**3GPP TSG-CT WG1 Meeting #129-eC1-212280\_r1**

**Electronic meeting, 19-23 April 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.229** | **CR** | **6518** | **rev** | **1** | **Current version:** | **17.2.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | Support for signed attestation for priority and emergency sessions |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | TEI17\_SAPES |  | ***Date:*** | 2021-03-31 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | SA2 defined requirements:- to support assertion, signing and verification of "Resource-Priority" header field for emergency, emergency callback, and priority IMS sessions;- to support assertion, signing and verification of "Priority" header field value "psap-callback" for emergency callback; and- extending the mechanism for attestation and signing of originating calling identification information using STIR/SHAKEN to apply it to emergency, emergency callback, and priority IMS sessions. |
|  |  |
| ***Summary of change:*** | Added:* support of RFC 8443 and draft-ietf-stir-rph-emergency-services;
* definition of "Priority verification using assertion of priority information" feature (similar to "Calling number verification using signature verification and attestation information" feature);
* if the the P‑CSCF received an an initial request from the user which performed an emergency registration, the P-CSCF may, based on operator policy, insert attestation information related to the asserted calling identity associated with an emergency session;
* that the AS may, based on operator policy, perform attestation of the user identity associated with an emergency session and add a Resource-Priority header field;
* if the IBCF included the Priority header field with a "psap-callback" header field value, the IBCF shall, based on operator policy, add a Resource-Priority header field containing a namespace of "esnet";
* for an emergency, emergency callback and priority IMS sessions received by an exit IBCF, the exit IBCF invokes an AS via the Ms reference point for the signing of Resource-Priority information and "Priority" header field value "psap-callback" (if present);
* for an emergency, emergency callback and priority IMS sessions received by an entry IBCF, the entry IBCF invokes an AS via the Ms reference point for the verification of an Identity header field associated with the Resource-Priority header field and with the header field value "psap-callback" of the Priority header field (if present).

Clauses in annex V are accordingly updated and a new verstatPriority claim is introduced within the verificationResponse to transport the verification value of the Resource-Priority header field and optionally the Priority header field set to the value "psap-callback". For the transport of the same information within SIP request a new Priority-Verstat header field is introduced. |
|  |  |
| ***Consequences if not approved:*** | Not complying to stage 2 requirements to support signed attestation for priority IMS sessions and emergency sessions. |
|  |  |
| ***Clauses affected:*** | 2, 3.1, 4.4.1, 4.4.6, 4.4.x (new), 4.11, 5.2.10.3, 5.7.1.14, 5.7.1.25, 5.7.1.25.1, 5.10.1, 5.10.10.2, 5.10.10.3, 7.2.x (new), 7.13.x (new), V.2.1, V.2.2, V.2.5.2, V.2.6.1, V.2.6.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\* First Change \*\*\*

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 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)".

[1C] 3GPP TS 22.011: "Service accessibility".

[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".

[7G] 3GPP TS 24.103: "Telepresence using the IP Multimedia (IM) Core Network (CN) Subsystem (IMS); Stage 3".

[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".

[8Y] 3GPP TS 24.322: "UE access to IMS services via restrictive access networks - stage 3".

[8Z] 3GPP TS 24.371: "Web Real Time Communication (WebRTC) Access to IMS".

[8ZA] 3GPP TS 24.525: "Business trunking; Architecture and functional description".

[8ZB] 3GPP TS 24.244: "Wireless LAN control plane protocol for trusted WLAN access to EPC; Stage 3".

[8ZC] 3GPP TS 24.337: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) inter-UE transfer; Stage 3".

[8ZD] 3GPP TS 24.334: "Proximity-services (ProSe) User Equipment (UE) to Proximity-services (ProSe) Function Protocol aspects; Stage 3".

[8ZE] 3GPP TS 24.379: "Mission Critical Push To Talk (MCPTT) call control; Stage 3".

[8ZF] 3GPP TS 24.628: "Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[8ZG] 3GPP TS 24.604: "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[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".

[9B] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[9C] 3GPP TS 26.267: "eCall Data Transfer; In-band modem solution; General description".

[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".

