapping result at E-CSCF	7.4.0	7.5.0	C1-061919
2006-09	CP-33	CP-060465	1413	1	Miscellaneous Corrections in Annex F	7.4.0	7.5.0	C1-061826
2006-09	CP-33	CP-060465	1420	1	Transit IMS	7.4.0	7.5.0	C1-061827
2006-09	CP-33	CP-060465	1425	1	P-CSCF procedures for session release when QoS resources are unavailable	7.4.0	7.5.0	C1-061830
2006-09	CP-33	CP-060465	1427	1	Make SDP bandwidth modifiers optional for standard RTCP usage	7.4.0	7.5.0	C1-061832
2006-09	CP-33	CP-060465	1430	3	Addition of the cpc parameter to TS24.229	7.4.0	7.5.0	C1-061882
2006-09	CP-33	CP-060466	1385	4	Introduction of GRUU in 24.229	7.4.0	7.5.0	C1-061858
2006-09	CP-33	CP-060466	1386	5	S-SCSF procedures to support GRUU	7.4.0	7.5.0	C1-061915
2006-09	CP-33	CP-060468	1405		Original dialog identifier	7.4.0	7.5.0	C1-061408
2006-09	CP-33	CP-060468	1406		No-fork	7.4.0	7.5.0	C1-061409
2006-09	CP-33	CP-060468	1409		Connection addres - zero	7.4.0	7.5.0	C1-061412
2006-09	CP-33	CP-060468	1415		Reference for populating the "Anonymous" From header	7.4.0	7.5.0	C1-061439

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2006-09	CP-33	CP-060468	1439	1	Usage of P-Associated-URI	7.4.0	7.5.0	C1-061759
2006-09	CP-33	CP-060468	1450		Clarification of network initiated deregistration to match reginfo format	7.4.0	7.5.0	C1-061585
2006-09	CP-33	CP-060468	1456	2	Authentication between UA and UA	7.4.0	7.5.0	C1-061851
2006-09	CP-33	CP-060468	1457	2	Treatment by S-CSCF of profile changes for registered PUIs	7.4.0	7.5.0	C1-061853
2006-09	CP-33	CP-060468	1458	1	Completionof RFC 4320 fixes for 100 Trying responses Non-INVITE Transactions RFC 4320 fixes for 100 Trying responses Non-INVITE Transactions tration	7.4.0	7.5.0	C1-061765
2006-09	CP-33	CP-060468	1463		Correction to S-CSCF procedures for UE-originated requests	7.4.0	7.5.0	C1-061646
2006-09	CP-33	CP-060468	1464	1	SCTP transport	7.4.0	7.5.0	C1-061766
2006-09	CP-33	CP-060504	1257	4	SDP usage at MGCF	7.4.0	7.5.0	C1-061847
2006-09	CP-33	CP-060504	1417	1	Type 3 orig-ioi in I-CSCF	7.4.0	7.5.0	C1-061744
2006-09	CP-33	CP-060504	1469		SDP corrections	7.4.0	7.5.0	C1-061659
2006-09	CP-33	CP-060504	1471		SDP completion	7.4.0	7.5.0	C1-061661
2006-09	CP-33	CP-060504	1478	1	Updates to Profile Tables UE Major Capabilities	7.4.0	7.5.0	C1-061754
2006-09	CP-33	CP-060504	1481		Removal of Editor's notes in 24.229, rel-6	7.4.0	7.5.0	C1-061745
2006-09	CP-33	CP-060504	1483		Final codec selection	7.4.0	7.5.0	C1-061850
2006-09	CP-33	CP-060526	1418	3	Originating requests on behalf of an unregistered user	7.4.0	7.5.0	C1-061758
2006-09					Version 7.5.1 created by MCC to correct styles	7.5.0	7.5.1	
2006-12	CP-34	CP-060655	1502	-	RFC reference update	7.5.1	7.6.0	C1-061977
2006-12	CP-34	CP-060655	1506	-	SDP group attribute correction	7.5.1	7.6.0	C1-061981
2006-12	CP-34	CP-060655	1504	1	Addressing editor's notes relating to trust domains	7.5.1	7.6.0	C1-062304
2006-12	CP-34	CP-060655	1546	-	Join header correction	7.5.1	7.6.0	C1-062205
2006-12	CP-34	CP-060655	1508	2	Processing the successful response at S-CSCF	7.5.1	7.6.0	C1-062434
2006-12	CP-34	CP-060655	1449	2	Correction of S-CSCF construction and UE interpretation of registration event notification	7.5.1	7.6.0	C1-062317
2006-12	CP-34	CP-060655	1514	1	Removal of more Editor's notes in 24.229, rel-6	7.5.1	7.6.0	C1-062310
2006-12	CP-34	CP-060659	1491	2	Location handling for emergency	7.5.1	7.6.0	C1-062437
2006-12	CP-34	CP-060659	1521	1	Location information for IMS emergency	7.5.1	7.6.0	C1-062293
2006-12	CP-34	CP-060659	1529	2	Emergency re-registration due to mobility	7.5.1	7.6.0	C1-062436
2006-12	CP-34	CP-060659	1515	1	Removal of Editor's notes on emergency call in clause 4	7.5.1	7.6.0	C1-062292
2006-12	CP-34	CP-060659	1484	1	Corrections to emergency call procedures for P-Asserted-Identity header	7.5.1	7.6.0	C1-062289

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2006-12	CP-34	CP-060659	1543	-	Next hop is the BGCF	7.5.1	7.6.0	C1-062181
2006-12	CP-34	CP-060659	1536	-	Editorial corrections to emergency call text	7.5.1	7.6.0	C1-062142
2006-12	CP-34	CP-060659	1542	1	minor correction to EMC of UE and PCSCF	7.5.1	7.6.0	C1-062299
2006-12	CP-34	CP-060659	1490	2	Emergency call on existing registration	7.5.1	7.6.0	C1-062435
2006-12	CP-34	CP-060660	1486	2	Introduction of communication service concept in TS 24229	7.5.1	7.6.0	C1-062451
2006-12	CP-34	CP-060662	1494	1	Tel URI translation	7.5.1	7.6.0	C1-062325
2006-12	CP-34	CP-060662	1523	1	I-CSCF procedure	7.5.1	7.6.0	C1-062333
2006-12	CP-34	CP-060662	1544	-	Clarification of UEs initial SDP offer	7.5.1	7.6.0	C1-062189
2006-12	CP-34	CP-060662	1493	1	Alias URI	7.5.1	7.6.0	C1-062324
2006-12	CP-34	CP-060662	1525	1	Clarification of iFC execution for UE-terminated requests at S-CSCF	7.5.1	7.6.0	C1-062334
2006-12	CP-34	CP-060662	1533	1	SIP response code to unknown method	7.5.1	7.6.0	C1-062336
2006-12	CP-34	CP-060662	1537	-	Originating requests on behalf of an unregistered user	7.5.1	7.6.0	C1-062143
2006-12	CP-34	CP-060662	1538	-	Treatment by S-CSCF of profile changes for registered PUIs	7.5.1	7.6.0	C1-062144
2006-12	CP-34	CP-060662	1547	-	Corrections to Profile table for RFC 4320 compliance	7.5.1	7.6.0	C1-062210
2006-12	CP-34	CP-060662	1539	-	Miscellaneous editorial corrections	7.5.1	7.6.0	C1-062145
2006-12	CP-34	CP-060662	1509	1	No-forking at AS	7.5.1	7.6.0	C1-062329
2006-12	CP-34	CP-060662	1528	2	P-Visited-Network-ID on ISC interface	7.5.1	7.6.0	C1-062442
2006-12	CP-34	CP-060662	1487	1	Introduction of P-Profile Key in TS 24.229	7.5.1	7.6.0	C1-062322
2006-12	CP-34	CP-060662	1522	1	Local numbering	7.5.1	7.6.0	C1-062338
2006-12	CP-34	CP-060662	1495	2	BGCF procedures	7.5.1	7.6.0	C1-062440
2006-12	CP-34	CP-060662	1498	2	AS acting as PSI	7.5.1	7.6.0	C1-062441
2006-12	CP-34	CP-060662	1524	-	Clarification of the URI in UE-terminating requests at the P-CSCF	7.5.1	7.6.0	C1-062061
2006-12	CP-34	CP-060662	1549	1	Core Network Service Authorizatrion	7.5.1	7.6.0	C1-062339
2006-12	CP-34	CP-060663	1527	3	Align with GRUU IETF draft 11	7.5.1	7.6.0	C1-062512
2006-12	CP-34	CP-060663	1496	1	I-CSCF processing GRUU	7.5.1	7.6.0	C1-062340
2006-12	CP-34	CP-060663	1497	1	S-CSCF processing GRUU	7.5.1	7.6.0	C1-062341
2006-12	CP-34	CP-060663	1422	3	GRUU processing by non-UE User Agents	7.5.1	7.6.0	C1-062343
2006-12	CP-34	CP-060667	1426	3	Allowing an asserted display name to be conveyed with a Public Identity	7.5.1	7.6.0	C1-062427
2006-12	CP-34	CP-060667	1429	4	Update to NAT Traversal procedures in support of Outbound and ICE	7.5.1	7.6.0	C1-062515
2006-12	CP-34	CP-060667	1540	2	Annex I (Transit IMS) improvements	7.5.1	7.6.0	C1-062516
2007-03	CP-35	CP-070130	1566	-	Session Establishment Interworking with Rel-5 UEs	7.6.0	7.7.0	C1-070052

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-03	CP-35	CP-070130	1638	-	Inclusion of draft-ietf-sip-uri-list-message in SIP profile	7.6.0	7.7.0	C1-070266
2007-03	CP-35	CP-070130	1619	-	Clarifications on resource reservation	7.6.0	7.7.0	C1-070180
2007-03	CP-35	CP-070130	1621	1	Routeing B2BUA handling of Replaces header	7.6.0	7.7.0	C1-070439
2007-03	CP-35	CP-070132	1609	-	Establishing an emergency session	7.6.0	7.7.0	C1-070147
2007-03	CP-35	CP-070132	1575	-	Deletion of editors note in subclause 5.1.6.5	7.6.0	7.7.0	C1-070068
2007-03	CP-35	CP-070132	1639	-	Identification of emergency calls	7.6.0	7.7.0	C1-070276
2007-03	CP-35	CP-070132	1593	1	Limitation on Emergency Registration	7.6.0	7.7.0	C1-070424
2007-03	CP-35	CP-070132	1586	1	Tidyup UE clause	7.6.0	7.7.0	C1-070418
2007-03	CP-35	CP-070132	1654	1	Double reference removal	7.6.0	7.7.0	C1-070381
2007-03	CP-35	CP-070132	1605	1	Emergency PUID	7.6.0	7.7.0	C1-070419
2007-03	CP-35	CP-070132	1569	1	Handling of parallel emergency registration	7.6.0	7.7.0	C1-070413
2007-03	CP-35	CP-070132	1574	1	Deletion of editors note in subclause 5.1.6.2	7.6.0	7.7.0	C1-070414
2007-03	CP-35	CP-070132	1568	1	Connecting to an Emergency APN	7.6.0	7.7.0	C1-070409
2007-03	CP-35	CP-070132	1581	1	Deletion of Editor' s notes in 5.2.10	7.6.0	7.7.0	C1-070416
2007-03	CP-35	CP-070132	1641	-	Correction of service-urn	7.6.0	7.7.0	C1-070278
2007-03	CP-35	CP-070132	1589	-	Correction of CR#1484r1 implementation error (subclause 5.1.6.8.3)	7.6.0	7.7.0	C1-070111
2007-03	CP-35	CP-070132	1610	-	Emergency session-no registration	7.6.0	7.7.0	C1-070148
2007-03	CP-35	CP-070134	1612	2	Emergency treatment at P-CSCF	7.6.0	7.7.0	C1-070563
2007-03	CP-35	CP-070134	1635	1	Remove the term ESRP	7.6.0	7.7.0	C1-070430
2007-03	CP-35	CP-070134	1607	2	Emergency call at P-CSCF	7.6.0	7.7.0	C1-070443
2007-03	CP-35	CP-070134	1632	1	Backward compatibility for using 380 response	7.6.0	7.7.0	C1-070429
2007-03	CP-35	CP-070134	1653	3	Location for emergency	7.6.0	7.7.0	C1-070618
2007-03	CP-35	CP-070134	1626	1	Handling of re-registration when user redial emergency number	7.6.0	7.7.0	C1-070426
2007-03	CP-35	CP-070134	1582	2	Deletion of editors notes in 5.11 and 5.4.8	7.6.0	7.7.0	C1-070615
2007-03	CP-35	CP-070134	1567	3	Home Network Indication for Emergency Calls	7.6.0	7.7.0	C1-070640
2007-03	CP-35	CP-070134	1631	2	Correction to emergency call procedure with non-emergency registration for P-Asserted-Identity header	7.6.0	7.7.0	C1-070617
2007-03	CP-35	CP-070137	1634	1	Profile definition for CSI application server	7.6.0	7.7.0	C1-070469
2007-03	CP-35	CP-070138	1660	1	Format of dsl-location	7.6.0	7.7.0	C1-070552
2007-03	CP-35	CP-070138	1595	1	Deletion of EN's in clause 5.10	7.6.0	7.7.0	C1-070547
2007-03	CP-35	CP-070138	1594	-	Deletion of EN's in Annex G	7.6.0	7.7.0	C1-070132
2007-03	CP-35	CP-070139	1613	2	Annex K NAT Traversal Procedural and References Updates	7.6.0	7.7.0	C1-070626

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-03	CP-35	CP-070139	1617	1	Routing of SIP URI "user=phone" when domain doesn't own target user	7.6.0	7.7.0	C1-070551
2007-03	CP-35	CP-070139	1614	1	Annex A updates for Annex K NAT Traversal Procedurals	7.6.0	7.7.0	C1-070550
2007-03	CP-35	CP-070140	1598	1	Forked MESSAGE request	7.6.0	7.7.0	C1-070451
2007-03	CP-35	CP-070140	1558	1	Removal of notes for screening functionality	7.6.0	7.7.0	C1-070441
2007-03	CP-35	CP-070140	1556	1	Handling of special characters in the local service number	7.6.0	7.7.0	C1-070458
2007-03	CP-35	CP-070140	1655	2	Forwarding a request by transit functions in the S-CSCF	7.6.0	7.7.0	C1-070586
2007-03	CP-35	CP-070140	1587	1	Terminating case in S-CSCF	7.6.0	7.7.0	C1-070449
2007-03	CP-35	CP-070140	1559	-	Completion of SIP timers functionality	7.6.0	7.7.0	C1-070039
2007-03	CP-35	CP-070140	1588	1	P-User-Database	7.6.0	7.7.0	C1-070450
2007-03	CP-35	CP-070140	1560	1	Removal of notes for SIGCOMP functionality	7.6.0	7.7.0	C1-070442
2007-03	CP-35	CP-070140	1557	-	Removal of normative statements in NOTEs	7.6.0	7.7.0	C1-070037
2007-03	CP-35	CP-070140	1604	1	Forwarding P-Charging-Vector outside the home network	7.6.0	7.7.0	C1-070453
2007-03	CP-35	CP-070140	1555	1	Removal of Editor's notes for message bodies	7.6.0	7.7.0	C1-070440
2007-03	CP-35	CP-070140	1652	-	Correction for local numbers	7.6.0	7.7.0	C1-070341
2007-03	CP-35	CP-070140	1601	-	Tel URI translation	7.6.0	7.7.0	C1-070139
2007-03	CP-35	CP-070140	1646	1	Align definition of Alias URI with the description in 23.228	7.6.0	7.7.0	C1-070455
2007-03	CP-35	CP-070140	1600	2	Dual IP addresses	7.6.0	7.7.0	C1-070584
2007-03	CP-35	CP-070142	1642	-	SIP extensions covering URI-lists	7.6.0	7.7.0	C1-070279
2007-03	CP-35	CP-070148	1564	1	Network Initiated / Modified Media PDP Contexts	7.6.0	7.7.0	C1-070447
2007-03	CP-35	CP-070149	1643	-	SDP usage in association with BFCP (additions to SDP profile)	7.6.0	7.7.0	C1-070282
2007-03	CP-35	CP-070151	1648	2	S-CSCF inserts P-Called-Party-ID before forwarding request towards served user	7.6.0	7.7.0	C1-070588
2007-03	CP-35	CP-070151	1597	1	Instance ID	7.6.0	7.7.0	C1-070461
2007-03	CP-35	CP-070151	1615	1	Signalling Public User Identity to AS when request URI is Temp-GRUU	7.6.0	7.7.0	C1-070463
2007-03	CP-35	CP-070214	1640	3	Location conveyance revisions	7.6.0	7.7.0	
2007-03	CP-35	CP-070242	1576	3	Deletion of editors notes in subclauses 5.1.6.8.2, 5.1.6.8.3, 5.1.6.8.4	7.6.0	7.7.0	
2007-03	CP-35	CP-070252	1658	4	Profile for IBCF	7.6.0	7.7.0	
2007-03	CP-35	CP-070254	1580	3	PCC introduction to TS 24.229	7.6.0	7.7.0	
2007-03	CP-35	CP-070255	1630	3	Corrections for the handling of target refresh requests at the S-CSCF	7.6.0	7.7.0	

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-03	CP-35	CP-070271	1623	5	Further alignment with phonebcp draft	7.6.0	7.7.0	
2007-06	CP-36	CP-070370	1749	1	Correction of coding rules of P-Access-Network-Info header	7.7.0	7.8.0	C1-071435
2007-06	CP-36	CP-070370	1689	2	Inclusion of "addressing an amplification vulnerability in session initiation protocol forking proxies" (draft-ietf-sip-fork-loop-fix) in the SIP profile	7.7.0	7.8.0	C1-071409
2007-06	CP-36	CP-070373	1666	2	Protocol between E-CSCF and LRF	7.7.0	7.8.0	C1-071040
2007-06	CP-36	CP-070373	1690	-	Further alignment with phonebcp draft	7.7.0	7.8.0	C1-070779
2007-06	CP-36	CP-070373	1763	1	Emergency registration clarification	7.7.0	7.8.0	C1-071441
2007-06	CP-36	CP-070373	1665	1	Definition of identities used for emergency call	7.7.0	7.8.0	C1-070957
2007-06	CP-36	CP-070374	1714	1	Alignment of layout of access technology specific annexes	7.7.0	7.8.0	C1-071032
2007-06	CP-36	CP-070374	1715	1	GPRS IP-CAN change of normative requirement out of scope to informative	7.7.0	7.8.0	C1-071033
2007-06	CP-36	CP-070374	1732	2	Clarification on iFC execution	7.7.0	7.8.0	C1-071460
2007-06	CP-36	CP-070374	1721	1	UE un-subscribing to reg-event	7.7.0	7.8.0	C1-071419
2007-06	CP-36	CP-070374	1722	-	MO Record-Route at P-CSCF	7.7.0	7.8.0	C1-071051
2007-06	CP-36	CP-070374	1723	1	MT Record-Route at P-CSCF	7.7.0	7.8.0	C1-071420
2007-06	CP-36	CP-070374	1727	1	Double registration	7.7.0	7.8.0	C1-071422
2007-06	CP-36	CP-070374	1730	1	Inclusion of new mandatory elements of SigComp	7.7.0	7.8.0	C1-071423
2007-06	CP-36	CP-070374	1731	1	Use of a presence specific dictionary in SigComp	7.7.0	7.8.0	C1-071424
2007-06	CP-36	CP-070374	1720	1	Registration and deregistration	7.7.0	7.8.0	C1-071418
2007-06	CP-36	CP-070374	1746	1	Correction to P-CSCF procedures for cancellation of a session currently being established	7.7.0	7.8.0	C1-071431
2007-06	CP-36	CP-070374	1762	1	Originating a terminating request in an AS	7.7.0	7.8.0	C1-071433
2007-06	CP-36	CP-070374	1769	2	Clarification to Original Dialog Identifier	7.7.0	7.8.0	C1-071463
2007-06	CP-36	CP-070374	1761	-	Local numbering clarification	7.7.0	7.8.0	C1-071196
2007-06	CP-36	CP-070374	1760	1	PANI related corrections	7.7.0	7.8.0	C1-071437
2007-06	CP-36	CP-070374	1743	1	The precondition mechanism may be required in subsequent SDP offer/answer exchanges	7.7.0	7.8.0	C1-071430
2007-06	CP-36	CP-070374	1772	-	Minor miscellaneous clean-up	7.7.0	7.8.0	C1-071231
2007-06	CP-36	CP-070374	1739	1	P-CSCF processing of P-Early-Media	7.7.0	7.8.0	C1-071428
2007-06	CP-36	CP-070374	1738	3	Originating UE sending of P-Early-Media	7.7.0	7.8.0	C1-071462
2007-06	CP-36	CP-070374	1737	2	Originating UE processing of P-Early-Media	7.7.0	7.8.0	C1-071461
2007-06	CP-36	CP-070375	1692	-	Profile support for a session initiation protocol event package and data format for various settings in support for the push-to-talk over cellular service (RFC4354)	7.7.0	7.8.0	C1-070781

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-06	CP-36	CP-070375	1562	4	Completion of Phone-context parameter in rel-7	7.7.0	7.8.0	C1-071009
2007-06	CP-36	CP-070375	1700	-	Translation of non-international format numbers	7.7.0	7.8.0	C1-070810
2007-06	CP-36	CP-070375	1680	-	Outgoing Request URI=pres or IM URI processing clarification and misc clean-up	7.7.0	7.8.0	C1-070705
2007-06	CP-36	CP-070375	1691	1	Profile support for the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular (draft-allen-sipping-poc-p-answer-state-header)	7.7.0	7.8.0	C1-070987
2007-06	CP-36	CP-070375	1678	1	Qvalue	7.7.0	7.8.0	C1-070984
2007-06	CP-36	CP-070375	1704	-	Minor miscellaneous clean-up	7.7.0	7.8.0	C1-070824
2007-06	CP-36	CP-070375	1703	-	Filter criteria evaluation when the AS changes the P-Asserted-Identity	7.7.0	7.8.0	C1-070823
2007-06	CP-36	CP-070378	1718	1	Addition to network initiated PDP context	7.7.0	7.8.0	C1-071346
2007-06	CP-36	CP-070380	1679	-	Cleanup of Signalling Public GRUU to AS	7.7.0	7.8.0	C1-070704
2007-06	CP-36	CP-070380	1663	-	Provide GRUU functionality in case of hosted NAT	7.7.0	7.8.0	C1-070663
2007-06	CP-36	CP-070380	1756	1	GRUU Alignment with stage 2	7.7.0	7.8.0	C1-071456
2007-06	CP-36	CP-070380	1686	2	Alternate GRUU for AS acting on behalf of Public User Identity	7.7.0	7.8.0	C1-071010
2007-06	CP-36	CP-070380	1713	2	Cleanup of GRUU	7.7.0	7.8.0	C1-071238
2007-06	CP-36	CP-070380	1766	1	Management of GRUU	7.7.0	7.8.0	C1-071457
2007-06	CP-36	CP-070380	1711	2	Use of GRUU for Emergency Sessions	7.7.0	7.8.0	C1-071458
2007-06	CP-36	CP-070383	1773	-	IMS Communication Service ID registration	7.7.0	7.8.0	C1-071234
2007-06	CP-36	CP-070383	1645	6	IMS Communication Service ID 24.229	7.7.0	7.8.0	C1-071475
2007-06	CP-36	CP-070388	1735	2	Correction on the handlng of CPC parameter regarding trust domain	7.7.0	7.8.0	C1-071464
2007-06	CP-36	CP-070388	1662	-	Tidyup open issues from FBI work item	7.7.0	7.8.0	C1-070662
2007-06	CP-36	CP-070388	1596	5	Update to NAT Traversal procedures in support of Outbound and ICE	7.7.0	7.8.0	C1-071400
2007-06	CP-36	CP-070388	1740	1	IBCF processing of P-Early-Media	7.7.0	7.8.0	C1-071404
2007-06	CP-36	CP-070388	1742	1	IBCF Path header	7.7.0	7.8.0	C1-071405
2007-06	CP-36	CP-070436	1696	3	Endorsement of P-Early-Media header draft	7.7.0	7.8.0	
2007-06	CP-36	CP-070447	1698	3	Report of new transit scenario documented in stage 2	7.7.0	7.8.0	-
2007-06	CP-36	CP-070450	1771	3	THIG processing correction to ensure conformity to RFC 3261	7.7.0	7.8.0	-
2007-06	CP-36	CP-070496	1717	4	PCC impact	7.7.0	7.8.0	-
2007-06	CP-36	CP-070393	1751	1	Resource-Priority header and trust domains	7.7.0	8.0.0	C1-071446
2007-06	CP-36	CP-070393	1695	2	Inclusion policy for Resource-Priority header in support of multimedia priority	7.7.0	8.0.0	C1-071443

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					service			
2007-06	CP-36	CP-070393	1694	2	Inclusion of "communications resource priority for the session initiation protocol" (RFC4412) in the SIP profile	7.7.0	8.0.0	C1-071444
2007-06	CP-36	CP-070393	1693	1	Inclusion of "extending the session initiation protocol Reason header for preemption events" (RFC4411) in the SIP profile	7.7.0	8.0.0	C1-070918
2007-06	CP-36	CP-070396	1682	2	IMS Enhancements to Support Number Portability (NP) for Cable Networks	7.7.0	8.0.0	C1-070994
2007-06	CP-36	CP-070396	1681	4	Enhancements to Support Preferred Circuit Carrier Access and Dial-Around for Cable Networks	7.7.0	8.0.0	C1-071294
2007-09	CP-37	CP-070578	1945		Correction of the Authorization Header in the Profile Table	8.0.0	8.1.0	C1-072085
2007-09	CP-37	CP-070578	1811		Integrity param in De- and ReREGISTER	8.0.0	8.1.0	C1-071573
2007-09	CP-37	CP-070579	1905	2	Clarification of DTD	8.0.0	8.1.0	C1-072150
2007-09	CP-37	CP-070580	1795	2	Unprotected registration at UE	8.0.0	8.1.0	C1-072153
2007-09	CP-37	CP-070580	1876		IETF reference updates	8.0.0	8.1.0	C1-071772
2007-09	CP-37	CP-070580	1924	1	P-Access-Network-Info header clarification	8.0.0	8.1.0	C1-072042
2007-09	CP-37	CP-070580	1922	1	Optional rport parameter in UE	8.0.0	8.1.0	C1-072039
2007-09	CP-37	CP-070580	1797	1	Unprotected registration at S-CSCF	8.0.0	8.1.0	C1-072052
2007-09	CP-37	CP-070584	1866		Emergency Registration without eAPN	8.0.0	8.1.0	C1-071728
2007-09	CP-37	CP-070585	1878		IETF reference updates relating to emergency call feature	8.0.0	8.1.0	C1-071776
2007-09	CP-37	CP-070585	1892	1	Correction of emergency procedures unregistered user case	8.0.0	8.1.0	C1-072018
2007-09	CP-37	CP-070585	1894		Emergency registration timer in visited network	8.0.0	8.1.0	C1-071808
2007-09	CP-37	CP-070585	1927		Contents of From header when initiating an emergency session within a emergency registration	8.0.0	8.1.0	C1-071874
2007-09	CP-37	CP-070586	1861	1	Correction for the URNs of IMS Communication Service Identifier and IMS Application Reference Identifier	8.0.0	8.1.0	C1-071956
2007-09	CP-37	CP-070586	1909	2	Completing UE ICSI/IARI procedures	8.0.0	8.1.0	C1-072162
2007-09	CP-37	CP-070586	1842	1	S-CSCF option to add P-Asserted-Service in UE-originated case	8.0.0	8.1.0	C1-071952
2007-09	CP-37	CP-070586	1911	2	Completing S-CSCF ICSI/IARI procedures	8.0.0	8.1.0	C1-072164
2007-09	CP-37	CP-070586	1826	1	Cleanup of text related to contact header dealing with ICSI	8.0.0	8.1.0	C1-071942
2007-09	CP-37	CP-070586	1838	2	Description of the ICSI as an assigned identifier	8.0.0	8.1.0	C1-072159
2007-09	CP-37	CP-070586	1929	1	ICSI Alignments with reqs 2, 3 and 11	8.0.0	8.1.0	C1-071947
2007-09	CP-37	CP-070586	1942	1	UE usage of ServideID received from the network	8.0.0	8.1.0	C1-072181

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-09	CP-37	CP-070586	1840		Correction of application server handling of ICSI and IARI values	8.0.0	8.1.0	C1-071676
2007-09	CP-37	CP-070590	1807	3	Trust Domain in IMS	8.0.0	8.1.0	C1-072185
2007-09	CP-37	CP-070590	1799	1	Unprotected registration at P-CSCF	8.0.0	8.1.0	C1-072054
2007-09	CP-37	CP-070590	1793	1	Protected registration	8.0.0	8.1.0	C1-072046
2007-09	CP-37	CP-070590	1804	1	No multiple simultanous Registration	8.0.0	8.1.0	C1-072056
2007-09	CP-37	CP-070590	1864	1	Corrections of tables in Annex A	8.0.0	8.1.0	C1-072065
2007-09	CP-37	CP-070590	1879	1	Essential corrections to P-Early-Media header procedures	8.0.0	8.1.0	C1-072062
2007-09	CP-37	CP-070590	1881		IETF SigComp reference updates	8.0.0	8.1.0	C1-071779
2007-09	CP-37	CP-070590	1934		SIP related reference update	8.0.0	8.1.0	C1-071888
2007-09	CP-37	CP-070590	1913	1	Removal of IBCF Route Headers Editors Note	8.0.0	8.1.0	C1-072073
2007-09	CP-37	CP-070590	1854	1	Clarification on P-Profile-Key	8.0.0	8.1.0	C1-072063
2007-09	CP-37	CP-070592	1817		Resolve FFS for AS-GRUU	8.0.0	8.1.0	C1-071581
2007-09	CP-37	CP-070596	1885	2	Update Emergency NAT Traversal Procedures Annex K	8.0.0	8.1.0	C1-072078
2007-09	CP-37	CP-070596	1883	1	Update GRUU NAT Traversal Procedures Annex-K	8.0.0	8.1.0	C1-071926
2007-09	CP-37	CP-070600	1750	3	Resource-Priority and priority	7.8.0	8.1.0	C1-072132
2007-09	CP-37	CP-070600	1919	2	Addition of MGCF for optional support of Resource-Priority	8.0.0	8.1.0	C1-072184
2007-09	CP-37	CP-070601	1815	2	Updates to Annex K in support of SIP Digest and TLS procedures	8.0.0	8.1.0	C1-072137
2007-09	CP-37	CP-070601	1812	4	UE Digest and TLS Procedures	8.0.0	8.1.0	C1-072172
2007-09	CP-37	CP-070601	1814	4	S-CSCF Digest and TLS Procedures	8.0.0	8.1.0	C1-072174
2007-09	CP-37	CP-070601	1813	4	P-CSCF Digest and TLS Procedures	8.0.0	8.1.0	C1-072173
2007-09	CP-37	CP-070603	1847	1	Cleanup of SigComp dictionary support	8.0.0	8.1.0	C1-072144
2007-09	CP-37	CP-070603	1896	1	S-CSCF procedure corrections	8.0.0	8.1.0	C1-072089
2007-09	CP-37	CP-070603	1935		Restructuring of subclause 5.2.6 (General treatment for all dialogs and standalone transactions excluding the REGISTER method) of the P-CSCF	8.0.0	8.1.0	C1-071891
2007-09	CP-37	CP-070603	1788	2	Request-URI in registration	8.0.0	8.1.0	C1-072154
2007-09	CP-37	CP-070670	1907	3	Definition of feature tag for IARI/ICSI	8.0.0	8.1.0	C1-072006
2007-09	CP-37	CP-070674	1791	2	Emergency registration	8.0.0	8.1.0	C1-072016
2007-09	CP-37	CP-070676	1851	4	P-CSCF behaviour upon loss of SIP signalling transport	8.0.0	8.1.0	C1-072178
2007-09	CP-37	CP-070691	1926	5	UE setting of IARI	8.0.0	8.1.0	C1-072166
2007-12	CP-38	CP-070735	2077	1	Update P-Early-Media Reference	8.1.0	8.2.0	C1-072750
2007-12	CP-38	CP-070785	2065		Authenticating with AKAv1-MD5	8.1.0	8.2.0	C1-072533
2007-12	CP-38	CP-070785	2115		Proxy profile corrections	8.1.0	8.2.0	C1-072922

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-12	CP-38	CP-070785	2111		Corrections to RFC 3329 entries in profile	8.1.0	8.2.0	C1-072918
2007-12	CP-38	CP-070785	2041	1	Corrections for re-authenticating user	8.1.0	8.2.0	C1-072553
2007-12	CP-38	CP-070785	2049	3	Introduction of versioning and conventions	8.1.0	8.2.0	C1-072989
2007-12	CP-38	CP-070788	2028	1	Coverage of access technology specific text	8.1.0	8.2.0	C1-072746
2007-12	CP-38	CP-070788	2017	2	Action on missing "integrity-protected" parameter	8.1.0	8.2.0	C1-073179
2007-12	CP-38	CP-070788	2035	1	MGCF does not act as a proxy	8.1.0	8.2.0	C1-072565
2007-12	CP-38	CP-070788	2070	1	Correction to subclause 7.2A.5.2.2	8.1.0	8.2.0	C1-073052
2007-12	CP-38	CP-070791	1999	1	380 at normal call setup	8.1.0	8.2.0	C1-072670
2007-12	CP-38	CP-070791	2062	2	Miscellaneous EMC1 corrections	8.1.0	8.2.0	C1-072748
2007-12	CP-38	CP-070791	2120		Introductory text for emergency service	8.1.0	8.2.0	C1-072930
2007-12	CP-38	CP-070794	1990		Correct sub-section references in Annex-K	8.1.0	8.2.0	C1-072295
2007-12	CP-38	CP-070794	2023		Correction of outbound and ice option tag support in profile tables	8.1.0	8.2.0	C1-072383
2007-12	CP-38	CP-070795	1986	1	Align with draft-gruu-reg-ev-09	8.1.0	8.2.0	C1-072752
2007-12	CP-38	CP-070795	2043	1	Addition of GRUU to emergency set-up when registration exists	8.1.0	8.2.0	C1-072599
2007-12	CP-38	CP-070799	2067	1	P-CSCF Releases/Rejects session due to PCRF responses	8.1.0	8.2.0	C1-073067
2007-12	CP-38	CP-070805	2053	2	Terminating UE ICSI procedures	8.1.0	8.2.0	C1-072708
2007-12	CP-38	CP-070805	2021	1	Correction to digest and TLS Procedures for Annex K	8.1.0	8.2.0	C1-072508
2007-12	CP-38	CP-070805	1951	1	Correction to the examples for ICSI and IARI values	8.1.0	8.2.0	C1-072490
2007-12	CP-38	CP-070805	2014	2	Encoding of ICSI and IARI within the g.ims.app_ref feature tag	8.1.0	8.2.0	C1-072704
2007-12	CP-38	CP-070805	2051	1	Multiple IARI/ICSI values in g.ims.app_ref feature tag	8.1.0	8.2.0	C1-072512
2007-12	CP-38	CP-070805	1969	1	One ICSI value per P-Preferred-Service header	8.0.0	8.2.0	C1-072496
2007-12	CP-38	CP-070805	1963	1	Change of name for feature tag g.ims.app_ref	8.0.0	8.2.0	C1-072492
2007-12	CP-38	CP-070806	2008	2	Handling of invalid and unauthorized media based on Communication Service Identifiers	8.1.0	8.2.0	C1-072702
2007-12	CP-38	CP-070806	2092	2	S-CSCF Processing of P-Preferred-Service and P-Asserted-Service	8.1.0	8.2.0	C1-073204
2007-12	CP-38	CP-070806	2107	2	The received list of ICSIs from the Network	8.1.0	8.2.0	C1-073206
2007-12	CP-38	CP-070806	2088		ICSI in Annex F	8.1.0	8.2.0	C1-072841
2007-12	CP-38	CP-070806	2019	2	Miscellaneous service identifier corrections	8.1.0	8.2.0	C1-073106
2007-12	CP-38	CP-070806	1965	3	Minor corrections to P-Preferred and P-Asserted Service headers	8.1.0	8.2.0	C1-073102
2007-12	CP-38	CP-070806	1976	2	Correction to S-CSCF handling of IMS	8.1.0	8.2.0	C1-072700

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					communication service			
2007-12	CP-38	CP-070807	2005	1	No SIPS	8.1.0	8.2.0	C1-072593
2007-12	CP-38	CP-070807	1961	1	Route header verification at P-CSCF	8.1.0	8.2.0	C1-072587
2007-12	CP-38	CP-070807	1955	1	Update of the reference for P-Profile-Key Private Header (P-Header)	8.1.0	8.2.0	C1-072487
2007-12	CP-38	CP-070807	2012		Reference alignment	8.1.0	8.2.0	C1-072364
2007-12	CP-38	CP-070807	2037	1	AS does not subscribe to reg-event package when user is unregistered	8.1.0	8.2.0	C1-072597
2007-12	CP-38	CP-070807	2045	2	Correction of mutually exclusive ICSI and GRUU	8.1.0	8.2.0	C1-072706
2007-12	CP-38	CP-070807	2055		Update of P-Answer-State header draft Reference	8.1.0	8.2.0	C1-072446
2007-12	CP-38	CP-070808	2057	2	Clarification of UE handling of the P-Early-Media header.	8.1.0	8.2.0	C1-072723
2007-12	CP-38	CP-070808	2100	1	Access Network Info for I-WLAN	8.1.0	8.2.0	C1-073075
2007-12	CP-38	CP-070808	2003	2	Service Profile Change	8.1.0	8.2.0	C1-072718
2007-12	CP-38	CP-070808	1957	4	Correction to the IBCF subsection in relation with trusted domain	8.1.0	8.2.0	C1-072687
2007-12	CP-38	CP-070808	2072	2	Correction to procedure when registration timer times out	8.1.0	8.2.0	C1-073173
2007-12	CP-38	CP-070808	2103	1	Access Network Info for 3GPP2/UMB	8.1.0	8.2.0	C1-073057
2007-12	CP-38	CP-070810	2081	3	Correction of multiple Contact headers in abnormal case	8.1.0	8.2.0	C1-073226
2007-12	CP-38	CP-070810	2117	1	Miscellaneous editorial corrections (part 3)	8.1.0	8.2.0	C1-073165
2007-12	CP-38	CP-070810	1932	4	Incorporation of draft-ietf-consent-framework	8.1.0	8.2.0	C1-073166
2007-12	CP-38	CP-070810	2098	1	Superfluous requirements for removing charging information at terminating P-CSCF	8.1.0	8.2.0	C1-073164
2007-12	CP-38	CP-070810	1974	1	Synchronization When Service Profile Being Modified	8.1.0	8.2.0	C1-072661
2007-12	CP-38	CP-070810	2029	3	Miscellaneous editorial corrections	8.1.0	8.2.0	C1-072764
2007-12	CP-38	CP-070810	2059	3	Miscellaneous editorial corrections (part 2)	8.1.0	8.2.0	C1-073162
2007-12	CP-38	CP-070811	2078	1	Clarification on interconnect functionalities	8.1.0	8.2.0	C1-073163
2007-12	CP-38	CP-070812	2086	1	Semantics for values in "integrity-protected" field	8.1.0	8.2.0	C1-073112
2007-12	CP-38	CP-070812	2060	3	Public user identity and private user identity derivation in UEs without UICC	8.1.0	8.2.0	C1-073201
2007-12	CP-38	CP-070812	2006	1	Digest Support in Profile Tables	8.1.0	8.2.0	C1-072623
2007-12	CP-38	CP-070812	2026	1	Security-related references and definitions	8.1.0	8.2.0	C1-072761
2007-12	CP-38	CP-070812	2025	3	Introduction to security mechanisms	8.1.0	8.2.0	C1-073175
2007-12	CP-38	CP-070812	1982	6	Updates to integrity protection for digest and TLS	8.1.0	8.2.0	C1-073202
2007-12	CP-38	CP-070814	2085	4	Addition of SIP header to support UUS1	8.1.0	8.2.0	C1-073208