[12A] 3GPP TS 29.273: "Evolved Packet System (EPS); 3GPP EPS AAA interfaces".

[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".

[19D] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[19E] 3GPP TS 36.413: "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)".

[19F] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[19G] 3GPP TS 38.331: " NR; Radio Resource Control (RRC); Protocol specification".

[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 6665 (July 2012): "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 7315 (July 2014): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP".

[52A] RFC 7976 (September 2016): "Updates to Private Header (P-Header) Extension Usage in Session Initiation Protocol (SIP) Requests and Responses".

[52B] draft-jesske-update-p-visited-network-01 (March 2019): "Update to Private Header Field P-Visited-Network-ID in Session Initiation Protocol (SIP) Requests and Responses".

Editor's note (WI: IMSProtoc9, CR#5979): The above document cannot be formally referenced until it is published as an RFC.

[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 7044 (February 2014): "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 Emergency and Other Well-Known 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.S0057-B v2.0: "E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects".

[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.S0059-200-A v1.0: "cdma2000 Femtocell Network: 1x and IMS Network Aspects".

[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 (V1.1.1): "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] Void.

[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] RFC 7433 (January 2015): "A Mechanism for Transporting User-to-User Call Control Information in SIP".

[126A] RFC 7434 (January 2015): "Interworking ISDN Call Control User Information with SIP".

[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] RFC 7316 (July 2014): "The Session Initiation Protocol (SIP) P-Private-Network-Indication PrivateHeader (P-Header)".

[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] RFC 8497 (November 2018): "Marking SIP Messages to Be Logged".

[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] RFC 7254 (May 2014): "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".

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

[155] RFC 7195 (May 2014): "Session Description Protocol (SDP) Extension for Setting Audio Media Streams over Circuit-Switched Bearers in the Public Switched Telephone Network (PSTN)".

[156] RFC 7006 (September 2013): "Miscellaneous Capabilities Negotiation in the Session Description Protocol (SDP)".

[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] RFC 7989 (October 2016): "End-to-End Session Identification in IP-Based Multimedia Communication Networks".

[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] RFC 6871 (February 2013): "SDP media capabilities Negotiation".

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

[174] Void.

[175] RFC 7462 (March 2015): "URNs for the Alert-Info Header Field of the Session Initiation Protocol (SIP)".

[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] RFC 8464 (September 2018): "A URN Namespace for Device Identity and Mobile Equipment Identity (MEID)".

[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] RFC 6809 (November 2012): "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)".

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

[192] RFC 6917 (April 2013): "Media Resource Brokering".

[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 Specification".

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

[197] RFC 7135 (May 2014): "IANA Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications".

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

[199] RFC 7339 (September 2014): "Session Initiation Protocol (SIP) Overload Control".

[200] RFC 7415 (February 2015): "Session Initiation Protocol (SIP) Rate Control".

[201] RFC 7200 (April 2014): "A Session Initiation Protocol (SIP) Load-Control Event Package".

[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".

[204] RFC 5506 (April 2009): "Support for Reduced-Size Real-Time Transport Control Protocol (RTCP)".

[205] RFC 3611 (November 2003): "RTP Control Protocol Extended Reports (RTCP XR)".

[206] RFC 4796 (February 2007): "The Session Description Protocol (SDP) Content Attribute".

[207] ISO 3166-1 (2006): "Codes for the representation of names of countries and their subdivisions – Part 1: Country codes".

[208] RFC 8055 (January 2017): "Session Initiation Protocol (SIP) Via Header Field Parameter to Indicate Received Realm".

[209] RFC 7090 (April 2014): "Public Safety Answering Point (PSAP) Callback".

[210] RFC 5285 (July 2008): "A General Mechanism for RTP Header Extensions".

[211] RFC 6236 (May 2011): "Negotiation of Generic Image Attributes in the Session Description Protocol (SDP)".

[212] RFC 20 (May 2011): "ASCII format for Network Interchange".

[213] RFC 5280 (May 2008): "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[214] RFC 6714 (August 2012): "Connection Establishment for Media Anchoring (CEMA) for the Message Session Relay Protocol (MSRP)".