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2007-12	CP-38	CP-070816	2024	5	Integration of text for digest and TLS plus digest into the main body of the specification	8.1.0	8.2.0	C1-073200
2007-12	CP-38	CP-070864	1953	5	Clarifications on NW-init and resource reservation	8.1.0	8.2.0	C1-073069
2007-12	CP-38	CP-070875	1997	4	Corrections for emergency procedures	8.1.0	8.2.0	C1-072991
2008-03	CP-39	CP-080120	2174		Reference correction for RFC 4244	8.2.0	8.3.0	C1-080147
2008-03	CP-39	CP-080120	2149		Handling of the reason header in requests at the MGCF	8.2.0	8.3.0	C1-080045
2008-03	CP-39	CP-080120	2162	1	Correction on handling of P-Charging-Vector at IBCF	8.2.0	8.3.0	C1-080515
2008-03	CP-39	CP-080120	2181	1	Correction of Alias	8.2.0	8.3.0	C1-080517
2008-03	CP-39	CP-080120	2176		SDP with precondition	8.2.0	8.3.0	C1-080149
2008-03	CP-39	CP-080126	2201	2	Handling of Service ID in interworking cases	8.2.0	8.3.0	C1-080630
2008-03	CP-39	CP-080126	2155	2	Clarification on the use of IARI in the contact header	8.2.0	8.3.0	C1-080635
2008-03	CP-39	CP-080126	2183	2	UE behaviour when no ICSI is contained in the Accept-Contact header	8.2.0	8.3.0	C1-080531
2008-03	CP-39	CP-080130	2143	1	Procedure at S-CSCF	8.2.0	8.3.0	C1-080600
2008-03	CP-39	CP-080130	2144		Empty RES	8.2.0	8.3.0	C1-080009
2008-03	CP-39	CP-080130	2145	1	Alias URI	8.2.0	8.3.0	C1-080601
2008-03	CP-39	CP-080130	2146	2	Notification at S-CSCF	8.2.0	8.3.0	C1-080631
2008-03	CP-39	CP-080130	2156	1	Correction of example of IARI coding	8.2.0	8.3.0	C1-080526
2008-03	CP-39	CP-080130	2160	1	Correction on the value used for P-Preferred-Identity header at UE	8.2.0	8.3.0	C1-080513
2008-03	CP-39	CP-080130	2170	1	Correction to user initiated mergency re-registration	8.2.0	8.3.0	C1-080405
2008-03	CP-39	CP-080130	2187	1	IPv4 and IPv6 support	8.2.0	8.3.0	C1-080609
2008-03	CP-39	CP-080130	2188	4	P-CSCF awareness for 3GPP accesses	8.2.0	8.3.0	C1-080658
2008-03	CP-39	CP-080130	2196	2	Annex K: ICE procedures for the IBCF	8.2.0	8.3.0	C1-080643
2008-03	CP-39	CP-080131	2192	1	Completion of CIC and DAI requirements for MGCF	8.2.0	8.3.0	C1-080472
2008-03	CP-39	CP-080132	2163	1	Miscelanous Corrections on SIP Digest	8.2.0	8.3.0	C1-080473
2008-03	CP-39	CP-080132	2189	1	Enhancements to security introduction text	8.2.0	8.3.0	C1-080474
2008-03	CP-39	CP-080134	2190	1	Inclusion of NASS bundled authentication	8.2.0	8.3.0	C1-080518
2008-03	CP-39	CP-080139	2164	1	SIP XML addition for support of transit specific content	8.2.0	8.3.0	C1-080533
2008-03	CP-39	CP-080140	2138	2	IP-CAN procedure for cdma2000	8.2.0	8.3.0	C1-080411
2008-03	CP-39	CP-080140	2141	2	P-CSCF interface to IP-CAN	8.2.0	8.3.0	C1-080413
2008-03	CP-39	CP-080140	2140	2	Access-network-charging-info for cdma2000 access	8.2.0	8.3.0	C1-080412
2008-03	CP-39	CP-080141	2197	1	Wildcarded Public User Identity: P-CSCF	8.2.0	8.3.0	C1-080612

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					impact			
2008-03	CP-39	CP-080141	2198	2	Wildcarded Public User Identity: S-CSCF impact	8.2.0	8.3.0	C1-080644
2008-03	CP-39	CP-080199	2147	4	NAT traversal	8.2.0	8.3.0	
2008-03	CP-39	CP-080201	2151	5	Handling of the reason header in responses	8.2.0	8.3.0	
2008-06	CP-40	CP-080338	2288	1	Correction to de-registration procedure when registration expirated	8.3.0	8.4.0	C1-081936
2008-06	CP-40	CP-080340	2215	-	Revision of references to documents from IETF ECRIT working group	8.3.0	8.4.0	C1-080854
2008-06	CP-40	CP-080341	2243	1	Correction to P-CSCF session release procedures	8.3.0	8.4.0	C1-081336
2008-06	CP-40	CP-080341	2275	2	Addition of AVPF support	8.3.0	8.4.0	C1-082022
2008-06	CP-40	CP-080341	2258	1	Correction on identifiers distinguishing the dialog	8.3.0	8.4.0	C1-081338
2008-06	CP-40	CP-080341	2238	1	Removal of reason header annex	8.3.0	8.4.0	C1-081334
2008-06	CP-40	CP-080341	2217	-	Revision of references to documents from IETF	8.3.0	8.4.0	C1-080858
2008-06	CP-40	CP-080341	2277	1	Addition of the SDP Capability Negotiaion mechanism	8.3.0	8.4.0	C1-081932
2008-06	CP-40	CP-080343	2158	6	Handling of SDP at the terminating UE	8.3.0	8.4.0	C1-082050
2008-06	CP-40	CP-080344	2290	-	Correction of GRUU references	8.3.0	8.4.0	C1-081799
2008-06	CP-40	CP-080349	2236	-	Revision of references to documents from IETF SIP working group	8.3.0	8.4.0	C1-080860
2008-06	CP-40	CP-080353	2203	1	Emergency calls - NAT traversal at UE	8.3.0	8.4.0	C1-081228
2008-06	CP-40	CP-080353	2204	1	NAT traversal for emergency calls at P-CSCF	8.3.0	8.4.0	C1-081229
2008-06	CP-40	CP-080353	2220	1	PANI header text revision	8.3.0	8.4.0	C1-081346
2008-06	CP-40	CP-080353	2225	1	Addition of 802.11n to P-Access-Network-Info header	8.3.0	8.4.0	C1-081348
2008-06	CP-40	CP-080353	2205	3	"im" URI	8.3.0	8.4.0	C1-081411
2008-06	CP-40	CP-080353	2254	2	Annex K: Moving of IBCF ICE procedures	8.3.0	8.4.0	C1-081469
2008-06	CP-40	CP-080353	2168	9	Correction of 3GPP IM CN subsystem XML handling	8.3.0	8.4.0	C1-081481
2008-06	CP-40	CP-080353	2221	1	Media transcoding control functionality in IBCF	8.3.0	8.4.0	C1-081347
2008-06	CP-40	CP-080353	2219	1	PANI header coding	8.3.0	8.4.0	C1-081345
2008-06	CP-40	CP-080353	2209	1	Alias URI	8.3.0	8.4.0	C1-081343
2008-06	CP-40	CP-080353	2136	7	3GPP IM CN subsystem XML Schema version	8.3.0	8.4.0	C1-081480
2008-06	CP-40	CP-080353	2255	3	Annex K: ICE procedures for the P-CSCF	8.3.0	8.4.0	C1-081470
2008-06	CP-40	CP-080354	2284	2	SDP Enhancements to support resource allocation	8.3.0	8.4.0	C1-082045
2008-06	CP-40	CP-080354	2218	2	B2BUA AS influence of filter criteria	8.3.0	8.4.0	C1-082033

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
					evaluation			
2008-06	CP-40	CP-080354	2263	1	Multiple contact addresses	8.3.0	8.4.0	C1-082041
2008-06	CP-40	CP-080354	2280	-	Annex A : SIP Record-Route header table correction	8.3.0	8.4.0	C1-081605
2008-06	CP-40	CP-080354	2206	2	"rport" and "received" parameters at P-CSCF	8.3.0	8.4.0	C1-081871
2008-06	CP-40	CP-080354	2282	1	Display Name in Reg Event	8.3.0	8.4.0	C1-082027
2008-06	CP-40	CP-080354	2285	-	Update IETF draft reference	8.3.0	8.4.0	C1-081701
2008-06	CP-40	CP-080354	2207	2	UE handling the "rport" parameter	8.3.0	8.4.0	C1-081872
2008-06	CP-40	CP-080355	2234	4	Annex K alignment with main body and cleanup	8.3.0	8.4.0	C1-082043
2008-06	CP-40	CP-080355	2291	1	Determining when to invoke SIP Digest procedures in S-CSCF	8.3.0	8.4.0	C1-081944
2008-06	CP-40	CP-080355	2269	1	Cleanup of SIP Digest/TLS procedures	8.3.0	8.4.0	C1-081942
2008-06	CP-40	CP-080359	2260	2	P-CSCF: Aligning P-Profile-Key behaviour for Wildcarded public user identities with Wildcarded PSI	8.3.0	8.4.0	C1-081476
2008-06	CP-40	CP-080359	2212	4	Dial string handling	8.3.0	8.4.0	C1-082110
2008-06	CP-40	CP-080359	2261	2	Trustdomain: Adding P-Profile-Key header to the trustdomain	8.3.0	8.4.0	C1-081477
2008-06	CP-40	CP-080359	2239	1	Trust domain changes for identity headers for business communication	8.3.0	8.4.0	C1-081206
2008-06	CP-40	CP-080359	2259	2	I-CSCF: Aligning P-Profile-Key behaviour for Wildcarded public user identities with Wildcarded PSI procedures	8.3.0	8.4.0	C1-081475
2008-06	CP-40	CP-080359	2232	2	Delivering Request-URI to UE managing several terminals	8.3.0	8.4.0	C1-081474
2008-06	CP-40	CP-080359	2262	-	Private network indication annex A changes	8.3.0	8.4.0	C1-081210
2008-06	CP-40	CP-080359	2240	3	Handling of private network indication	8.3.0	8.4.0	C1-081953
2008-06	CP-40	CP-080360	2273	1	Event package usage for Message Waiting Indication (MWI) service	8.3.0	8.4.0	C1-081901
2008-06	CP-40	CP-080360	2226	3	XML-support of transit specific content Tables	8.3.0	8.4.0	C1-081905
2008-06	CP-40	CP-080364	2222	3	Depth of IMS service level trace	8.3.0	8.4.0	C1-081955
2008-06	CP-40	CP-080366	2252	1	Emergency CS call set up procedures for non-3GPP systems	8.3.0	8.4.0	C1-081465
2008-06	CP-40	CP-080366	2268	1	Different IP addresses	8.3.0	8.4.0	C1-081945
2008-06	CP-40	CP-080366	2251	1	Remove specific codec requirement	8.3.0	8.4.0	C1-081464
2008-06	CP-40	CP-080400	2208	2	"rport" parameter	8.3.0	8.4.0	-
2008-06	CP-40	CP-080402	2296	-	IARI and ICSI in different feature tags	8.3.0	8.4.0	-
2008-06	CP-40	CP-080417	2211	5	Call forwarding in IMS	8.3.0	8.4.0	-
2008-06					Editorial change done by MCC	8.4.0	8.4.1	
2008-09	CP-41	CP-080643	2177	7	Allow Multiple Registrations in Rel 8 by	8.4.1	8.5.0	

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					using Outbound			
2008-09	CP-41	CP-080539	2178	6	Add Timestamp in Register Request	8.4.1	8.5.0	C1-082810
2008-09	CP-41	CP-080527	2297	1	Cleanup of P-CSCF procedures for inclusion of "tls-yes" and "tls-pending"	8.4.1	8.5.0	C1-082623
2008-09	CP-41	CP-080538	2298	1	Introduction of GIBA (Early IMS) procedures	8.4.1	8.5.0	C1-082657
2008-09	CP-41	CP-080527	2299	1	Add reference to draft-dotson-sip-mutual-auth	8.4.1	8.5.0	C1-082621
2008-09	CP-41	CP-080523	2301	1	Correction of DHCP reference	8.4.1	8.5.0	C1-082620
2008-09	CP-41	CP-080523	2302		Reference correction	8.4.1	8.5.0	C1-082142
2008-09	CP-41	CP-080515	2306	1	Annex A: Correction of SDP connection information	8.4.1	8.5.0	C1-082611
2008-09	CP-41	CP-080523	2308	1	Backward compability issue with P-Access-Network-Info ABNF extension	8.4.1	8.5.0	C1-082625
2008-09	CP-41	CP-080517	2314		Addition of AVPF support and SDP capability negotiation mechanism	8.4.1	8.5.0	C1-082268
2008-09	CP-41	CP-080520	2316		Profile corrections for outbound	8.4.1	8.5.0	C1-082270
2008-09	CP-41	CP-080531	2319		Support of Direct Ethernet access as IP-CAN	8.4.1	8.5.0	C1-082324
2008-09	CP-41	CP-080520	2323	1	Update Outbound Reference	8.4.1	8.5.0	C1-082626
2008-09	CP-41	CP-080523	2325	2	Error Response for Different S-CSCF Assignment	8.4.1	8.5.0	C1-082770
2008-09	CP-41	CP-080527	2328	1	Annex K Technical Corrections	8.4.1	8.5.0	C1-082622
2008-09	CP-41	CP-080528	2329	1	Adding P-Debug-ID to SIP Profile Tables	8.4.1	8.5.0	C1-082752
2008-09	CP-41	CP-080528	2330	2	Subscribing to the debug event package	8.4.1	8.5.0	C1-082781
2008-09	CP-41	CP-080522	2331	4	EPS as IP-CAN	8.4.1	8.5.0	C1-083637
2008-09	CP-41	CP-080523	2333	2	Alignment of IP-CAN specific annexes	8.4.1	8.5.0	C1-082778
2008-09	CP-41	CP-080516	2336		Emergency PUID	8.4.1	8.5.0	C1-082864
2008-09	CP-41	CP-080667	2340	3	Initial emergency registration	8.4.1	8.5.0	
2008-09	CP-41	CP-080516	2342	2	Emergency session set-up	8.4.1	8.5.0	C1-083532
2008-09	CP-41	CP-080516	2344	1	P-CSCF handling of emergency sessions	8.4.1	8.5.0	C1-083391
2008-09	CP-41	CP-080516	2346	3	S-CSCF handling of emergency registration	8.4.1	8.5.0	C1-083534
2008-09	CP-41	CP-080523	2347	1	Informative Explanation and Corrections of Profile Tables	8.4.1	8.5.0	C1-083353
2008-09	CP-41	CP-080523	2350	1	More than one contact address per UE	8.4.1	8.5.0	C1-083351
2008-09	CP-41	CP-080528	2351	1	IMS Trace for entities not on the path of the register request	8.4.1	8.5.0	C1-083383
2008-09	CP-41	CP-080528	2352	1	Start and stop procedures for IMS trace	8.4.1	8.5.0	C1-083384
2008-09	CP-41	CP-080636	2353	1	Align emergency session handling outside a security association or TLS session	8.4.1	8.5.0	
2008-09	CP-41	CP-080637	2354	3	Addressing privacy requirement	8.4.1	8.5.0	

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2008-09	CP-41	CP-080523	2359	2	SDP Offer	8.4.1	8.5.0	C1-083398
2008-09	CP-41	CP-080515	2362		SDP referencing error for IBCF (IMS-ALG)	8.4.1	8.5.0	C1-082927
2008-09	CP-41	CP-080523	2363	2	Addition of draft-ietf-sip-199-00	8.4.1	8.5.0	C1-083399
2008-09	CP-41	CP-080523	2365	1	Usage of draft-holmberg-sip-keep-01 for emergency session	8.4.1	8.5.0	C1-083395
2008-09	CP-41	CP-080537	2366	1	Mediactrl and netann specifications	8.4.1	8.5.0	C1-083363
2008-09	CP-41	CP-080536	2369	1	S-CSCF and AS procedures with Enhanced Filter Criteria	8.4.1	8.5.0	C1-083501
2008-09	CP-41	CP-080617	2371	2	Correct handling for <reason> element	8.4.1	8.5.0	
2008-09	CP-41	CP-080539	2375		Modification of ci-3gpp2 parameter	8.4.1	8.5.0	C1-083200
2008-09	CP-41	CP-080668	2377	3	Alignment of usage of terms ISIM and ISIM Application	8.4.1	8.5.0	
2008-09	CP-41	CP-080524	2378	1	Introduction additional methods of P-CSCF discovery to support IMS Local Breakout	8.4.1	8.5.0	C1-083400
2008-09	CP-41	CP-080515	2381		Alignment with current version of draft-ietf-sip-fork-loop-fix	8.4.1	8.5.0	C1-083246
2008-09	CP-41	CP-080522	2386	1	Relationship to IP-CAN	8.4.1	8.5.0	C1-083424
2008-09					Editorial change done by MCC	8.5.0	8.5.1	
2008-12	CP-42	CP-080942	2324	9	Introduction of IMC in support of common IMS	8.5.1	8.6.0	-
2008-12	CP-42	CP-080847	2327	5	SDP Enhancements to support resource allocation	8.5.1	8.6.0	C1-084937
2008-12	CP-42	CP-080840	2332	3	Additional changes for private network indication	8.5.1	8.6.0	C1-084441
2008-12	CP-42	CP-080847	2358	7	Prevent DDOS attack on PSAP	8.5.1	8.6.0	C1-085454
2008-12	CP-42	CP-080840	2383	1	Modifications to private network indication in profile	8.5.1	8.6.0	C1-084080
2008-12	CP-42	CP-080847	2388	3	Annex A fixes regarding draft-ietf-sip-199	8.5.1	8.6.0	C1-085202
2008-12	CP-42	CP-080847	2389	1	Annex A fixes regarding draft-holmberg-sip-keep	8.5.1	8.6.0	C1-084278
2008-12	CP-42	CP-080847	2394	-	Correction on setting P-Served-User	8.5.1	8.6.0	C1-083694
2008-12	CP-42	CP-080847	2396	1	Clarification on ICSI and IARI	8.5.1	8.6.0	C1-084203
2008-12	CP-42	CP-080847	2402	2	Interface identifier	8.5.1	8.6.0	C1-085204
2008-12	CP-42	CP-080844	2403	2	UE subscription to reg-evet	8.5.1	8.6.0	C1-084420
2008-12	CP-42	CP-080844	2405	3	UE - multiple contacts registration	8.5.1	8.6.0	C1-085205
2008-12	CP-42	CP-080844	2406	1	UE - multiple contacts authentication and deregistration	8.5.1	8.6.0	C1-084282
2008-12	CP-42	CP-080844	2407	1	UE using multiple contacts	8.5.1	8.6.0	C1-084283
2008-12	CP-42	CP-080845	2408	4	Introduction of additional methods of P-CSCF discovery for EPS to support IMS Local Breakout	8.5.1	8.6.0	C1-085206
2008-12	CP-42	CP-080956	2409	5	UE procedures when multiple P-CSCF discovery procedures are supported	8.5.1	8.6.0	-