[215] RFC 6135 (February 2011): "An Alternative Connection Model for the Message Session Relay Protocol (MSRP)".

[216] Void.

[217] RFC 7345 (August 2014): "UDP Transport Layer (UDPTL) over Datagram Transport Layer Security (DTLS)".

[218] RFC 4279 (December 2005): "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".

[219] RFC 8841 (January 2021): "Session Description Protocol (SDP) Offer/Answer Procedures for Stream Control Transmission Protocol (SCTP) over Datagram Transport Layer Security (DTLS) Transport".

[220] RFC 2817 (May 2000): "Upgrading to TLS Within HTTP/1.1".

[221] RFC 6062 (November 2010): "Using Relays around NAT (TURN) Extensions for TCP Allocations".

[222] RFC 5763 (May 2010): "Framework for Establishing a Secure Real-time Transport Protocol (SRTP) Security Context Using Datagram Transport Layer Security (DTLS)".

[223] RFC 5764 (May 2010): " Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)".

[224] RFC 7675 (October 2015): "STUN Usage for Consent Freshness".

[225] RFC 7549 (May 2015): "3GPP SIP URI Inter Operator Traffic Leg Parameter".

[226] Void.

[227] RFC 4169 (November 2005): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2".

[228] RFC 6947 (May 2013): "The Session Description Protocol (SDP) Alternate Connectivity (ALTC) Attribute".

[229] Void.

[230] RFC 8119 (March 2017): "SIP "cause" URI Parameter for Service Number Translation".

[231] RFC 7647 (September 2015): "Clarifications for the Use of REFER with RFC6665".

[232] RFC 7614 (August 2015): "Explicit Subscriptions for the REFER Method".

[233] RFC 7621 (August 2015): "A Clarification on the Use of Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP) Event Notification Framework".

[234] RFC 7913 (June 2016): "P-Access-Network-Info ABNF Update".

[235] RFC 7519 (May 2015): "JSON Web Token (JWT)".

[236] Void.

[237] RFC 5761 (April 2010): "Multiplexing RTP Data and Control Packets on a Single Port".

[237A] RFC 8035 (November 2016): "Session Description Protocol (SDP) Offer/Answer Clarifications for RTP/RTCP Multiplexing".

[238] RFC 8864 (January 2021): " Negotiation Data Channels Using the Session Description Protocol (SDP)".

[239] RFC 8498 (February 2019): "A P-Served-User Header Field Parameter for an Originating Call Diversion (CDIV) Session Case in the Session Initiation Protocol (SIP)".

[240] RFC 8842 (January 2021): "Session Description Protocol (SDP) Offer/Answer Considerations for Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS)".

[241] RFC 8122 (March 2017): "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)".[242] RFC 3863 (August 2004): "Presence Information Data Format".

[243] RFC 4661 (September 2006): "An Extensible Markup Language (XML) Based Format for Event Notification Filtering".

[244] RFC 8147 (May 2017): "Next-Generation Pan-European eCall".

[245] CEN EN 15722:2015 (April 2015): "Intelligent transport systems - ESafety - ECall minimum set of data".

[246] RFC 8858 (January 2021): "Indicating Exclusive Support of RTP and RTP Control Protocol (RTCP) Multiplexing Using the Session Description Protocol (SDP)".

[247] RFC 7303 (July 2014): "XML Media Types".

[248] IEEE Std 802.11-2016: "IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[249] RFC 8853 (January 2021): "Using Simulcast in Session Description Protocol (SDP) and RTP Sessions".

[250] RFC 8851 (January 2021): "RTP Payload Format Restrictions".

[251] RFC 7728 (February 2016): "RTP Stream Pause and Resume".

[252] RFC 8224 (February 2018): "Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[253] RFC 5279 (July 2008): "A Uniform Resource Name (URN) Namespace for the 3rd Generation Partnership Project (3GPP)".

[254] RFC 8197 (July 2017): "A SIP Response Code for Unwanted Calls".

[255] RFC 8606 (June 2019): "ISDN User Part (ISUP) Cause Location Parameter for the SIP Reason Header Field".

[256] RFC 8262 (October 2017): "Content-ID Header Field in the Session Initiation Protocol (SIP)".