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2008-12	CP-42	CP-080854	2411	1	Cr addition to section 4	8.5.1	8.6.0	C1-084230
2008-12	CP-42	CP-080854	2412	2	Netann, mediactrl text improvements	8.5.1	8.6.0	C1-084434
2008-12	CP-42	CP-080854	2413	2	Media control for charging, delegation	8.5.1	8.6.0	C1-085256
2008-12	CP-42	CP-080847	2421	-	Trademark CDMA terminology	8.5.1	8.6.0	C1-083983
2008-12	CP-42	CP-080843	2423	2	Aligning initial INVITE request usage of Accept header field and profile tables	8.5.1	8.6.0	C1-084438
2008-12	CP-42	CP-080858	2424	1	Clarification of security-verify for TLS	8.5.1	8.6.0	C1-084234
2008-12	CP-42	CP-080840	2425	2	Setting of the Phone-contex paramater when IP-CAN is Ethernet	8.5.1	8.6.0	C1-085201
2008-12	CP-42	CP-080847	2427	-	P-CSCF call release upon reception of indication that no ressource is available.	8.5.1	8.6.0	C1-084024
2008-12	CP-42	CP-080847	2428	2	Removing of the cpc parameter by the terminating S-CSCF removes CPC	8.5.1	8.6.0	C1-084435
2008-12	CP-42	CP-080844	2430	2	Clarification of abnormal case for deregistration	8.5.1	8.6.0	C1-085158
2008-12	CP-42	CP-080847	2431	-	P-CSCF handling of “integrity-protected”	8.5.1	8.6.0	C1-084048
2008-12	CP-42	CP-080839	2432	2	Registration Procedure for ICS	8.5.1	8.6.0	C1-085200
2008-12	CP-42	CP-080870	2434	1	SMSIP related changes for the profile tables	8.5.1	8.6.0	C1-084202
2008-12	CP-42	CP-080853	2435	1	Adding roles defined for service level interworking for messaging to the profile table	8.5.1	8.6.0	C1-084270
2008-12	CP-42	CP-080840	2436	-	Downloading of information to the P-CSCF	8.5.1	8.6.0	C1-084082
2008-12	CP-42	CP-080835	2440	2	Adding reference to Internet Draft on sos URI parameter for emergency calls	8.5.1	8.6.0	C1-085260
2008-12	CP-42	CP-080857	2441	-	Update reference for DAI Parameter for the "tel" URI	8.5.1	8.6.0	C1-084120
2008-12	CP-42	CP-080847	2442	3	Inclusion of draft-ietf-sip-body-handling in the profile tables	8.5.1	8.6.0	C1-085209
2008-12	CP-42	CP-080856	2443	3	Deterministic Routeing for overlap signalling	8.5.1	8.6.0	C1-085239
2008-12	CP-42	CP-080840	2444	1	Allowing P-Asserted Identity from an UE	8.5.1	8.6.0	C1-085254
2008-12	CP-42	CP-080835	2446	-	Emergency call	8.5.1	8.6.0	C1-084649
2008-12	CP-42	CP-080843	2448	1	Deregistration in 200 (OK)	8.5.1	8.6.0	C1-085435
2008-12	CP-42	CP-080939	2449	2	Revision of 24.229-2449r1 (C1-085416)	8.5.1	8.6.0	-
2008-12	CP-42	CP-080844	2450	2	Usage of outbound in call setup	8.5.1	8.6.0	C1-085450
2008-12	CP-42	CP-080844	2451	-	Multiple registrations at P-CSCF	8.5.1	8.6.0	C1-084655
2008-12	CP-42	CP-080940	2452	2	Revision of 24.229-2452r1 (C1-085418)	8.5.1	8.6.0	-
2008-12	CP-42	CP-080844	2454	1	Multiple registrations at S-CSCF	8.5.1	8.6.0	C1-085419
2008-12	CP-42	CP-080869	2456	-	Correction of ICSI and IARI feature tag name	8.5.1	8.6.0	C1-084689
2008-12	CP-42	CP-080862	2457	2	Inclusion and Modification of Resource-Priority header at P-CSCF	8.5.1	8.6.0	C1-085451

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2008-12	CP-42	CP-080854	2458	1	Media control related profile table updates	8.5.1	8.6.0	C1-085255
2008-12	CP-42	CP-080854	2459	1	Mediactrl reference updates	8.5.1	8.6.0	C1-085257
2008-12	CP-42	CP-080839	2460	2	Instance ID definition	8.5.1	8.6.0	C1-085459
2008-12	CP-42	CP-080844	2462	2	GRUU and Multilple registration	8.5.1	8.6.0	C1-085468
2008-12	CP-42	CP-080959	2464	4	Overlap signalling procedures	8.5.1	8.6.0	-
2008-12	CP-42	CP-080841	2469	-	Reference updates (release 6 ietf dependencies)	8.5.1	8.6.0	C1-084898
2008-12	CP-42	CP-080843	2471	-	Reference updates (release 7 ietf dependencies)	8.5.1	8.6.0	C1-084903
2008-12	CP-42	CP-080858	2472	1	No domain field for SIP digest	8.5.1	8.6.0	C1-085261
2008-12	CP-42	CP-080858	2473	1	Digest Authentication of Non-Register requests	8.5.1	8.6.0	C1-085262
2008-12	CP-42	CP-080855	2477	1	Minor corrections to configuration of entities for trace	8.5.1	8.6.0	C1-085128
2008-12	CP-42	CP-080843	2479	-	Inclusion of missing RFC 3351 reference	8.5.1	8.6.0	C1-085011
2008-12	CP-42	CP-080847	2480	2	Documentation of INFO within the IM CN subsystem	8.5.1	8.6.0	C1-085424
2008-12	CP-42	CP-080847	2481	-	Removal of TrGw normative requirements from IBCF	8.5.1	8.6.0	C1-085015
2008-12	CP-42	CP-080847	2482	-	Editorial consistency and best practice	8.5.1	8.6.0	C1-085016
2008-12	CP-42	CP-080965	2483	3	Updates to profile tables to include ICS additions	8.5.1	8.6.0	-
2008-12	CP-42	CP-080849	2484	-	Cleanup of various GIBA Editor's notes	8.5.1	8.6.0	C1-085025
2008-12	CP-42	CP-080853	2485	1	Addition of cpim/message and message/imdn+xml	8.5.1	8.6.0	C1-085291
2008-12	CP-42	CP-080847	2494	3	Documenting RFC 5373	8.5.1	8.6.0	C1-085483
2008-12	CP-42	CP-080873	2495	1	S-CSCF and AS procedures with Enhanced Filter Criteria	8.5.1	8.6.0	C1-085292
2008-12	CP-42	CP-080847	2498	2	Call release by the P-CSCF upon resource reservation faillure	8.5.1	8.6.0	C1-085467
2008-12	CP-42	CP-080847	2499	1	Hosted NAT traversal for media flows	8.5.1	8.6.0	C1-085430
2008-12	CP-42	CP-080846	2501	1	Reference updates (release 8 ietf dependencies)	8.5.1	8.6.0	C1-085426
2008-12	CP-42	CP-080847	2502	-	Corrections to security overview	8.5.1	8.6.0	C1-085093
2008-12	CP-42	CP-080847	2505	-	Identification of public user identity in absence of Authorization header	8.5.1	8.6.0	C1-085131
2008-12	CP-42				Editorial cleanup by ETSI EditHelp! and MCC	8.5.1	8.6.0	
2009-03	CP-43	CP-090134	2438	7	Correction of non UE detectable emergency call procedures	8.6.0	8.7.0	C1-091088
2009-03	CP-43	CP-090121	2507		Correction of URN-value for Service Identifiers	8.6.0	8.7.0	C1-090012
2009-03	CP-43	CP-090134	2508	1	Re-selection of S-CSCF during Terminating and Originating Procedures	8.6.0	8.7.0	C1-090991

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2009-03	CP-43	CP-090146	2509	2	Re-selection of S-CSCF during Terminating and Originating Procedures when restoration is supported.	8.6.0	8.7.0	C1-091066
2009-03	CP-43	CP-090245	2510	4	Returning an error to trigger a new registration when IMS restoration is supported	8.6.0	8.7.0	-
2009-03	CP-43	CP-090225	2511	4	Re-selection of S-CSCF during Re-registration when IMS restoration is supported	8.6.0	8.7.0	-
2009-03	CP-43	CP-090134	2514	1	Outbound with IMS AKA	8.6.0	8.7.0	C1-090992
2009-03	CP-43	CP-090134	2515	2	Registration procedure at the S-CSCF	8.6.0	8.7.0	C1-091041
2009-03	CP-43	CP-090134	2516	3	P-CSCFprocessing 200 (OK)	8.6.0	8.7.0	C1-091085
2009-03	CP-43	CP-090134	2517	4	Multiple de-registrations	8.6.0	8.7.0	C1-091111
2009-03	CP-43	CP-090134	2519	1	Instance-ID in INVITE	8.6.0	8.7.0	C1-090997
2009-03	CP-43	CP-090134	2520		Multiple contact addresses	8.6.0	8.7.0	C1-090042
2009-03	CP-43	CP-090130	2524	3	Support for eHRPD	8.6.0	8.7.0	C1-091381
2009-03	CP-43	CP-090155	2525	1	Adding the role of The Early Session Disposition Type	8.6.0	8.7.0	C1-090950
2009-03	CP-43	CP-090134	2527		Cleanup inclusion of draft-ietf-sip-body-handling in the profile tables	8.6.0	8.7.0	C1-090201
2009-03	CP-43	CP-090116	2529	2	Aligning with draft-ietf-sip-location-conveyance-12	8.6.0	8.7.0	C1-091040
2009-03	CP-43	CP-090134	2530	1	Addressing privacy requirement for emergency calls	8.6.0	8.7.0	C1-090999
2009-03	CP-43	CP-090116	2532	1	Correcting condition for using indicating use of emergency registration	8.6.0	8.7.0	C1-090959
2009-03	CP-43	CP-090224	2534	3	Overlap signalling en-bloc conversion procedures	8.6.0	8.7.0	-
2009-03	CP-43	CP-090209	2535	3	Overlap signalling digit collection procedures	8.6.0	8.7.0	-
2009-03	CP-43	CP-090134	2537	1	Correction of registration duration value	8.6.0	8.7.0	C1-091024
2009-03	CP-43	CP-090127	2540	1	Corrections to E-UTRAN specific aspects	8.6.0	8.7.0	C1-090850
2009-03	CP-43	CP-090134	2541		Miscellaneous corrections to annex B	8.6.0	8.7.0	C1-090377
2009-03	CP-43	CP-090142	2543	1	Miscellaneous corrections to Annex M	8.6.0	8.7.0	C1-090985
2009-03	CP-43	CP-090142	2544	1	Phone-context parameter value for cdma2000®	8.6.0	8.7.0	C1-090986
2009-03	CP-43	CP-090142	2545	1	Common IMS for MGW and MRF	8.6.0	8.7.0	C1-090987
2009-03	CP-43	CP-090134	2546	4	Deterministic behaviour for Call Forwarding	8.6.0	8.7.0	C1-091122
2009-03	CP-43	CP-090136	2547	1	Overlap Corrections	8.6.0	8.7.0	C1-090962
2009-03	CP-43	CP-090116	2550	1	Alignment of emergency indication with draft-patel-ecrit-sos-parameter-03	8.6.0	8.7.0	C1-090968
2009-03	CP-43	CP-090272	2553	3	Use of multiple access technologies in IMS	8.6.0	8.7.0	-
2009-03	CP-43	CP-090134	2555		Alignment of authentication parameter terminology	8.6.0	8.7.0	C1-090534

Change history								
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**	**WG doc**
2009-03	CP-43	CP-090134	2556		Use of access-class and access-type constructs in the P-Access-Network-Info header field	8.6.0	8.7.0	C1-090535
2009-03	CP-43	CP-090134	2558		P-Served-User header field corrections (profile)	8.6.0	8.7.0	C1-090537
2009-03	CP-43	CP-090134	2560		Editorial consistency and best practice	8.6.0	8.7.0	C1-090539
2009-03	CP-43	CP-090141	2561	1	Removal of redundant NASS bundled authentication text for S-CSCF	8.6.0	8.7.0	C1-090969
2009-03	CP-43	CP-090150	2564	1	Emergency call handling for CS media	8.6.0	8.7.0	C1-090908
2009-03	CP-43	CP-090118	2574	2	Correction to Annex A / SIP extensions for media authorization	8.6.0	8.7.0	C1-091120
2009-03	CP-43	CP-090275	2578	4	Correction to Annex A /P-Access-Network-Info	8.6.0	8.7.0	-
2009-03	CP-43	CP-090134	2579	2	Correction to Annex A /P-User-Database header	8.6.0	8.7.0	C1-091084
2009-03	CP-43	CP-090134	2582	2	Routeing B2BUA transparency	8.6.0	8.7.0	C1-091078
2009-03	CP-43	CP-090134	2583	1	Call release by P-CSCF- Editorial correction	8.6.0	8.7.0	C1-091013
2009-03	CP-43	CP-090118	2584	1	References correction	8.6.0	8.7.0	C1-091014
2009-03	CP-43	CP-090142	2595	1	Corrections for cdma2000® HRPD Emergency Services	8.6.0	8.7.0	C1-090988
2009-03	CP-43	CP-090127	2596		Corrections to EPS as IMS access technology Annex	8.6.0	8.7.0	C1-090685
2009-03	CP-43	CP-090135	2597	1	Update of references to SIP debug internet drafts	8.6.0	8.7.0	C1-090970
2009-03	CP-43	CP-090159	2598	1	Handling of provisioned mode of the resource allocation used for IMS media	8.6.0	8.7.0	C1-091069
2009-03	CP-43	CP-090237	2601	2	Reference correction	8.6.0	8.7.0	C1-091115
2009-06	CP-44	CP-090428	2518	5	Flow- token in the Record-Route	8.7.0	8.8.0	C1-091475
2009-06	CP-44	CP-090398	2539	8	Mechanism for UE to identify a SIP URI that has an associated tel URI	8.7.0	8.8.0	C1-092241
2009-06	CP-44	CP-090428	2557	3	Application server usage of P-Served-User header field	8.7.0	8.8.0	C1-092077
2009-06	CP-44	CP-090399	2605	2	P-CSCF releasing a dialog	8.7.0	8.8.0	C1-092084
2009-06	CP-44	CP-090399	2607	2	S-CSCF releasing a dialog	8.7.0	8.8.0	C1-092086
2009-06	CP-44	CP-090428	2608	2	GRUU translation	8.7.0	8.8.0	C1-092087
2009-06	CP-44	CP-090428	2610	1	Correct backwards emergency notification procedure	8.7.0	8.8.0	C1-092072
2009-06	CP-44	CP-090428	2611		Correction of implementation error of CR2537r1	8.7.0	8.8.0	C1-091494
2009-06	CP-44	CP-090428	2612	1	BGCF routing	8.7.0	8.8.0	C1-092074
2009-06	CP-44	CP-090403	2614		Correction of 3GPP URN link	8.7.0	8.8.0	C1-091504
2009-06	CP-44	CP-090428	2616	2	RFC 2833 substituted by RFC 4733	8.7.0	8.8.0	C1-092050
2009-06	CP-44	CP-090428	2617		Call Forwarding Leftover	8.7.0	8.8.0	C1-091510

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2009-06	CP-44	CP-090415	2618	1	Correction Identity handling for NGCN	8.7.0	8.8.0	C1-091974
2009-06	CP-44	CP-090419	2619		Reference Update draft-ietf-mmusic-sdp-cs	8.7.0	8.8.0	C1-091513
2009-06	CP-44	CP-090428	2620	1	RFC reference fix	8.7.0	8.8.0	C1-092075
2009-06	CP-44	CP-090428	2625	1	Deterministic XML schema	8.7.0	8.8.0	C1-092204
2009-06	CP-44	CP-090398	2634		Emergency call treatment of P-Preferred-Identity header field in profile	8.7.0	8.8.0	C1-091649
2009-06	CP-44	CP-090405	2635	1	Subdivision of digit collection text	8.7.0	8.8.0	C1-091967
2009-06	CP-44	CP-090428	2636		Editorial changes	8.7.0	8.8.0	C1-091655
2009-06	CP-44	CP-090398	2639	1	Correcting emergency registration support and access type	8.7.0	8.8.0	C1-092003
2009-06	CP-44	CP-090397	2645	1	Correction to Annex A /Caller preferences directives	8.7.0	8.8.0	C1-092079
2009-06	CP-44	CP-090428	2657	2	Alignment of Cx reference point procedures withTS 29.228 procedures	8.7.0	8.8.0	C1-092211
2009-06	CP-44	CP-090415	2658	2	Correction to GRUU procedures to ensure that sessions using UE assigned Public GRUUs don't fail	8.7.0	8.8.0	C1-092219
2009-06	CP-44	CP-090428	2659		Removing obsolete Editor's Note	8.7.0	8.8.0	C1-091854
2009-06	CP-44	CP-090428	2660	1	Correction of instance ID related Editor's Note and text	8.7.0	8.8.0	C1-092076
2009-06	CP-44	CP-090398	2662		Version update for "sos" URI parameter Internet Draft	8.7.0	8.8.0	C1-091857
2009-06	CP-44	CP-090428	2663		Contact Header in PUBLISH method	8.7.0	8.8.0	C1-091879
2009-06	CP-44	CP-090428	2666		Removing non-essential and incorrect statement regarding ordering of codec formats in the SDP offer	8.7.0	8.8.0	C1-092114
2009-06	CP-44	CP-090400	2667	1	Correction to Annex A /P-User-Database	8.7.0	8.8.0	C1-092209
2009-06	CP-44	CP-090430	2644	2	Addition of capability for delivering the original Request-URI	8.8.0	9.0.0	C1-092227
2009-09	CP-45	CP-090696	2671	2	Service-Route/Path header handling for fetching bindings	9.0.0	9.1.0	C1-093049
2009-09	CP-45	CP-090644	2674	2	Inconsistency between text and XML schema	9.0.0	9.1.0	C1-093709
2009-09	CP-45	CP-090650	2675		Confusing text in L.2.2.5.1A	9.0.0	9.1.0	C1-092401
2009-09	CP-45	CP-090658	2676	3	Emergency call handling in P-CSCF and UE	9.0.0	9.1.0	C1-093070
2009-09	CP-45	CP-090649	2679	1	TISPAN IBCF review comment fixes	9.0.0	9.1.0	C1-092903
2009-09	CP-45	CP-090696	2680		TISPAN review comments - minor fixes	9.0.0	9.1.0	C1-092407
2009-09	CP-45	CP-090657	2682	1	Contact port in non REGISTER request with AKA	9.0.0	9.1.0	C1-092409
2009-09	CP-45	CP-090696	2684	1	reg/debug event package subscription headers	9.0.0	9.1.0	C1-092987
2009-09	CP-45	CP-090664	2686	2	Connection of complex UEs to IMS	9.0.0	9.1.0	C1-093739
2009-09	CP-45	CP-090737	2689	2	Calling party category (cpc)	9.0.0	9.1.0	-
2009-09	CP-45	CP-090696	2691	1	UE procedure on registration failure	9.0.0	9.1.0	C1-093015
2009-09	CP-45	CP-090658	2693	1	Correction of BGCF procedures	9.0.0	9.1.0	C1-092989