[257] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[258] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (5GS); Stage 3".

[259] RFC 4715 (November 2006): "The Integrated Services Digital Network (ISDN) Subaddress Encoding Type for tel URI".

[260] 3GPP TS 38.304: " NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state".

[261] RFC 8588 (May 2019): "Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)".

[262] RFC 8225 (February 2018): "PASSporT: Personal Assertion Token"

[263] 3GPP TS 24.502: " Access to the 3GPP 5G Core Network (5GCN) via Non-3GPP Access Networks (N3AN); Stage 3".

[264] 3GPP TS 37.340: "Evolved Universal Terrestrial Radio Access (E-UTRA) and NR; Multi-connectivity; Stage 2".

[265] RFC 8946 (February 2021): "Personal Assertion Token (PASSporT) Extension for Diverted Calls".

[266] RFC 8787 (May 2020): "Location Source Parameter for the SIP Geolocation Header Field".

[267] RFC 5491 (March 2009): "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations".

[268] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[269] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[270] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description; Stage 2".

[271] 3GPP TS 38.321: "NR; Medium Access Control (MAC) protocol specification".

[272] 3GPP TS 23.221: "Architectural requirements".

[273] 3GPP TS 29.514: "5G System; Policy Authorization Service; Stage 3".

[274] 3GPP TS 29.562: "Home Subscriber Server (HSS) Services for Interworking with the IP Multimedia Subsystem (IMS); Stage 3".

[275] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[276] 3GPP TS 26.238: "Uplink Streaming".

[277] IETF RFC 4574 (August 2006): "The Session Description Protocol (SDP) Label Attribute".

[nn1] RFC 8443 (August 2018): "Personal Assertion Token (PASSporT) Extension for Resource Priority Authorization".

[nn2] IETF draft-ietf-stir-rph-emergency-services-07 (March 2021): "Assertion Values for a Resource Priority Header Claim and a SIP Priority Header Claim in Support of Emergency Services Networks".

Editor's note [WI: TEI17\_SAPES, CR #tba]: The above document cannot be formally referenced until it is published as an RFC.

\*\*\* Next Change \*\*\*

## 3.1 Definitions

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

**3GPP PS data off status:** indicates state of usage of the 3GPP PS data off. 3GPP PS data off status at the UE can be either "active" or "inactive".

**Country**: For the purposes of emergency service URNs in the present document, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], an ISO 3166-1 alpha-2 code as specified in ISO 3166-1 [207] is used to identify a region or a country.

**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 RFC 8464 [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 3 or 4 when forwarding requests towards the UE. According to 3GPP TS 33.203 [19], flow 2 is only used for UE generated requests and 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]).

**HSS based P-CSCF restoration procedures:** the procedures for the IP-CAN, the IM CN subsystem, the HSS and the UE to handle P-CSCF service interruption scenarios (see 3GPP TS 23.380 [7D]). In 5GS the procedure is called UDM/HSS based P-CSCF restoration (see 3GPP TS 23.380 [7D]) since the UDM participates in the procedure.

**PCRF based P-CSCF restoration procedures:** the procedures for the IP-CAN, the IM CN subsystem, the PCRF and the UE to handle P-CSCF service interruption scenarios (see 3GPP TS 23.380 [7D]). In 5GS the procedure is called PCF based P-CSCF restoration (see 3GPP TS 23.380 [7D]) since the PCF takes the role of the PCRF.

**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.

**Privileged sender:** A privileged 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].

**UE performing the functions of an external attached network:** an independent network connected to an IMS network over the Gm interface, through a single point and which is seen by the IMS network as a specific UE; e.g. an IP-PBX.

**Static Mode of Operation:** a mode of operation where the UE performing the functions of an external attached network does not initiate any IMS level registration procedures towards the operator IMS.

**Canonical form of a SIP URI**: Canoncial form of a SIP URI takes the form "sip:username@domain" as specified in RFC 3261 [26] subclause 10.3. SIP URI comparisons are performed as defined in RFC 3261 [26] subclause 19.1.4.

**Originating home network:** the home network of a user originating a transaction, and if applicable, the associated dialog.

**Originating visited network:** the visited network of a user originating a transaction, and if applicable, the associated dialog.

**Terminating home network:** the home network of a user terminating a transaction, and if applicable, the associated dialog.

**Terminating visited network:** the visited network of a user terminating a transaction, and if applicable, the associated dialog.

**Type of emergency service**: The type of emergency service is either an emergency call type standardized by 3GPP (see 3GPP TS 22.101 [8] subclause 10.1) or a similar capability not standardised by 3GPP and defined by national regulatory requirements. The generic (sos) service, identified by urn:service:sos, does not have a type of emergency service (even though usage of the generic (sos) service in the emergency call is defined).

**Resource sharing:** one dedicated EPS bearer is sharing resources among several ongoing sessions such that the highest GBR (and optionally MBR) to be shared for the set of PCC/QoS rules bound to the same bearer is used as input for the calculation of the GBR (and optionally MBR) of that bearer among the sessions sharing the resources.

**Fully-Qualified Domain Name (FQDN):** the syntax of the FQDN used in this specification is defined in RFC 3261 [26] subclause 25.1.

**Trusted WLAN:** A trusted non-3GPP access, where the non-3GPP access is a WLAN IP access.

**Untrusted WLAN:** An untrusted non-3GPP access, where the non-3GPP access is a WLAN IP access.

**Calling number verification status determination:** A feature which enables the terminating UE to determine whether number has been verified by the network as specified in RFC 8224 [252].

**Calling number verification using** **signature verification and attestation information**: A feature which enables a calling identity validation as specified in RFC 8224 [252] and uses an attestation information to vouch for the accuracy of the source of origin of the call. Attestation information consists of an attestation level and an origination identifier and may be included in the Identity header field as defined in RFC 8588 [261] and in the Attestation-Info and Origination-Id header fields as defined in subclauses 7.2.18 and 7.2.19.

**Priority verification using assertion of priority information**: A feature which enables validation of a priority level provided in the Resource-Priority header field as specified in RFC 8443 [nn1] and the header field value "psap-callback" provided in the Priority header field as specified in draft-ietf-stir-rph-emergency-services [nn2]. As defined in RFC 8443 [nn1] the Identity header field is used for the purpose of authentication of the Resource-Priority header field and by extension the Priority header field value "psap-callback".

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:

**Equivalent Home PLMN (EHPLMN)**

**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, 5.10, annex U, and annex W 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)**

**IMS Services for roaming users in deployments without IMS-level roaming interfaces**

**Local service number**

**IP-Connectivity Access Network (IP-CAN)**

**P-CSCF enhanced for WebRTC (eP-CSCF)**

**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**

**WebRTC IMS Client (WIC)**

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:

**eCall over IMS**

**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**

**spi\_uc**

**spi\_us**

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 3GPP TS 33.310 [19D] annex E and documents referenced therein:

**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**

**Persistent EPS bearer context**

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**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.302 [8U] apply:

**Restrictive non-3GPP access network**

**S2a**

**S2b**

**S2c**

**Trusted non-3GPP access**

**Untrusted non-3GPP access**

**Unauthenticated IMSI**

**Firewall traversal tunnel**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 32.240 [16] apply:

**Charging Data Function (CDF);**

**Charging Data Record (CDR)**

**Online Charging Function (OCF)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 32.260 [17] apply:

**IM CN subsystem Charging Identifier (ICID)**

For the purposes of the present document, the following terms and definitions given in RFC 8119 [230] apply:

**Service access number**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.101 [1A] apply:

**eCall**

**Minimum Set of Data (MSD)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 22.011 [1C] apply:

**3GPP PS data off**

**3GPP PS data off exempt services**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.402 [7E] apply.

**TWAN**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.604 [8ZG] apply.

**Diverting user**

**Diverted-to party**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.221 [272] apply:

**Restricted Local Operator Services**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.501 [257] apply:

**Stand-alone Non-Public Network**

\*\*\* Next Change \*\*\*

### 4.4.1 General

A trust domain can apply for specific header fields, tel URI parameters and SIP URI parameters within the IM CN subsystem.

For the IM CN subsystem, this trust domain consists of the functional entities that belong to the same operator's network (P-CSCF, the eP-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.