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2009-09	CP-45	CP-090696	2694	2	Topology hiding on Path header	9.0.0	9.1.0	C1-093016
2009-09	CP-45	CP-090682	2695	1	Create XML source files	9.0.0	9.1.0	C1-093029
2009-09	CP-45	CP-090667	2697	1	Correcting preventing of DDOS attack on registrar	9.0.0	9.1.0	C1-092952
2009-09	CP-45	CP-090657	2700		Correcting mismatch in conditions for non-UE detectable emergency call	9.0.0	9.1.0	C1-092494
2009-09	CP-45	CP-090659	2702	1	The “comp” parameter	9.0.0	9.1.0	C1-093702
2009-09	CP-45	CP-090659	2704		Routing procedure	9.0.0	9.1.0	C1-092501
2009-09	CP-45	CP-090664	2706		UE as an externally attached network	9.0.0	9.1.0	C1-092503
2009-09	CP-45	CP-090725	2710	2	Require with the option-tag "outbound"	9.0.0	9.1.0	-
2009-09	CP-45	CP-090658	2712	1	Outbound support	9.0.0	9.1.0	C1-092994
2009-09	CP-45	CP-090657	2718	2	Contact header in registration	9.0.0	9.1.0	C1-093704
2009-09	CP-45	CP-090659	2720	1	S-CSCF not supporting Outbound registration	9.0.0	9.1.0	C1-093002
2009-09	CP-45	CP-090648	2722	2	NAT traversal without outbound	9.0.0	9.1.0	C1-093041
2009-09	CP-45	CP-090651	2724		Duplicate subclauses in Annex O	9.0.0	9.1.0	C1-092530
2009-09	CP-45	CP-090664	2727	2	P-CSCF handling alignments for priviledged senders	9.0.0	9.1.0	C1-093486
2009-09	CP-45	CP-090664	2729	1	P-CSCF handling for NCGN as regular UE	9.0.0	9.1.0	C1-092932
2009-09	CP-45	CP-090664	2731	5	S-CSCF handling alignments for NGCN	9.0.0	9.1.0	C1-093910
2009-09	CP-45	CP-090664	2741	2	Use of GRUU by UEs that perform the functions of an external attached network	9.0.0	9.1.0	C1-093905
2009-09	CP-45	CP-090658	2743		Correction of alignment of Cx reference point procedures withTS 29.228 procedures	9.0.0	9.1.0	C1-092658
2009-09	CP-45	CP-090659	2745		Reference update for draft-montemurro-gsma-imei-urn	9.0.0	9.1.0	C1-092660
2009-09	CP-45	CP-090696	2746	1	Annex K: P-CSCF alignment	9.0.0	9.1.0	C1-093017
2009-09	CP-45	CP-090696	2747	1	Annex K: S-CSCF alignment	9.0.0	9.1.0	C1-093018
2009-09	CP-45	CP-090696	2748		Annex K: Removal of IBCF modifications	9.0.0	9.1.0	C1-092664
2009-09	CP-45	CP-090658	2752	2	Keep-alives for emergency calls	9.0.0	9.1.0	C1-093043
2009-09	CP-45	CP-090649	2755	1	P-CSCF forwarding request towards entry point	9.0.0	9.1.0	C1-092910
2009-09	CP-45	CP-090659	2759	1	Re-INVITE for precondition status indication	9.0.0	9.1.0	C1-093011
2009-09	CP-45	CP-090658	2761	1	Digest URI verification fix	9.0.0	9.1.0	C1-093034
2009-09	CP-45	CP-090696	2762		SDP in session modification messages	9.0.0	9.1.0	C1-092678
2009-09	CP-45	CP-090658	2764		Correction of table condition: AoC roles	9.0.0	9.1.0	C1-092680
2009-09	CP-45	CP-090732	2766	5	Aligning IANA registration of MIME type "application/3gpp-ims+xml"	9.0.0	9.1.0	-
2009-09	CP-45	CP-090690	2767	4	Emergency call introduction	9.0.0	9.1.0	C1-093946
2009-09	CP-45	CP-090690	2768	1	Emergency call changes to Annex B (GPRS)	9.0.0	9.1.0	C1-092825
2009-09	CP-45	CP-090690	2769	1	Emergency call changes to Annex L (EPS)	9.0.0	9.1.0	C1-092826
2009-09	CP-45	CP-090667	2778	1	How the P-CSCF forwards the request to the	9.0.0	9.1.0	C1-093006

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					next hop excluding the REGISTER method.			
2009-09	CP-45	CP-090696	2779	1	Clarification of a target refresh request.	9.0.0	9.1.0	C1-093007
2009-09	CP-45	CP-090660	2780	1	No Proxy-Authentication-Info header	9.0.0	9.1.0	C1-093721
2009-09	CP-45	CP-090664	2781	2	No P-P-I from NGCN	9.0.0	9.1.0	C1-093790
2009-09	CP-45	CP-090696	2784	1	Trust domain clarification	9.0.0	9.1.0	C1-093753
2009-09	CP-45	CP-090696	2785	1	Clarification of Handling of geo-local numbers	9.0.0	9.1.0	C1-093754
2009-09	CP-45	CP-090645	2789		IOI Handling	9.0.0	9.1.0	C1-093266
2009-09	CP-45	CP-090671	2791	1	Invalid Registration	9.0.0	9.1.0	C1-093745
2009-09	CP-45	CP-090665	2793	1	IBCF and P-Asserted-Identity	9.0.0	9.1.0	C1-093783
2009-09	CP-45	CP-090657	2797	1	Correct the preconditions for NBA mechanism	9.0.0	9.1.0	C1-093760
2009-09	CP-45	CP-090682	2800	4	Correction of dialog correlation	9.0.0	9.1.0	C1-093985
2009-09	CP-45	CP-090696	2801		Corrections to SDP profile table entries	9.0.0	9.1.0	C1-093449
2009-09	CP-45	CP-090657	2803	1	Adding RFC 3890 and maximum packet rate to SDP profile tables	9.0.0	9.1.0	C1-093762
2009-09	CP-45	CP-090679	2806	2	Correcting duplicate mentioning of 802.3y	9.0.0	9.1.0	C1-093913
2009-09	CP-45	CP-090647	2813		Update of reference to I-D for sos URI parameter and miscellaneous reference corrections	9.0.0	9.1.0	C1-093574
2009-09	CP-45	CP-090659	2815	2	Use of ports for SIP between UE and P-CSCF	9.0.0	9.1.0	C1-093908
2009-09	CP-45	CP-090659	2817	1	Profile table correction on the support of security mechanism	9.0.0	9.1.0	C1-093578
2009-09	CP-45	CP-090696	2819	1	Correction on the summary of security mechanism	9.0.0	9.1.0	C1-093767
2009-09	CP-45	CP-090657	2827	1	Clarification on identity usage for NBA	9.0.0	9.1.0	C1-093769
2009-09	CP-45	CP-090664	2829		Describe the right behaviour of the IBCF	9.0.0	9.1.0	C1-093609
2009-12	CP-46	CP-090923	2834	3	Correction to introduce support for IMSVoPS	9.1.0	9.2.0	C1-095602
2009-12	CP-46	CP-090923	2835	2	Transcoding Control at MRF using RFC 4117	9.1.0	9.2.0	C1-094737
2009-12	CP-46	CP-090890	2839		Inclusion of draft-ietf-sipcore-invfix	9.1.0	9.2.0	C1-094120
2009-12	CP-46	CP-090890	2843	1	Inclusion of draft-ietf-sip-ipv6-abnf-fix	9.1.0	9.2.0	C1-094531
2009-12	CP-46	CP-090891	2847		Change of ua-profile package to xcap-diff package	9.1.0	9.2.0	C1-094131
2009-12	CP-46	CP-090892	2850		Release 7 IETF reference updates for emergency call	9.1.0	9.2.0	C1-094134
2009-12	CP-46	CP-090940	2854		Inclusion of draft-ietf-sip-record-route-fix	9.1.0	9.2.0	C1-094152
2009-12	CP-46	CP-090940	2855	1	Correction of support of trust domain boundaries for identity	9.1.0	9.2.0	C1-094566
2009-12	CP-46	CP-090923	2856	1	Inclusion of roles for XCAP client / server at the Ut reference point for supplementary services	9.1.0	9.2.0	C1-094538
2009-12	CP-46	CP-090920	2858		Update of draft-ietf-sip-body-handling reference to RFC 5621	9.1.0	9.2.0	C1-094215
2009-12	CP-46	CP-090940	2860		xsd file alignment with main document	9.1.0	9.2.0	C1-094316

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2009-12	CP-46	CP-090940	2861	1	Textual layout errors in Annex A	9.1.0	9.2.0	C1-094568
2009-12	CP-46	CP-090936	2863	2	Media plane security	9.1.0	9.2.0	C1-094729
2009-12	CP-46	CP-090940	2866	1	3rd party registration failure	9.1.0	9.2.0	C1-094336
2009-12	CP-46	CP-090923	2689	4	Detecting requests destined for a PSAP	9.1.0	9.2.0	C1-095704
2009-12	CP-46	CP-091016	2875	5	Alignment of 24.229 with draft-ietf-sipcore-info-events	9.1.0	9.2.0	-
2009-12	CP-46	CP-090940	2877	1	Correction of indication to the user that an emergency call was made	9.1.0	9.2.0	C1-094582
2009-12	CP-46	CP-090940	2881	2	Annex A /183 (Session Progress) response	9.1.0	9.2.0	C1-094733
2009-12	CP-46	CP-090890	2885		Annex A / c and m paramters in media description in SDP	9.1.0	9.2.0	C1-094382
2009-12	CP-46	CP-090890	2889		Annex A / User-Agent in PUBLISH responses	9.1.0	9.2.0	C1-094387
2009-12	CP-46	CP-091049	2891	3	Annex A / Allow events	9.1.0	9.2.0	-
2009-12	CP-46	CP-090940	2892	1	Annex A /MIME-Version header	9.1.0	9.2.0	C1-094571
2009-12	CP-46	CP-090940	2893	2	Annex A / Require header	9.1.0	9.2.0	C1-094734
2009-12	CP-46	CP-090940	2894	1	Application of trust domains to the P-Early-media header field	9.1.0	9.2.0	C1-094573
2009-12	CP-46	CP-090923	2895	2	Allowing direct routing between AS and MRFC	9.1.0	9.2.0	C1-094736
2009-12	CP-46	CP-090936	2900	3	Registration of IMS media plane security capabilities	9.1.0	9.2.0	C1-094730
2009-12	CP-46	CP-090893	2905		Updating of outbound and related references	9.1.0	9.2.0	C1-094826
2009-12	CP-46	CP-090894	2908		Updating of GRUU references	9.1.0	9.2.0	C1-094832
2009-12	CP-46	CP-090940	2909		Miscellaneous editorial corrections	9.1.0	9.2.0	C1-094850
2009-12	CP-46	CP-090892	2912	1	Removal of outstanding Editor's notes for EMC1	9.1.0	9.2.0	C1-095486
2009-12	CP-46	CP-090896	2914		Removal of outstanding Editor's note for ServID	9.1.0	9.2.0	C1-094855
2009-12	CP-46	CP-090903	2916		Removal of outstanding Editor's note for Overlap	9.1.0	9.2.0	C1-094857
2009-12	CP-46	CP-090940	2924	2	Definition of globally Globally Routeable SIP URI.	9.1.0	9.2.0	C1-095676
2009-12	CP-46	CP-090940	2925	1	Handling of Request-URI with tel URI and sip URI containing user=phone by the BGCF	9.1.0	9.2.0	C1-095438
2009-12	CP-46	CP-090940	2926	2	Additional routeing capabilities	9.1.0	9.2.0	C1-095677
2009-12	CP-46	CP-090902	2932	1	Handling of Route by the I-CSCF	9.1.0	9.2.0	C1-095607
2009-12	CP-46	CP-090902	2934	1	Annex A/ P-Charging-Vector	9.1.0	9.2.0	C1-095606
2009-12	CP-46	CP-090902	2936	2	REGISTERs for Keeping NAT binding /Annex F	9.1.0	9.2.0	C1-095703
2009-12	CP-46	CP-090938	2940	1	Mi reference point additions – general aspects	9.1.0	9.2.0	C1-095467
2009-12	CP-46	CP-090938	2941	1	Mi reference point additions – location determination summary	9.1.0	9.2.0	C1-095468
2009-12	CP-46	CP-090938	2942	3	Mi reference point additions – E-CSCF changes	9.1.0	9.2.0	C1-095726
2009-12	CP-46	CP-090938	2943	3	Mi reference point additions – new LRF functionality	9.1.0	9.2.0	C1-095727

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2009-12	CP-46	CP-090938	2944		MI reference point additions – profile changes	9.1.0	9.2.0	C1-094995
2009-12	CP-46	CP-090902	2946		Correction of profile table on the role for UE	9.1.0	9.2.0	C1-094997
2009-12	CP-46	CP-090936	2951	2	Indicating End-to-Access Edge Media Plane Security in session set-up	9.1.0	9.2.0	C1-095700
2009-12	CP-46	CP-090895	2954	2	Correct Phone-Context parameter coding	9.1.0	9.2.0	C1-095688
2009-12	CP-46	CP-090940	2955	2	Human readable UE name	9.1.0	9.2.0	C1-095648
2009-12	CP-46	CP-090927	2959	2	E-CSCF invoking EATF	9.1.0	9.2.0	C1-095718
2009-12	CP-46	CP-090930	2960	2	IMEI in unauthenticated emergency call in EPS and GPRS	9.1.0	9.2.0	C1-095714
2009-12	CP-46	CP-090930	2961	1	Emergency bearer activation in EPS and GPRS	9.1.0	9.2.0	C1-095309
2009-12	CP-46	CP-090892	2964		Alignment of 24.229 with draft-patel-ecrit-sos-parameter-07	9.1.0	9.2.0	C1-095069
2009-12	CP-46	CP-090892	2967	1	Removal of editor's note in 5.4.8.2 – use of "sos" in GRUU	9.1.0	9.2.0	C1-095489
2009-12	CP-46	CP-090923	2971	1	Reason header in provisional responses	9.1.0	9.2.0	C1-095472
2009-12	CP-46	CP-090940	2976		Correcting SIP interface to VoiceXML media services	9.1.0	9.2.0	C1-095187
2009-12	CP-46	CP-090940	2980	1	Annex A: Support of INFO for CAT and CRS	9.1.0	9.2.0	C1-095445
2009-12	CP-46	CP-090940	2981	2	Removal of editor’s note on 199 provisional response	9.1.0	9.2.0	C1-095649
2009-12	CP-46	CP-090983	2970	2	Update to annex J based on draft-patel-dispatch-cpc-oli-parameter	9.1.0	9.2.0	-
2010-03	CP-47	CP-100131	2810	3	Correcting handling of emergency session requests made by unregistered users	9.2.0	9.3.0	C1-101129
2010-03	CP-47	CP-100110	2930	4	Handling of Request-URI with tel URI and sip URI containing user=phone by the S-CSCF	9.2.0	9.3.0	C1-100993
2010-03	CP-47	CP-100104	2958	4	Emergency session with P-CSCF in visited network	9.2.0	9.3.0	C1-100720
2010-03	CP-47	CP-100110	2990	1	IETF reference updates (IMSProtoc2 related)	9.2.0	9.3.0	C1-100210
2010-03	CP-47	CP-100124	2992	3	Support of draft-ietf-mmusic-sdp-media-capabilities	9.2.0	9.3.0	C1-101151
2010-03	CP-47	CP-100153	2994	5	Adding 1XRTT Femto support for the 3GPP2-1X access type	9.2.0	9.3.0	C1-101180
2010-03	CP-47	CP-100149	2996	1	Correction for e2ae syntax	9.2.0	9.3.0	C1-100200
2010-03	CP-47	CP-100153	2997	2	Implications of resource reservation failure	9.2.0	9.3.0	C1-100704
2010-03	CP-47	CP-100143	2998	1	RFC 4488 in Annex A	9.2.0	9.3.0	C1-100176
2010-03	CP-47	CP-100153	3000	1	Removing an Editor's note in the reference section	9.2.0	9.3.0	C1-100135
2010-03	CP-47	CP-100153	3001	4	Handling of Subscription context information by intermediary entities	9.2.0	9.3.0	C1-101116
2010-03	CP-47	CP-100151	3002	1	Editorial update: adding missing defenitions, correcting typos and inconsistencies	9.2.0	9.3.0	C1-100198
2010-03	CP-47	CP-100151	3003	3	Correcting providing of additional location information to LRF	9.2.0	9.3.0	C1-101117

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2010-03	CP-47	CP-100149	3004	1	Editorial amendments for end to access edge media security	9.2.0	9.3.0	C1-100233
2010-03	CP-47	CP-100149	3005	2	Improvements to end to access edge security text	9.2.0	9.3.0	C1-100780
2010-03	CP-47	CP-100149	3006	1	MGCF is not involved in e2ae security	9.2.0	9.3.0	C1-100234
2010-03	CP-47	CP-100149	3007	1	UE requirements in the absence of P-CSCF support of end to access edge security	9.2.0	9.3.0	C1-100202
2010-03	CP-47	CP-100149	3008	1	Profile additions for end to access edge security	9.2.0	9.3.0	C1-100203
2010-03	CP-47	CP-100149	3009	1	Coverage of media security in the security introduction	9.2.0	9.3.0	C1-100204
2010-03	CP-47	CP-100151	3010	1	Making the E-CSCF responsible for the domain of incoming Request-URI	9.2.0	9.3.0	C1-100230
2010-03	CP-47	CP-100151	3011	1	Usage of P-Charging-Vector header within the emergency call architecture	9.2.0	9.3.0	C1-100199
2010-03	CP-47	CP-100151	3013	1	Delivery of location by the E-CSCF	9.2.0	9.3.0	C1-100159
2010-03	CP-47	CP-100151	3014	2	Structure of reference identifier	9.2.0	9.3.0	C1-100941
2010-03	CP-47	CP-100151	3015	1	Handling of editor's note on subscribing to all dialogs	9.2.0	9.3.0	C1-100160
2010-03	CP-47	CP-100109	3017		Resolution of editor's notes related to PRIOR	9.2.0	9.3.0	C1-100208
2010-03	CP-47	CP-100230	3019	1	Removal of editor's notes relating to learning of trust domain boundaries and information saved during registration	9.2.0	9.3.0	-
2010-03	CP-47	CP-100135	3020	1	Correcting IP-CAN documentation	9.2.0	9.3.0	C1-100944
2010-03	CP-47	CP-100153	3024		P-CSCF Note correction	9.2.0	9.3.0	C1-100339
2010-03	CP-47	CP-100153	3025		Authentication-Info header field	9.2.0	9.3.0	C1-100340
2010-03	CP-47	CP-100153	3026	4	DTMF Info Package definition	9.2.0	9.3.0	C1-101119
2010-03	CP-47	CP-100110	3028		Removal of editor’s note: 199 (Early Dialog Terminated) option-tag	9.2.0	9.3.0	C1-100366
2010-03	CP-47	CP-100111	3031		Removal of editor’s note: Annex K NAT traversal	9.2.0	9.3.0	C1-100369
2010-03	CP-47	CP-100107	3035		Closure of SAES related editor's notes	9.2.0	9.3.0	C1-100419
2010-03	CP-47	CP-100117	3037		Addressing editor's notes relating to NASS bundled authentication	9.2.0	9.3.0	C1-100421
2010-03	CP-47	CP-100110	3039		Removal of editor's notes relating to emergency call	9.2.0	9.3.0	C1-100423
2010-03	CP-47	CP-100110	3043		Removal of outstanding Editor's note on IOI	9.2.0	9.3.0	C1-100436
2010-03	CP-47	CP-100107	3045		Incorrect NAS message in Annex L	9.2.0	9.3.0	C1-100454
2010-03	CP-47	CP-100135	3048	2	Delete EN pertaining to RFC 4117	9.2.0	9.3.0	C1-101156
2010-03	CP-47	CP-100122	3053		Incorrect trigger in I-CSCF for restoration procedures	9.2.0	9.3.0	C1-100462
2010-03	CP-47	CP-100112	3054	1	Clean up editor's notes on subscription to debug event package	9.2.0	9.3.0	C1-100983
2010-03	CP-47	CP-100149	3055	1	Exchanging media plane security capabilities at registration	9.2.0	9.3.0	C1-100971