The trust domain can exist for a number of purposes:

a) for the protection of information specific to an operator;

b) to provide for privacy requirements of the end user; or

c) to ensure that information is only passed to another entity if certain responsibilities related to that information are met by the receiving entity, for example that the signalled requirements in the Privacy header field will be met (see subclause 4.4.2 and 4.4.4).

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 for that header field, tel URI parameter, or SIP URI parameter, 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, Feature-Caps, Restoration-Info, Relayed-Charge, Service-Interact-Info, Cellular-Network-Info, Response-Source, Attestation-Info, Origination-Id, Additional-Identity and Priority-Verstat. A trust domain applies for the purpose of the CPC and OLI tel URI parameters. A trust domain applies for the iotl SIP URI parameter. The trust domains of these header fields and parameters need not have the same boundaries. Clause 5 defines additional procedures concerning these header fields, tel URI parameters and SIP URI parameter.

\*\*\* Next Change \*\*\*

### 4.4.6 Resource-Priority

If Priority verification using assertion of priority information features described in subclause 3.1 is supported then a functional entity at the boundary of the trust domain will need to determine, based on the operator policy, whether to remove a Resource-Priority header field.

Otherwise, if Priority verification using assertion of priority information features described in subclause 3.1 is not supported 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.

\*\*\* Next Change \*\*\*

### 4.4.x Priority-Verstat header field

A functional entity at the boundary of the trust domain will need to determine whether to remove the Priority-Verstat header field according to subclause 7.2.x when SIP signalling crosses the boundary of the trust domain.

\*\*\* Next Change \*\*\*

## 4.11 Priority mechanisms

In support of priority, the IM CN subsystem uses the mechanisms of RFC 4412 [116]. The request for prioritisation of a transaction / dialog may, for some deployments, be marked with the Resource-Priority header field by the UE. For other deployments, the request is not marked for priority by the UE, but the request is instead identified as a priority request and marked for priority (via a Resource-Priority header field) by a functional entity (e.g., P-CSCF) within the network. Subsequent to successful authorisation at an authorisation point (e.g. AS), request is considered to be authorised.

The characteristics of any priority scheme is defined by the namespace that is used. This determines how priority is applied to the SIP signalling, to the bearer carrying the SIP signalling, and to the bearers carrying any media. Different priority levels exist within each namespace. Priority levels in one namespace have no relationship to the priority levels in any other namespace, i.e. priority level "1" in namespace "A" may have an entirely different level and characteristic of priority treatment to an identically labelled priority level "1" in namespace "B".

A network can support multiple namespaces. It is up to the network operator (potentially based on regulatory or contractural obligations) to define the relationship between the priority mechanisms for each namespace, and indeed with calls that are not given any priority. It is normal that prioritised calls do not have access to 100% of any available resource and indeed are limited to a much lower figure. Priority is optional, and this document places no requirement on a conformant IM CN subsystem implementation to support priority, or indeed any namespace in a priority scheme. Regulators can however place their own requirements on an operator. Emergency transactions or dialogs (see subclause 4.7) can also have their own priority scheme.

RFC 4412 [116] specifies several resource priority namespaces. For example, certain national MPS implementations use resource priority namespaces of ETS (Emergency Telecommunications Service) and WPS (Wireless Priority Service).

Several ways of using priority exist, depending on the authorisation mechanism adopted. These are identified as follows. In each of these authorisation means authorisation to use the service, the namespace, and the priority level within that namespace:

1) Authorisation based on subscription in the IM CN subsystem only, priority requested by the UE using the Resource Priority header field. Whether the user is allowed to use priority or not, and the appropriate namespace and priority levels, is stored as part of the user profile in the HSS. As part of the reg event package subscription, this information is given to the P-CSCF when the contact information for any public user identity changes, and based on this information, the P-CSCF acts as the authorisation point for priority on individual requests. At the P-CSCF, when a Resource-Priority header field is received from the UE, if the requested priority equates to a value (namespace and priority level) that the P-CSCF knows is allowed for that public user identity, the priority is authorised.