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2010-03	CP-47	CP-100218	3056	2	Profile table changes for exchanging media plane security capabilities at registration	9.2.0	9.3.0	-
2010-03	CP-47	CP-100153	3057	1	Corrections to profile table entries related to security agreement	9.2.0	9.3.0	C1-100973
2010-03	CP-47	CP-100110	3059	1	Inclusion of draft alert-urns for INVITE Responses	9.2.0	9.3.0	C1-100954
2010-03	CP-47	CP-100119	3063		Reference update of draft-ietf-mediactrl-vxml	9.2.0	9.3.0	C1-100518
2010-03	CP-47	CP-100118	3065	1	Address the UUS related Editor's Note	9.2.0	9.3.0	C1-100986
2010-03	CP-47	CP-100110	3069	1	Correcting missing reference	9.2.0	9.3.0	C1-100991
2010-03	CP-47	CP-100153	3072	4	Session ID profile table alignment	9.2.0	9.3.0	C1-101176
2010-03	CP-47	CP-100105	3075	1	Annex A/ Fixing of missing status support in Tables	9.2.0	9.3.0	C1-100982
2010-03	CP-47	CP-100105	3078		Annex A/ P-Media-Authorization support	9.2.0	9.3.0	C1-100666
2010-03	CP-47	CP-100105	3081		Annex A / integration of resource management and SIP	9.2.0	9.3.0	C1-100670
2010-03	CP-47	CP-100247	3082	2	Additional routeing capabilities	9.2.0	9.3.0	-
2010-03	CP-47	CP-100138	3083	3	P-CSCF Restoration Procedures	9.2.0	9.3.0	C1-101262
2010-03	CP-47	CP-100110	3086		New version of IETF draft-yu-tel-dai	9.2.0	9.3.0	C1-100684
2010-03	CP-47	CP-100110	3092		Abnormal Digest procedures fix	9.2.0	9.3.0	C1-100692
2010-03	CP-47	CP-100128	3094		IMDN reference update	9.2.0	9.3.0	C1-100694
2010-03	CP-47	CP-100140	3095	1	I4 applicability and EATF functionality	9.2.0	9.3.0	C1-100940
2010-03	CP-47	CP-100153	3096		Failure of GPRS and EPS resource reservation	9.2.0	9.3.0	C1-100703
2010-03	CP-47	CP-100142	3097	3	Addition of Dialog Event package to profile tables in support of Inter-UE transfer	9.2.0	9.3.0	C1-101162
2010-03	CP-47	CP-100151	3098		Correction of reference to RFC 4235	9.2.0	9.3.0	C1-100966
2010-03	CP-47	CP-100144	3099		Emergency call clarifications in the absence of registration	9.2.0	9.3.0	C1-100774
2010-03	CP-47	CP-100110	3101		Correct authentication and registration referencing for emergency registration	9.2.0	9.3.0	C1-100805
2010-03	CP-47	CP-100107	3103		P-Access-Network-Info correction for LTE	9.2.0	9.3.0	C1-100808
2010-03	CP-47	CP-100104	3106		Update reference for draft-patel-ecrit-sos-parameter	9.2.0	9.3.0	C1-100811
2010-03	CP-47	CP-100216	3033	2	Updating of SAES related references	9.2.0	9.3.0	-
2010-03	CP-47				Editorial correction	9.3.0	9.3.1	-
2010-06	CP-48	CP-100364	3012	3	Completion of dialog event package usage	9.3.1	9.4.0	C1-101860
2010-06	CP-48	CP-100363	3118	1	Profile table changes for SDES media plane security role	9.3.1	9.4.0	C1-101889
2010-06	CP-48	CP-100363	3119		Using SDES cryptro attribute	9.3.1	9.4.0	C1-101395
2010-06	CP-48	CP-100346	3121		Wrong requirements for ICS MSC in profile tables	9.3.1	9.4.0	C1-101399
2010-06	CP-48	CP-100337	3129		Reference updates	9.3.1	9.4.0	C1-101472
2010-06	CP-48	CP-100359	3130	1	norefersub corrections	9.3.1	9.4.0	C1-101859

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2010-06	CP-48	CP-100364	3131		Charging tidyup	9.3.1	9.4.0	C1-101487
2010-06	CP-48	CP-100359	3136	1	MSC Server assisted mid-call feature - conferencing	9.3.1	9.4.0	C1-102032
2010-06	CP-48	CP-100340	3142	1	RFC4694 for IBCF	9.3.1	9.4.0	C1-101814
2010-06	CP-48	CP-100364	3148		3xx response replaced by response	9.3.1	9.4.0	C1-101584
2010-06	CP-48	CP-100340	3151	1	Use of P-Served-User header field in user location procedure	9.3.1	9.4.0	C1-101812
2010-06	CP-48	CP-100340	3155	2	IBCF and Content-Disposition	9.3.1	9.4.0	C1-102031
2010-06	CP-48	CP-100351	3158	1	Addition of MSRP SDP a=path attribute	9.3.1	9.4.0	C1-101820
2010-06	CP-48	CP-100363	3161	1	Roles relating to media plane security	9.3.1	9.4.0	C1-101890
2010-06	CP-48	CP-100354	3162	2	IMS available	9.3.1	9.4.0	C1-102103
2010-06	CP-48	CP-100367	3040	1	Identifying an emergency call at the P-CSCF	9.4.0	10.0.0	C1-101504
2010-06	CP-48	CP-100367	3110		Handling of Privacy header	9.4.0	10.0.0	C1-101838
2010-06	CP-48	CP-100367	3113	2	S-CSCF triggering of Additional Routeing capability	9.4.0	10.0.0	C1-102042
2010-06	CP-48	CP-100367	3114	2	xPON access type values in P-Access-Network-Info	9.4.0	10.0.0	C1-102043
2010-06	CP-48	CP-100367	3116	1	Digit manipulation	9.4.0	10.0.0	C1-101843
2010-06	CP-48	CP-100371	3124	1	Digest authentication without Authorization header	9.4.0	10.0.0	C1-102012
2010-06	CP-48	CP-100367	3126	1	Corrections for NASS-Bundled authentication	9.4.0	10.0.0	C1-101844
2010-06	CP-48	CP-100367	3134		Miscellaneous editorial issues	9.4.0	10.0.0	C1-101503
2010-06	CP-48	CP-100371	3137		Usage of "trusted node authentication"	9.4.0	10.0.0	C1-101509
2010-06	CP-48	CP-100367	3146	1	Annex A, Table A.4, item 2C, reference update	9.4.0	10.0.0	C1-101845
2010-09	CP-49	CP-100510	3168	3	Outbound reregistration at P-CSCF	10.0.0	10.1.0	C1-102822
2010-09	CP-49	CP-100500	3171	3	Initial registration for GPRS-IMS at S-CSCF	10.0.0	10.1.0	C1-102848
2010-09	CP-49	CP-100511	3172	5	Privacy protection in IBCF	10.0.0	10.1.0	C1-103526
2010-09	CP-49	CP-100639	3176	3	Alignment with RFC 5552	10.0.0	10.1.0	-
2010-09	CP-49	CP-100511	3178	6	User-related policy data enforcement by the P-CSCF	10.0.0	10.1.0	C1-103517
2010-09	CP-49	CP-100640	3180	3	Handling of aliases URIs	10.0.0	10.1.0	-
2010-09	CP-49	CP-100641	3181	3	Structure of the Request URI sent by a UE	10.0.0	10.1.0	-
2010-09	CP-49	CP-100481	3188	2	Home network check for (E)UTRAN access	10.0.0	10.1.0	C1-103041
2010-09	CP-49	CP-100482	3196	1	Updates to references pertaining to Internet Drafts for tel URI parameters	10.0.0	10.1.0	C1-102676
2010-09	CP-49	CP-100519	3197	1	Usage of alternative P-CSCF address during registration	10.0.0	10.1.0	C1-102631
2010-09	CP-49	CP-100496	3198	8	Mandate registeration with IMS in order to receive audio/voice services	10.0.0	10.1.0	C1-103536
2010-09	CP-49	CP-100510	3200		Annex A, Reason header	10.0.0	10.1.0	C1-102448
2010-09	CP-49	CP-100652	3205	3	Emergency registration in HPLMN	10.0.0	10.1.0	-

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2010-09	CP-49	CP-100486	3209	1	Keep-alive corrections	10.0.0	10.1.0	C1-102624
2010-09	CP-49	CP-100511	3211	4	Passing policy with subscription information to UE and P-CSCF	10.0.0	10.1.0	C1-103504
2010-09	CP-49	CP-100486	3214	1	Wildcarded identity AVP correction	10.0.0	10.1.0	C1-102685
2010-09	CP-49	CP-100486	3217		Subclause reference correction	10.0.0	10.1.0	C1-102492
2010-09	CP-49	CP-100483	3221		Update of draft-rosenberg-sip-app-media-tag reference	10.0.0	10.1.0	C1-102532
2010-09	CP-49	CP-100511	3222	3	Location number	10.0.0	10.1.0	C1-103543
2010-09	CP-49	CP-100487	3226		Updates to references pertaining to Internet Drafts for tel URI parameters	10.0.0	10.1.0	C1-102679
2010-09	CP-49	CP-100511	3236	2	Insertion of IMS access gateway by P-CSCF	10.0.0	10.1.0	C1-103518
2010-09	CP-49	CP-100511	3237	4	Enforcement of P-Early-Media indication by P-CSCF	10.0.0	10.1.0	C1-103544
2010-09	CP-49	CP-100508	3239		EN pertaining to Media Plane Securtiy	10.0.0	10.1.0	C1-103039
2010-09	CP-49	CP-100481	3243	2	Detecting valid emergency identifiers	10.0.0	10.1.0	C1-103542
2010-09	CP-49	CP-100501	3245	2	Emergency PDN connection usage control in P-CSCF	10.0.0	10.1.0	C1-103513
2010-09	CP-49	CP-100510	3249	1	IBCF procedures for SIP message	10.0.0	10.1.0	C1-103382
2010-09	CP-49	CP-100519	3250	2	Indicating wildcarded IMPU in reg-event	10.0.0	10.1.0	C1-103528
2010-09	CP-49	CP-100501	3252	1	Wildcarded Identities handling	10.0.0	10.1.0	C1-103354
2010-09	CP-49	CP-100481	3256	2	Correction of Stage 3 misalignment with Stage 1 and Stage 2 on use of SIP 380 response.	10.0.0	10.1.0	C1-103389
2010-09	CP-49	CP-100519	3257	3	SigComp disabling	10.0.0	10.1.0	C1-103530
2010-09	CP-49	CP-100486	3258	2	Ensuring PSAP receives correctly formatted request	10.0.0	10.1.0	C1-103568
2010-09	CP-49	CP-100486	3261	1	Mandate registeration with IMS in order to receive audio/voice services	10.0.0	10.1.0	C1-103508
2010-12	CP-50	CP-100843	3305	2	SRVCC enhancements - ATCF invocation	10.1.0	10.2.0	C1-104362
2010-12	CP-50	CP-100728	3267	1	Protected AKA registration at S-CSCF	10.1.0	10.2.0	C1-104197
2010-12	CP-50	CP-100728	3270	1	Protected Digest registration at S-CSCF	10.1.0	10.2.0	C1-104300
2010-12	CP-50	CP-100728	3273	2	Unprotected registration at S-CSCF	10.1.0	10.2.0	C1-104370
2010-12	CP-50	CP-100750	3278		Supported header field corrected	10.1.0	10.2.0	C1-103619
2010-12	CP-50	CP-100728	3281	1	Update reference	10.1.0	10.2.0	C1-104310
2010-12	CP-50	CP-100725	3285		Correcting mixed references in IBCF	10.1.0	10.2.0	C1-103761
2010-12	CP-50	CP-100728	3288	3	Conference and IBCF IMS_ALG and removal of an Editor's note.	10.1.0	10.2.0	C1-105071
2010-12	CP-50	CP-100735	3291		Correcting errors in S-CSCF restoration procedures	10.1.0	10.2.0	C1-103773
2010-12	CP-50	CP-100728	3301		Incorrect sequence of steps in P-CSCF	10.1.0	10.2.0	C1-104316
2010-12	CP-50	CP-100723	3304		Emergency registration and normal registration	10.1.0	10.2.0	C1-104183
2010-12	CP-50	CP-100738	3314	1	Updating IMEI URN draft reference	10.1.0	10.2.0	C1-104328

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2010-12	CP-50	CP-100721	3319		IETF reference updates	10.1.0	10.2.0	C1-103921
2010-12	CP-50	CP-100722	3324		IETF reference updates	10.1.0	10.2.0	C1-103926
2010-12	CP-50	CP-100726	3328		IETF reference updates	10.1.0	10.2.0	C1-103936
2010-12	CP-50	CP-100728	3331		IETF reference updates	10.1.0	10.2.0	C1-104337
2010-12	CP-50	CP-100728	3334		EN removal: Retry-After Header field value in 503 response	10.1.0	10.2.0	C1-103955
2010-12	CP-50	CP-100728	3340		EN removal: Network inserted codecs	10.1.0	10.2.0	C1-103961
2010-12	CP-50	CP-100723	3344	1	Further modifications required to SIP 380 response to remove new requirements.	10.1.0	10.2.0	C1-104187
2010-12	CP-50	CP-100864	3345	4	Inclusion of IMEI in the sip.instance of the initial SIP-Register request	10.1.0	10.2.0	C1-105086
2010-12	CP-50	CP-100733	3348		Handling of editor's note relating to private network traffic breakout and breakin	10.1.0	10.2.0	C1-103984
2010-12	CP-50	CP-100726	3354	2	Inclusion of file transfer attributes	10.1.0	10.2.0	C1-104986
2010-12	CP-50	CP-100752	3355	2	IBCF and 3xx responses	10.1.0	10.2.0	C1-104595
2010-12	CP-50	CP-100752	3356		Non E.164 Tel URI conversion failure	10.1.0	10.2.0	C1-104464
2010-12	CP-50	CP-100750	3357	2	max-time and base-time parameters provision	10.1.0	10.2.0	C1-105207
2010-12	CP-50	CP-100752	3358		reference correction	10.1.0	10.2.0	C1-104466
2010-12	CP-50	CP-100728	3361	1	AKA registration at S-CSCF	10.1.0	10.2.0	C1-104991
2010-12	CP-50	CP-100728	3364	2	Autentication already performed	10.1.0	10.2.0	C1-105203
2010-12	CP-50	CP-100728	3367	1	Digest registration at S-CSCF	10.1.0	10.2.0	C1-104997
2010-12	CP-50	CP-100728	3370	1	Bundle registration	10.1.0	10.2.0	C1-105000
2010-12	CP-50	CP-100720	3377	1	Codec and DTMF correction	10.1.0	10.2.0	C1-104980
2010-12	CP-50	CP-100728	3380		Definition: multiple registrations	10.1.0	10.2.0	C1-104535
2010-12	CP-50	CP-100871	3383	1	Reference update: draft-ietf-sipcore-199	10.1.0	10.2.0	-
2010-12	CP-50	CP-100724	3387		Reference update: draft-ietf-sipcore-keep	10.1.0	10.2.0	C1-104547
2010-12	CP-50	CP-100864	3388	2	Modifications to priority handling in support of MPS	10.1.0	10.2.0	C1-105095
2010-12	CP-50	CP-100885	3389	3	Updating the restoration procedure definition	10.1.0	10.2.0	-
2010-12	CP-50	CP-100752	3390		Adding RFC 5318 to major capabilities tables	10.1.0	10.2.0	C1-105226
2010-12	CP-50	CP-100728	3393	1	Handling of the isfocus media feature tag in P-CSCF	10.1.0	10.2.0	C1-105003
2010-12	CP-50	CP-100752	3394		Annex A, Table A.4, item 29+72 and Table A.4A, prerequisite	10.1.0	10.2.0	C1-104618
2010-12	CP-50	CP-100728	3397		“ob” parameter in case of no registration	10.1.0	10.2.0	C1-105006
2010-12	CP-50	CP-100728	3401	2	Addition of Target-Dialog header and capability in Annex A	10.1.0	10.2.0	C1-105074
2010-12	CP-50	CP-100766	3405	2	Alternative emergency session handling in non-roaming cases (P-CSCF)	10.1.0	10.2.0	C1-105052
2010-12	CP-50	CP-100766	3406	2	Alternative emergency session handling in non-roaming cases (S-CSCF)	10.1.0	10.2.0	C1-105053

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2010-12	CP-50	CP-100766	3407		Alternative emergency session handling in non-roaming cases (E-CSCF)	10.1.0	10.2.0	C1-104682
2010-12	CP-50	CP-100749	3409		Removal of erroneous passing on of IOI value to PSAP	10.1.0	10.2.0	C1-104718
2010-12	CP-50	CP-100766	3411		Additions to E-CSCF functionality for IESE	10.1.0	10.2.0	C1-104721
2010-12	CP-50	CP-100766	3412		IBCF detection and routeing of emergency call	10.1.0	10.2.0	C1-104722
2010-12	CP-50	CP-100864	3413	3	Introduction to priority schemes in the IM CN subsystem	10.1.0	10.2.0	C1-105221
2010-12	CP-50	CP-100766	3414	1	Addition to introductory clauses in support of IESE	10.1.0	10.2.0	C1-104974
2010-12	CP-50	CP-100725	3415	1	Correction of the usage for type 3 IOI	10.1.0	10.2.0	C1-105051
2010-12	CP-50	CP-100864	3425	2	P-CSCF behaviour for insufficient bandwidth	10.1.0	10.2.0	C1-105058
2010-12	CP-50	CP-100752	3416	1	Text corrections	10.1.0	10.2.0	C1-104969
2010-12	CP-50	CP-100727	3420		Update of IETF reference	10.1.0	10.2.0	C1-104842
2011-03	CP-51	CP-110181	3371	4	Sending of location information from LRF to E-CSCF	10.2.0	10.3.0	C1-110671
2011-03	CP-51	CP-110181	3429	2	Response code in Reason header field	10.2.0	10.3.0	C1-110659
2011-03	CP-51	CP-110164	3432	1	UE initiated deregistration	10.2.0	10.3.0	C1-110581
2011-03	CP-51	CP-110181	3433		Other databases	10.2.0	10.3.0	C1-110010
2011-03	CP-51	CP-110181	3434	1	Clarification of possible triggers for network-initiated reauthentication	10.2.0	10.3.0	C1-110560
2011-03	CP-51	CP-110161	3435	6	Update to IMS registration procedures due to USAT initiated Refresh for ISIM/USIM EFs	10.2.0	10.3.0	C1-111511
2011-03	CP-51	CP-110184	3436	1	Optimal Media Routeing – SDP attribute syntax definition	10.2.0	10.3.0	C1-110558
2011-03	CP-51	CP-110184	3437	1	Update SDP profile table for Optimal Media Routeing	10.2.0	10.3.0	C1-110559
2011-03	CP-51	CP-110196	3439	1	Modifications to S-CSCF procedures in support of MPS	10.2.0	10.3.0	C1-110562
2011-03	CP-51	CP-110196	3440	1	Modifications to P-CSCF and IBCF procedures in support of MPS	10.2.0	10.3.0	C1-110563
2011-03	CP-51	CP-110201	3441	1	Select E-CSCF upon S-SCSF failure	10.2.0	10.3.0	C1-110557
2011-03	CP-51	CP-110158	3445	1	Correct P-CSCF handling of requests for emergency services with Route header fields	10.2.0	10.3.0	C1-110567
2011-03	CP-51	CP-110196	3450		Clarification on P-CSCF behaviour in case of insufficient bandwidth	10.2.0	10.3.0	C1-110180
2011-03	CP-51	CP-110166	3453	2	New Reference for Alert-URN	10.2.0	10.3.0	C1-111349
2011-03	CP-51	CP-110187	3457	5	Explicit Congestion Notification (ECN) for RTP over UDP	10.2.0	10.3.0	C1-111360
2011-03	CP-51	CP-110196	3458	4	Clarify the P-CSCF restoration procedure	10.2.0	10.3.0	C1-111271
2011-03	CP-51	CP-110164	3461	1	Reference update: draft-ietf-mmusic-ice-tcp	10.2.0	10.3.0	C1-110578
2011-03	CP-51	CP-110164	3464	1	Reference update: RFC 6086	10.2.0	10.3.0	C1-110589
2011-03	CP-51	CP-110159	3468		Reference update: draft-ietf-sipcore-keep	10.2.0	10.3.0	C1-110267

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2011-03	CP-51	CP-110164	3471	3	P-CSCF Path SIP URI and IMS flow token correction	10.2.0	10.3.0	C1-111283
2011-03	CP-51	CP-110196	3474	1	Encoding of PANI for E-UTRAN	10.2.0	10.3.0	C1-110442
2011-03	CP-51	CP-110196	3475	3	Insertion of “orig” parameter by IBCF	10.2.0	10.3.0	C1-110665
2011-03	CP-51	CP-110196	3479	5	Removal of reference CPC and OLI Internet Draft	10.2.0	10.3.0	C1-111329
2011-03	CP-51	CP-110158	3483	2	Specifying "sos" URI parameter in 24.229	10.2.0	10.3.0	C1-111087
2011-03	CP-51	CP-110196	3484	7	Example of IMS Registration conditions, taking into account the network operator’s preference for selection of the voice domain	10.2.0	10.3.0	C1-111270
2011-03	CP-51	CP-110181	3486	2	Removal of Sigcomp disabling	10.2.0	10.3.0	C1-111266
2011-03	CP-51	CP-110164	3489		New registration	10.2.0	10.3.0	C1-110842
2011-03	CP-51	CP-110309	3490	6	Inclusion of MEID in the sip.instance of the SIP-Register request	10.2.0	10.3.0	-
2011-03	CP-51	CP-110181	3491	1	Disabling SigComp by default in E-UTRAN	10.2.0	10.3.0	C1-111221
2011-03	CP-51	CP-110164	3495	1	S-CSCF Service-Route SIP URI	10.2.0	10.3.0	C1-111274
2011-03	CP-51	CP-110184	3496	4	Introduction of OMR procedures in AS, MGCF and P-CSCF	10.2.0	10.3.0	C1-111359
2011-03	CP-51	CP-110181	3497		Removal of editor’s note: different sets of policies for a user	10.2.0	10.3.0	C1-111235
2011-03	CP-51	CP-110181	3498		Removal of editor’s note: additional policy elements	10.2.0	10.3.0	C1-110939
2011-03	CP-51	CP-110164	3501		Reference update and procedure correction: 199	10.2.0	10.3.0	C1-111277
2011-03	CP-51	CP-110162	3502	1	Contact header clarification	10.2.0	10.3.0	C1-111240
2011-03	CP-51	CP-110160	3507	1	MGCF procedure corrections related to SIP preconditions	10.2.0	10.3.0	C1-111259
2011-03	CP-51	CP-110164	3510		Erroneous row reference in Table A.50A	10.2.0	10.3.0	C1-111000
2011-03	CP-51	CP-110164	3514	1	Correction reference	10.2.0	10.3.0	C1-111280
2011-03	CP-51	CP-110176	3517	2	Correction to the header field indicating where the request comes from in E-CSCF procedures	10.2.0	10.3.0	C1-111325
2011-03	CP-51	CP-110181	3519	1	Editiorial corrections to S-CSCF registration subclauses	10.2.0	10.3.0	C1-111241
2011-03	CP-51	CP-110181	3520	3	Clarification of authentication of 380 and 504 responses with multiple registration	10.2.0	10.3.0	C1-111337
2011-03	CP-51	CP-110181	3521	1	Provision of phone-context parameter value via MO	10.2.0	10.3.0	C1-111245
2011-03	CP-51	CP-110010	3522	3	P-CSCF graceful shutdown	10.2.0	10.3.0	-
2011-06	CP-52	CP-110450	3532	1	Reference update: 199	10.3.0	10.4.0	C1-112024
2011-06	CP-52	CP-110445	3536	1	Reference update: RFC 6223	10.3.0	10.4.0	C1-112013
2011-06	CP-52	CP-110450	3539		Annex A: RFC 6086 reference corrections	10.3.0	10.4.0	C1-111556
2011-06	CP-52	CP-110468	3540	1	Removal of Annex F.3	10.3.0	10.4.0	C1-112015
2011-06	CP-52	CP-110468	3541	1	Moving of P-CSCF ICE procedures (Annex K.3.2 and K.5.3)	10.3.0	10.4.0	C1-112016

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2011-06	CP-52	CP-110468	3542	1	Removal of Annex G	10.3.0	10.4.0	C1-112014
2011-06	CP-52	CP-110468	3545	1	S-CSCF-initiated session release	10.3.0	10.4.0	C1-112025
2011-06	CP-52	CP-110450	3548	1	Service-Route at the UE	10.3.0	10.4.0	C1-112040
2011-06	CP-52	CP-110450	3551	1	Service-Route at the P-CSCF	10.3.0	10.4.0	C1-112043
2011-06	CP-52	CP-110450	3554	2	Service-Route at the S-CSCF	10.3.0	10.4.0	C1-112227
2011-06	CP-52	CP-110450	3557	1	Path header field at the S-CSCF	10.3.0	10.4.0	C1-112049
2011-06	CP-52	CP-110450	3560	1	S-CSCF releasing the dialogs	10.3.0	10.4.0	C1-112052
2011-06	CP-52	CP-110450	3563	1	NOTIFY request	10.3.0	10.4.0	C1-112028
2011-06	CP-52	CP-110450	3566	1	Network Initiated deregistration at S-CSCF	10.3.0	10.4.0	C1-112031
2011-06	CP-52	CP-110450	3569	2	Network Initiated deregistration at P-CSCF	10.3.0	10.4.0	C1-112223
2011-06	CP-52	CP-110450	3572	1	Network Initiated deregistration at UE	10.3.0	10.4.0	C1-112037
2011-06	CP-52	CP-110468	3573		UE initiated deregistration	10.3.0	10.4.0	C1-111590
2011-06	CP-52	CP-110448	3578	1	P-Access-Network-Info : ABNF correction	10.3.0	10.4.0	C1-112004
2011-06	CP-52	CP-110468	3579	1	Moving of IBCF ICE procedures (Annex K.5.4)	10.3.0	10.4.0	C1-112017
2011-06	CP-52	CP-110531	3583	1	SRVCC enhancements in Annex A	10.3.0	10.4.0	-
2011-06	CP-52	CP-110469	3584		ENs on P-CSCF invoking ATCF	10.3.0	10.4.0	C1-111614
2011-06	CP-52	CP-110465	3585	1	Inclusion of MEID in the sip.instance of the SIP-Register request	10.3.0	10.4.0	C1-112201
2011-06	CP-52	CP-110465	3586	1	Clarification of scope of section 5.1.6 on Emergency Call	10.3.0	10.4.0	C1-112089
2011-06	CP-52	CP-110447	3591	1	Fraud prevention for deregistration for ICS	10.3.0	10.4.0	C1-112061
2011-06	CP-52	CP-110474	3596	2	UICC Access to IMS	10.3.0	10.4.0	C1-112249
2011-06	CP-52	CP-110447	3599	1	Updating IMEI URN draft reference	10.3.0	10.4.0	C1-112058
2011-06	CP-52	CP-110468	3602	2	Insertion of "gated" parameter by the P-CSCF	10.3.0	10.4.0	C1-112231
2011-06	CP-52	CP-110451	3605	1	Removal of dial around indicator	10.3.0	10.4.0	C1-112235
2011-06	CP-52	CP-110477	3606	1	OMR designation as media level attributes in profile	10.3.0	10.4.0	C1-112096
2011-06	CP-52	CP-110472	3612	2	Application server detection and routeing of emergency call	10.3.0	10.4.0	C1-112232
2011-06	CP-52	CP-110468	3613	1	Removal of duplicate material in P-CSCF emergency call handling	10.3.0	10.4.0	C1-112094
2011-06	CP-52	CP-110468	3622		Miscellaneous 24.229 corrections	10.3.0	10.4.0	C1-111949
2011-06	CP-52	CP-110521	3611	3	Removal of repetition of IOI header field parameters	10.3.0	10.4.0	-
2011-06	CP-52	CP-110535	3518	4	Reference Location for Emergency Service	10.4.0	11.0.0	-
2011-09	CP-53	CP-110686	3624	1	Reference update	11.0.0	11.1.0	C1-112731
2011-09	CP-53	CP-110654	3633	3	Correcting errors in S-CSCF restoration procedure	11.0.0	11.1.0	C1-113584
2011-09	CP-53	CP-110656	3641	2	P-Profile-Key header field corrections in I-CSCF	11.0.0	11.1.0	C1-112915
2011-09	CP-53	CP-110693	3648	3	Emergency session when IMS voice over PS is	11.0.0	11.1.0	C1-113170

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					not supported			
2011-09	CP-53	CP-110666	3651		EATF in Annex A	11.0.0	11.1.0	C1-112512
2011-09	CP-53	CP-110695	3657	2	Correction on call initiation procedure at the MGCF	11.0.0	11.1.0	C1-112945
2011-09	CP-53	CP-110686	3658		Editorial corrections on SIP header field name	11.0.0	11.1.0	C1-112519
2011-09	CP-53	CP-110689	3659	1	Address the Editor's Note in RLI	11.0.0	11.1.0	C1-112725
2011-09	CP-53	CP-110704	3665	3	Additional IOI correction for SIP responses	11.0.0	11.1.0	-
2011-09	CP-53	CP-110653	3669	1	Replacement of draft-garcia-mmusic-sdp-misc-cap with draft-garcia-mmusic-sdp-miscellaneous-caps	11.0.0	11.1.0	C1-113294
2011-09	CP-53	CP-110686	3670	4	Filtering of P-Associated-URI at P-CSCF	11.0.0	11.1.0	C1-113440
2011-09	CP-53	CP-110674	3676	2	Modification on roles of ATCF	11.0.0	11.1.0	C1-112928
2011-09	CP-53	CP-110651	3683	1	Emergency call – correction of requests covered at the P-CSCF	11.0.0	11.1.0	C1-112832
2011-09	CP-53	CP-110658	3687		IETF reference update	11.0.0	11.1.0	C1-112647
2011-09	CP-53	CP-110681	3689	1	Removal of "select an E-CSCF"	11.0.0	11.1.0	C1-112754
2011-09	CP-53	CP-110686	3691	2	Release of Media Bearers	11.0.0	11.1.0	C1-112937
2011-09	CP-53	CP-110686	3693	2	Network identified by IOI header field parameter	11.0.0	11.1.0	C1-112960
2011-09	CP-53	CP-110648	3700		"P-Visited-Network-ID" correction	11.0.0	11.1.0	C1-113004
2011-09	CP-53	C1-110715	3701	2	Emergency session handling correction	11.0.0	11.1.0	-
2011-09	CP-53	CP-110681	3703		Deletion of Editor's Note Concerning P-CSCF Dialstring Recognition	11.0.0	11.1.0	C1-113087
2011-09	CP-53	CP-110693	3707	1	Emergency Session Setup – Incorrect Reference	11.0.0	11.1.0	C1-113445
2011-09	CP-53	CP-110677	3713	2	Policy passing when different policies are related to different IMPIs sharing an IMPU	11.0.0	11.1.0	C1-113698
2011-09	CP-53	CP-110681	3715		ENs on XML namespace registration	11.0.0	11.1.0	C1-113176
2011-09	CP-53	CP-110656	3719	1	Adding Call-Info to SUBSCRIBE in annex A	11.0.0	11.1.0	C1-113529
2011-09	CP-53	CP-110653	3730		Updating IMEI URN draft reference	11.0.0	11.1.0	C1-113287
2011-09	CP-53	CP-110653	3732	2	Including draft-holmberg-sipcore-proxy-feature	11.0.0	11.1.0	C1-113594
2011-09	CP-53	CP-110687	3740		Transit IOI principles	11.0.0	11.1.0	C1-113595
2011-09	CP-53	CP-110681	3744		Deletion of Editor's Note in 24.229 on authentication mechanism (Rel-10)	11.0.0	11.1.0	C1-113374
2011-09	CP-53	CP-110681	3746	1	Deletion of Editor's Note in 24.229 on aor attribute (Rel-10)	11.0.0	11.1.0	C1-113476
2011-09	CP-53	CP-110661	3758		Deletion of Editor's Note in 24.229 on NASS error message (Rel-8)	11.0.0	11.1.0	C1-113388
2011-09	CP-53	CP-110686	3759		Inter-operator identifier corrections	11.0.0	11.1.0	C1-113392
2011-09	CP-53	CP-110736	3762	2	Correction on EMC handling of S-CSCF	11.0.0	11.1.0	-
2011-09	CP-53	CP-110690	3763		3GPP2 reference corrections	11.0.0	11.1.0	C1-113396
2011-12	CP-54	CP-110887	3673	9	“Default handling” triggering correction	11.1.0	11.2.0	C1-115232

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2011-12	CP-54	CP-110887	3766	3	AS determination of the served user identity	11.1.0	11.2.0	C1-114942
2011-12	CP-54	CP-110887	3771		Editorial correction of the P-CSCF behavior for TCP connection	11.1.0	11.2.0	C1-113821
2011-12	CP-54	CP-110873	3773	1	Update draft-atarius-dispatch-meid-urn	11.1.0	11.2.0	C1-114376
2011-12	CP-54	CP-110887	3786	1	Correction on conditional expression of Major Capabilities	11.1.0	11.2.0	C1-114384
2011-12	CP-54	CP-110852	3790	4	P-CSCF behaviour for emergency calls when failure occurs	11.1.0	11.2.0	C1-115362
2011-12	CP-54	CP-110887	3794	3	Adding missing handling in NOTIFY body for a registration event	11.1.0	11.2.0	C1-114462
2011-12	CP-54	CP-110887	3803	1	P-Profile-Key header field corrections in AS	11.1.0	11.2.0	C1-114214
2011-12	CP-54	CP-110887	3807	1	P-Profile-Key header field corrections in S-CSCF	11.1.0	11.2.0	C1-114215
2011-12	CP-54	CP-110887	3809		S-CSCF flow selection correction	11.1.0	11.2.0	C1-114106
2011-12	CP-54	CP-110887	3810		S-CSCF determing supported IP version by UE for media	11.1.0	11.2.0	C1-114107
2011-12	CP-54	CP-110881	3812	3	ICSI to visited network	11.1.0	11.2.0	C1-115170
2011-12	CP-54	CP-110868	3819	1	Removal of editor's notes relating to insertion of P-Access-Network-Info header field by a proxy	11.1.0	11.2.0	C1-114206
2011-12	CP-54	CP-110887	3820		Editorial corrections on SIP header field name	11.1.0	11.2.0	C1-114534
2011-12	CP-54	CP-110887	3821	1	Addition of IEEE802.3ah to P-Access-Network-Info header	11.1.0	11.2.0	C1-115154
2011-12	CP-54	CP-110887	3822		Editorial correction on de-registration of emergency service	11.1.0	11.2.0	C1-114536
2011-12	CP-54	CP-110856	3827	1	Incorrect reference to RFC 5261	11.1.0	11.2.0	C1-115009
2011-12	CP-54	CP-110873	3834	2	proxy-feature I-D reference update	11.1.0	11.2.0	C1-115288
2011-12	CP-54	CP-110861	3840		Inclusion of media feature tag ASN.1 identifiers	11.1.0	11.2.0	C1-114594
2011-12	CP-54	CP-110887	3845		Record-Route reference correction	11.1.0	11.2.0	C1-114600
2011-12	CP-54	CP-110887	3846	1	Number of emergency registrations	11.1.0	11.2.0	C1-115167
2011-12	CP-54	CP-110850	3850	2	Reference update: Reason header in SIP responses	11.1.0	11.2.0	C1-115274
2011-12	CP-54	CP-110887	3855	4	Additional granularity for IMS Communication Service Identifier	11.1.0	11.2.0	C1-115348
2011-12	CP-54	CP-110869	3857		Correction UE handling compression	11.1.0	11.2.0	C1-114687
2011-12	CP-54	CP-110880	3859	1	Routing of emergency requests via S-CSCF	11.1.0	11.2.0	C1-115178
2011-12	CP-54	CP-110887	3860	1	S-CSCF terminating procedures	11.1.0	11.2.0	C1-115155
2011-12	CP-54	CP-110873	3862	2	Transcoding Control at the IMS-ALG in the P-CSCF and related ECN corrections.	11.1.0	11.2.0	C1-115340
2011-12	CP-54	CP-110887	3863	1	T1 Timer value for MRFC	11.1.0	11.2.0	C1-115158
2011-12	CP-54	CP-110881	3868	1	Adding availability for SMS over IMS determination	11.1.0	11.2.0	C1-114971
2011-12	CP-54	CP-110881	3869	1	ICSI included by AS in Feature-Caps header field in terminating requests	11.1.0	11.2.0	C1-115171

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2011-12	CP-54	CP-110881	3870		Indicating Multimedia Telephony Application Server in Feature-Caps header field	11.1.0	11.2.0	C1-114779
2011-12	CP-54	CP-110865	3874	1	3GPP2 reference corrections	11.1.0	11.2.0	C1-115192
2011-12	CP-54	CP-110887	3879	2	Correction on MRFC handling when receiving an INVITE message	11.1.0	11.2.0	C1-115235
2011-12	CP-54	CP-110885	3891	2	Additional routeing function behaviour for transit ioi	11.1.0	11.2.0	C1-115231
2011-12	CP-54	CP-110887	3892	2	Clarification on I-CSCF routeing procedure for incoming call with Request-URI in SIP URI format	11.1.0	11.2.0	C1-115252
2012-01					Correction of formatting in tables of annex A	11.2.0	11.2.1	
2012-03	CP-55	CP-120118	3835	4	IPXS: Application invocation procedures	11.2.1	11.3.0	C1-120849
2012-03	CP-55	CP-120165	3844	3	Updating of UUS references	11.2.1	11.3.0	-
2012-03	CP-55	CP-120096	3900		Corrections on the conditions of MSRP SDP a=path attribute	11.2.1	11.3.0	C1-120114
2012-03	CP-55	CP-120117	3901		Addition of procedures in case of Fiber access network	11.2.1	11.3.0	C1-120148
2012-03	CP-55	CP-120117	3902		Removal of Editor's Note about access-info of P-Access-Network-Info header	11.2.1	11.3.0	C1-120149
2012-03	CP-55	CP-120124	3903	1	ICSI to visited network - ENs	11.2.1	11.3.0	C1-120778
2012-03	CP-55	CP-120117	3905	2	S-CSCF behavior when the number of simultaneous registrations for the same UE is reached.	11.2.1	11.3.0	C1-120880
2012-03	CP-55	CP-120117	3906	3	P-CSCF address provided by OMA DM for fixed access (Annex E).	11.2.1	11.3.0	C1-120906
2012-03	CP-55	CP-120124	3909	3	Use of Contact Parameters in a 3XX Response from an LRF	11.2.1	11.3.0	C1-120898
2012-03	CP-55	CP-120093	3916	1	Geo-Redundancy Registration	11.2.1	11.3.0	C1-120556
2012-03	CP-55	CP-120107	3918	2	P-CSCF forwarding REGISTER when ATCF is used	11.2.1	11.3.0	C1-120869
2012-03	CP-55	CP-120112	3920		IMS-ALG in the P-CSCF is invoked for Transcoding Control	11.2.1	11.3.0	C1-120212
2012-03	CP-55	CP-120117	3921	2	P-Served-User to BGCF	11.2.1	11.3.0	C1-120854
2012-03	CP-55	CP-120090	3928	1	Location Conveyance: Reference update	11.2.1	11.3.0	C1-120562
2012-03	CP-55	CP-120117	3933	1	Location Conveyance: Location Forwarding to MGCF and PSAP	11.2.1	11.3.0	C1-120563
2012-03	CP-55	CP-120112	3940	1	Reference update: draft-holmberg-sipcore-proxy-feature	11.2.1	11.3.0	C1-120619
2012-03	CP-55	CP-120112	3942	1	UE usage of Feature-Caps	11.2.1	11.3.0	C1-120617
2012-03	CP-55	CP-120124	3945	1	GRUU: UE self-assigned GRUU	11.2.1	11.3.0	C1-120766
2012-03	CP-55	CP-120116	3947	2	IMS_IOI_CH input on IBCF behaviour	11.2.1	11.3.0	C1-120848
2012-03	CP-55	CP-120115	3948	1	GINI input on profile tables	11.2.1	11.3.0	C1-120696
2012-03	CP-55	CP-120092	3957	1	Updating references to IMEI URN and XML body handling drafts	11.2.1	11.3.0	C1-120583
2012-03	CP-55	CP-120112	3960	1	Removing contradictory statement from User	11.2.1	11.3.0	C1-120621

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					initiated deregstration procedure			
2012-03	CP-55	CP-120117	3961		Editorial corrections	11.2.1	11.3.0	C1-120321
2012-03	CP-55	CP-120124	3962	1	Clarification on forking related issues	11.2.1	11.3.0	C1-120768
2012-03	CP-55	CP-120115	3967	2	Add general support for RFC 6140	11.2.1	11.3.0	C1-120850
2012-03	CP-55	CP-120115	3968	2	Add complex UE support for RFC 6140 mainline GIN registration functionality	11.2.1	11.3.0	C1-120851
2012-03	CP-55	CP-120115	3969	2	Add S-CSCF support for RFC 6140 mainline GIN registration functionality	11.2.1	11.3.0	C1-120852
2012-03	CP-55	CP-120119	3970	3	Introduction of MRB functional entity	11.2.1	11.3.0	C1-120896
2012-06	CP-56	CP-120299	3896	2	Reference update for MIKEY_TICKET RFC	11.3.0	11.4.0	C1-121104
2012-06	CP-56	CP-120314	3904	6	P-Served-User and session case	11.3.0	11.4.0	C1-122360
2012-06	CP-56	CP-120307	3946	2	P-CSCF releasing the session when resource is lost	11.3.0	11.4.0	C1-121545
2012-06	CP-56	CP-120307	3952	8	Correcting procedure for propagating service profile update to the UE	11.3.0	11.4.0	C1-122450
2012-06	CP-56	CP-120324	3971	6	Addition of the transit and roaming function	11.3.0	11.4.0	C1-122413
2012-06	CP-56	CP-120323	3975	4	PANI header support of network provided location information	11.3.0	11.4.0	C1-122508
2012-06	CP-56	CP-120323	3976	4	Distribution of location information- AS procedures	11.3.0	11.4.0	C1-122509
2012-06	CP-56	CP-120289	3983		Correction on SDP Profile Status	11.3.0	11.4.0	C1-121042
2012-06	CP-56	CP-120314	3984	1	Editorial correction on SDP Profile Status	11.3.0	11.4.0	C1-121540
2012-06	CP-56	CP-120286	3989		GRUU: S-CSCF URI matching	11.3.0	11.4.0	C1-121054
2012-06	CP-56	CP-120284	3993	1	Reference update: draft-salud-alert-info-urns	11.3.0	11.4.0	C1-121416
2012-06	CP-56	CP-120307	3997	2	Restoration procedures missing in entry IBCF	11.3.0	11.4.0	C1-122250
2012-06	CP-56	CP-120306	3998	2	Missing emergency call procedure in S-CSCF	11.3.0	11.4.0	C1-121658
2012-06	CP-56	CP-120324	4000	6	Loopback routeing	11.3.0	11.4.0	C1-122412
2012-06	CP-56	CP-120322	4005	1	Removal of EN regarding PUI format	11.3.0	11.4.0	C1-121529
2012-06	CP-56	CP-120303	4011		Correcting implementation error, dai parameter	11.3.0	11.4.0	C1-121178
2012-06	CP-56	CP-120307	4012		E-CSCF handling of PAI in responses	11.3.0	11.4.0	C1-121179
2012-06	CP-56	CP-120307	4013		Editorial corrections to 24.229	11.3.0	11.4.0	C1-121190
2012-06	CP-56	CP-120314	4018	1	Correcting incorrect references in P-CSCF procedures when emergency call failure occurs	11.3.0	11.4.0	C1-121406
2012-06	CP-56	CP-120314	4019	7	Correcting IBCF and profile tables for use of 3GPP IM CN subsystem XML body in restoration procedures	11.3.0	11.4.0	C1-122415
2012-06	CP-56	CP-120322	4020	7	Addition of GRUU procedures for RFC6140 procedures	11.3.0	11.4.0	C1-122480
2012-06	CP-56	CP-120286	4025	1	Correcting contradictory statements regarding GRUU handling by IBCF	11.3.0	11.4.0	C1-121411
2012-06	CP-56	CP-120314	4026	2	Transparent passing of contact feature tags by B2BUA AS	11.3.0	11.4.0	C1-121719

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2012-06	CP-56	CP-120307	4027	1	Use of Contact Parameters in a 3XX Response from an LRF	11.3.0	11.4.0	C1-121546
2012-06	CP-56	CP-120301	4030	1	Reference update: draft-ietf-avtcore-ecn-for-rtp	11.3.0	11.4.0	C1-122285
2012-06	CP-56	CP-120427	4031	2	Update to reference titles in TS 24.229	11.3.0	11.4.0	-
2012-06	CP-56	CP-120314	4032	1	Transparency to GRUU of B2BUA AS	11.3.0	11.4.0	C1-122369
2012-06	CP-56	CP-120314	4033	2	Addressing potential abuse of 3xx responses	11.3.0	11.4.0	C1-122414
2012-06	CP-56	CP-120303	4038	2	Correcting ambiguity in restoration procedures definitions	11.3.0	11.4.0	C1-122445
2012-06	CP-56	CP-120307	4041	1	Adding the related-icid in charging overview	11.3.0	11.4.0	C1-122365
2012-06	CP-56	CP-120295	4045		Updating of UUS references	11.3.0	11.4.0	C1-121944
2012-06	CP-56	CP-120292	4049		IETF reference update (mixer-control)	11.3.0	11.4.0	C1-121948
2012-06	CP-56	CP-120290	4058	1	Correction on profile of REFER request	11.3.0	11.4.0	C1-122268
2012-06	CP-56	CP-120314	4059		Contact header field parameter values	11.3.0	11.4.0	C1-121970
2012-06	CP-56	CP-120314	4064	1	Adding 3gpp body xml schema to archive	11.3.0	11.4.0	C1-122372
2012-06	CP-56	CP-120314	4069	3	New technology annex when using the EPC via WLAN to access IM CN subsystem	11.3.0	11.4.0	C1-122513
2012-06	CP-56	CP-120290	4074		Handling of EN relating to granularity of access class	11.3.0	11.4.0	C1-122089
2012-06	CP-56	CP-120314	4075	2	Provision of access-type values in the P-CSCF, and Support of network location reporting for IMS functionality over GxGxx interfaces	11.3.0	11.4.0	C1-122491
2012-06	CP-56	CP-120314	4076	2	Correction to the technology annex when using I- WLAN to access IM CN subsystem	11.3.0	11.4.0	C1-122486
2012-06	CP-56	CP-120314	4077		P-CSCF handling UE port along with IP address during registration	11.3.0	11.4.0	C1-122116
2012-06	CP-56	CP-120307	4079	2	Use of Contact Parameters in a 3XX Response from an LRF	11.3.0	11.4.0	C1-122499
2012-09	CP-57	CP-120583	4039	5	SMS domain selection	11.4.0	11.5.0	C1-123296
2012-09	CP-57	CP-120566	4068	5	Emergency sub-service type handling	11.4.0	11.5.0	C1-123416
2012-09	CP-57	CP-120597	4078	1	Support of MRB Query mode in 3GPP TS 24.229	11.4.0	11.5.0	C1-122938
2012-09	CP-57	CP-120603	4082	2	Application servers and RAVEL	11.4.0	11.5.0	C1-123288
2012-09	CP-57	CP-120586	4083	1	Annex A updates for USSI	11.4.0	11.5.0	C1-123264
2012-09	CP-57	CP-120588	4084	1	Correction of correction to profile tables for use of 3GPP IM CN subsystem XML body in restoration procedures	11.4.0	11.5.0	C1-123172
2012-09	CP-57	CP-120588	4085	1	Correcting profile tables for use of 3GPP IM CN subsystem XML body in response to request for emergency services	11.4.0	11.5.0	C1-123168
2012-09	CP-57	CP-120582	4088	2	Reference update and technical changes: draft-ietf-sipcore-proxy-feature	11.4.0	11.5.0	C1-123348
2012-09	CP-57	CP-120601	4089	1	Annex A: P-Access-Network-Info in ACK	11.4.0	11.5.0	C1-123256
2012-09	CP-57	CP-120569	4094	1	Correction of SDP Profile about RFC 4145	11.4.0	11.5.0	C1-123104
2012-09	CP-57	CP-120582	4097	1	Feature-Caps header field part of trust domain	11.4.0	11.5.0	C1-123158

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2012-09	CP-57	CP-120599	4098		Removing an EN regarding missing charging related headers	11.4.0	11.5.0	C1-122680
2012-09	CP-57	CP-120603	4099		Removing an EN regarding preservation of parameters in AS	11.4.0	11.5.0	C1-122686
2012-09	CP-57	CP-120603	4100		Removing EN regarding number normalization and enum translation	11.4.0	11.5.0	C1-122687
2012-09	CP-57	CP-120603	4107	1	IOI usage between TRF and terminating side	11.4.0	11.5.0	C1-123284
2012-09	CP-57	CP-120603	4108	1	Co-location of TRF	11.4.0	11.5.0	C1-123285
2012-09	CP-57	CP-120569	4114	1	Correct handling of PPR in S-CSCF	11.4.0	11.5.0	C1-123109
2012-09	CP-57	CP-120583	4115	1	Correction ue initiated deregistration	11.4.0	11.5.0	C1-123295
2012-09	CP-57	CP-120577	4118	1	Condition for usage of Session-ID header filed within MESSAGE response	11.4.0	11.5.0	C1-123134
2012-09	CP-57	CP-120597	4119		Reference update: draft-ietf-mediactrl-mrb	11.4.0	11.5.0	C1-122765
2012-09	CP-57	CP-120597	4120	3	Visited network MRB information	11.4.0	11.5.0	C1-123396
2012-09	CP-57	CP-120583	4121	3	PCSCF discovery clarification	11.4.0	11.5.0	C1-123440
2012-09	CP-57	CP-120600	4122	2	Clarifications of used identities for registration procedures	11.4.0	11.5.0	C1-123355
2012-09	CP-57	CP-120588	4123	3	DVB-RCS2 satellite access network as IP-CAN for IMS	11.4.0	11.5.0	C1-123428
2012-09	CP-57	CP-120600	4124	3	Add reg-event changes for RFC 6140	11.4.0	11.5.0	C1-123378
2012-09	CP-57	CP-120583	4126	1	P-CSCF registration context lost	11.4.0	11.5.0	C1-123297
2012-09	CP-57	CP-120588	4131	1	Correction DHCP mechanism for P-CSCF discovery in Annex M	11.4.0	11.5.0	C1-123293
2012-09	CP-57	CP-120588	4132	1	Correction to DHCP mechanism for P-CSCF discovery in Annex O	11.4.0	11.5.0	C1-123294
2012-09	CP-57	CP-120588	4133		Correction to Annex 9.2	11.4.0	11.5.0	C1-122849
2012-09	CP-57	CP-120570	4137	1	Reference update: draft-ietf-mmusic-ice-tcp	11.4.0	11.5.0	C1-123130
2012-09	CP-57	CP-120601	4140	1	Network provided location information inserted by the MSC server enhanced for ICS	11.4.0	11.5.0	C1-123259
2012-09	CP-57	CP-120591	4146		Specification of ISC gateway function – general clauses	11.4.0	11.5.0	C1-122928
2012-09	CP-57	CP-120591	4147	1	Specification of ISC gateway function – SIP procedures	11.4.0	11.5.0	C1-123271
2012-09	CP-57	CP-120591	4148	1	Specification of application gateway function – SDP procedures	11.4.0	11.5.0	C1-123272
2012-09	CP-57	CP-120588	4151		Reversal of terminology change in annex D	11.4.0	11.5.0	C1-122939
2012-09	CP-57	CP-120588	4152	1	Emergency priority using the Resource-Priority header field	11.4.0	11.5.0	C1-123173
2012-09	CP-57	CP-120641	4153	3	Description of overload control	11.4.0	11.5.0	-
2012-09	CP-57	CP-120642	4154	3	Support of overload control	11.4.0	11.5.0	-
2012-09	CP-57	CP-120664	4156	5	Media plane security	11.4.0	11.5.0	-
2012-09	CP-57	CP-120576	4159	1	mediasec ref deletions	11.4.0	11.5.0	C1-123141
2012-09	CP-57	CP-120603	4162		Updates to charging introduction for RAVEL	11.4.0	11.5.0	C1-122968

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2012-09	CP-57	CP-120588	4163	1	Condition for restoration procedures causing UE reregistration	11.4.0	11.5.0	C1-123174
2012-09	CP-57	CP-120588	4164	1	Missing procedure for NASS-IMS bundled authentication at S-CSCF	11.4.0	11.5.0	C1-123171
2012-09	CP-57	CP-120574	4180	2	Emergency and normal registration independence	11.4.0	11.5.0	C1-123374
2012-09	CP-57	CP-120606	4185	2	Support of T.38 related SDP attributes	11.4.0	11.5.0	C1-123400
2012-09	CP-57	CP-120578	4188		Correcting incorrect references in P-CSCF procedures when emergency call failure occurs	11.4.0	11.5.0	C1-123164
2012-09	CP-57	CP-120656	4189	1	Reference list correction to align with the corrected TS 29.212 title	11.4.0	11.5.0	-
2012-12	CP-58	CP-120802	4106	5	Additional guidance on use of 3xx responses	11.5.0	11.6.0	C1-124983
2012-12	CP-58	CP-120802	4127	2	Update the general requirements for tunnel procedures	11.5.0	11.6.0	C1-123886
2012-12	CP-58	CP-120802	4128	4	IP address obtained on S2a interface	11.5.0	11.6.0	C1-124274
2012-12	CP-58	CP-120802	4129	4	Tunnel modification by the UE	11.5.0	11.6.0	C1-124275
2012-12	CP-58	CP-120802	4130	5	Tunnel modification by the network	11.5.0	11.6.0	C1-124276
2012-12	CP-58	CP-120804	4149	3	Specification of ISC gateway function – SIP profile	11.5.0	11.6.0	C1-124261
2012-12	CP-58	CP-120804	4150	2	Specification of application gateway function – SDP profile	11.5.0	11.6.0	C1-124100
2012-12	CP-58	CP-120787	4187	1	IANA registration of OMR parameters	11.5.0	11.6.0	C1-123575
2012-12	CP-58	CP-120783	4196		Delete IETF mediasec draft reference	11.5.0	11.6.0	C1-123520
2012-12	CP-58	CP-120783	4197		IMS media security profile table cleanup	11.5.0	11.6.0	C1-123521
2012-12	CP-58	CP-120793	4201	4	Contents of From and To header fields in SUBSCRIBE message	11.5.0	11.6.0	C1-124950
2012-12	CP-58	CP-120802	4202	4	Correction on handling of rn parameter and npdi parameter at S-CSCF.	11.5.0	11.6.0	C1-125015
2012-12	CP-58	CP-120821	4203	2	Support of T.38 SDP attributes in IMS	11.5.0	11.6.0	C1-124158
2012-12	CP-58	CP-120801	4204	1	Transit-ioi is removed from fowarded message to visited network	11.5.0	11.6.0	C1-124092
2012-12	CP-58	CP-120815	4205	5	Overload control clarifications	11.5.0	11.6.0	C1-125010
2012-12	CP-58	CP-120812	4206	3	Removing ENs about IBCF and OMR	11.5.0	11.6.0	C1-124262
2012-12	CP-58	CP-120812	4207		Removing an EN regarding PSI	11.5.0	11.6.0	C1-123620
2012-12	CP-58	CP-120812	4212		Correcting the UE-originating case indication	11.5.0	11.6.0	C1-123630
2012-12	CP-58	CP-120793	4214	6	Correcting procedures for re-establishment a context for SIP signalling	11.5.0	11.6.0	C1-124952
2012-12	CP-58	CP-120773	4219	4	Correction of emergency sub-service type handling	11.5.0	11.6.0	C1-124284
2012-12	CP-58	CP-120793	4220	2	Remaining corrections to emergency sub-service type handling	11.5.0	11.6.0	C1-124181
2012-12	CP-58	CP-120782	4223	2	Corrections to E-CSCF and LRF handling for emergency calls	11.5.0	11.6.0	C1-124764
2012-12	CP-58	CP-120812	4224		Application servers and RAVEL	11.5.0	11.6.0	C1-123577

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2012-12	CP-58	CP-120777	4228	1	Correction of 3GPP IM CN subsystem XML handling	11.5.0	11.6.0	C1-123972
2012-12	CP-58	CP-120793	4229	3	PCSCF discovery Annex L editorial	11.5.0	11.6.0	C1-124989
2012-12	CP-58	CP-120776	4234		Table A.162, item 61 referencing incorrect document	11.5.0	11.6.0	C1-123669
2012-12	CP-58	CP-120802	4235	1	SDP impacts due to IP-CAN bearer release	11.5.0	11.6.0	C1-124006
2012-12	CP-58	CP-120802	4236	1	Precondition and INVITE without SDP offer	11.5.0	11.6.0	C1-124007
2012-12	CP-58	CP-120802	4237	1	User rejecting media stream during set up of multimedia session	11.5.0	11.6.0	C1-124008
2012-12	CP-58	CP-120812	4239	1	Decission on loop back routing in S-CSCF	11.5.0	11.6.0	C1-124102
2012-12	CP-58	CP-120793	4241	1	Correct Defintion of Temporarily Authorized Resource-Priority	11.5.0	11.6.0	C1-124003
2012-12	CP-58	CP-120791	4243	2	Reference update: draft-ietf-sipcore-proxy-feature	11.5.0	11.6.0	C1-124766
2012-12	CP-58	CP-120791	4244	1	Feature-Caps header field in target refresh requests and responses	11.5.0	11.6.0	C1-124122
2012-12	CP-58	CP-120804	4247	1	Specification of application gateway function – SDP procedures	11.5.0	11.6.0	C1-124098
2012-12	CP-58	CP-120810	4248	1	Profiles change for P-Access-Network-Info header	11.5.0	11.6.0	C1-124111
2012-12	CP-58	CP-120810	4249	3	Correction to the coding of UE-time-zone	11.5.0	11.6.0	C1-124273
2012-12	CP-58	CP-120810	4250	2	Removal of Editor's Note on NPLI inserted by both P-CSCF and AS	11.5.0	11.6.0	C1-124223
2012-12	CP-58	CP-120793	4251	1	Correct emergency call description when roaming	11.5.0	11.6.0	C1-124116
2012-12	CP-58	CP-120782	4254		Dialog state notification clarification	11.5.0	11.6.0	C1-123752
2012-12	CP-58	CP-120785	4257	1	Emergency and normal registration independence	11.5.0	11.6.0	C1-123994
2012-12	CP-58	CP-120815	4258	5	Overload control -Inconstancies correction	11.5.0	11.6.0	C1-125009
2012-12	CP-58	CP-120815	4262	3	Event-based overload control procedures	11.5.0	11.6.0	C1-124856
2012-12	CP-58	CP-120780	4263	2	Correction to integrity-protected usage in S-CSCF	11.5.0	11.6.0	C1-124150
2012-12	CP-58	CP-120809	4273		Mz Reference Point – ISC alternative	11.5.0	11.6.0	C1-124301
2012-12	CP-58	CP-120812	4275	1	Removing the g.3gpp.loopback in TRF	11.5.0	11.6.0	C1-124850
2012-12	CP-58	CP-120788	4281		Reference update: RFC 6679	11.5.0	11.6.0	C1-124369
2012-12	CP-58	CP-120775	4285	3	Updating IMEI URN draft reference	11.5.0	11.6.0	C1-125006
2012-12	CP-58	CP-120793	4286	2	Default ICSI value selected by S-CSCF	11.5.0	11.6.0	C1-124951
2012-12	CP-58	CP-120810	4287		Correction of "UE-time-zone" to "local-time-zone" in TS 24.229	11.5.0	11.6.0	C1-124433
2012-12	CP-58	CP-120801	4288		Transit IOI general description	11.5.0	11.6.0	C1-124439
2012-12	CP-58	CP-120801	4289	1	Including transit-IOI in SIP responses	11.5.0	11.6.0	C1-124843
2012-12	CP-58	CP-120802	4294	1	Removal of internal references from IBCF procedures	11.5.0	11.6.0	C1-124772

Change history								
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2012-12	CP-58	CP-120815	4296	2	Closure of open issues in IOC work item	11.5.0	11.6.0	C1-125008
2012-12	CP-58	CP-120793	4299	1	P-CSCF registration context lost – text correction	11.5.0	11.6.0	C1-124896
2012-12	CP-58	CP-120793	4300		NAT detection by the UE- text correction	11.5.0	11.6.0	C1-124521
2012-12	CP-58	CP-120780	4305		Correction on integrity-protected handling in S-CSCF	11.5.0	11.6.0	C1-124528
2012-12	CP-58	CP-120793	4311	1	Correction to challenge response examination in P-CSCF	11.5.0	11.6.0	C1-124903
2014-03-22	Deutsche Telekom	FMED-321			Complete revision of Annex and change of baseline to Release 11	Draft 1.0.0	Version Final 2.0.0	