2) Authorisation based on a database deployed by an AS; priority requested by the UE using a special dialstring. In this case the user requires no priority subscription information in the HSS. Specific dialstrings are configured in the P-CSCF. When a request is received from the UE by the P-CSCF, if the request contains a specific dialstring that is recognised by the P-CSCF as being eligible for priority treatment, the request is marked for temporary priority, subject to subsequent authorisation by an authorisation point (i.e., AS). And all such requests are routed to an AS. Final authorisation is granted by the AS, based on a PIN or password exchange with the UE. Subsequent requests or responses after authorisation are only given priority by the P-CSCF and S-CSCF if some backwards indication is received for that specific dialog. The definition of this backwards indication is outside the scope of this document (because non-standardised mechanisms have already been implemented in association with this approach).

3) Authorisation based on subscription in the IM CN subsystem and on a database deployed by an AS; priority requested by the UE using a special dialstring. Specific dialstrings are configured in the P-CSCF. When a request is received from the UE by the P-CSCF, if the request contains a specific dialstring that is recognised by the P-CSCF as being eligible for priority treatment, the request is marked for temporary priority, subject to subsequent authorisation by an authorisation point (i.e., AS). Based on iFC functionality that exists at the S-CSCF (from the users subscription in the HSS), such requests are routed to an AS. Final authorisation is granted by the AS, based on a PIN or password exchange with the UE or based on user profile. Subsequent requests or responses after authorisation are only given priority by the P-CSCF and S-CSCF if some backwards indication is received for that specific dialog. The definition of this backwards indication is outside the scope of this document (because non-standardised mechanisms have already been implemented in association with this approach).

Some administrations can require the use of multiple approaches in the same network.

For the cases of interworking with other networks, where the P-CSCF of the other network does not support priority, but it is intended or required to give users of that P-CSCF priority in the home network, provision is made for recognition of dialstrings by the IBCF and the S-CSCF. In such scenarios, when the IBCF or S-CSCF recognize that a request contains a dialstring as being eligible for priority treatment, the request is marked by the IBCF or S-CSCF for temporary priority, subject to subsequent authorisation by an authorisation point (i.e. AS). This mechanism does not have an impact on the network where the P-CSCF resides.

Where the network has a requirement to prioritise emergency calls, it can either perform this function by the use of the "esnet" namespace in the Resource-Priority header field (as defined in RFC 7135 [197]), or by recognition of the presence of the service URN relating to an emergency. Where the Resource-Priority header field is used for this purpose, it is inserted by the entity identifying the emergency call, i.e. the P-CSCF or the IBCF. There is no usage of this namespace from the UE, and when this namespace is used, the trust domain implementation is set to remove it if it occurs from the UE.

Where the network has requirements on attestation and signing of originating calling identification information for emergency, emergency callback and priority IMS sessions, and on authentication of a Resource-Priority header field and a header field value "psap-callback" of a Priority header field, Calling number verification using signature verification and attestation information and Priority verification using assertion of priority information features described in subclause 3.1 shall be supported.

\*\*\* Next Change \*\*\*

#### 5.2.10.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method after emergency registration

If the P-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user over the security association, TLS session, or IP association that was created during the emergency registration, as identified by the presence of the "sos" SIP URI parameter in the Contact header field of the 200 (OK) response, the P-CSCF shall inspect the Request-URI independent of values of possible entries in the received Route header fields for emergency service identifiers. The P-CSCF shall consider the Request URI of the initial request as an emergency service identifier, if it is an emergency number or an emergency service URN from the configurable lists that are associated with:

- the country of the operator to which the P-CSCF belongs to; and

- for inbound roamers, the country from which the UE is roaming from. The P-CSCF determines the country to which the UE is belonging to based on the content of the P-Assserted-Identity header field which contains the home network domain name in a SIP URI belonging to the user.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method does not match any one of the emergency service identifiers in the associated lists, the P-CSCF shall either:

- reject the request by returning a 403 (Forbidden) response to the UE; or

- if the Request-URI is a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]:

1) the P-CSCF sets the Request-URI to an operator defined emergency service URN that matches one of the emergency service identifiers; or

2) remove the right most service identifier and re-inspect the Request-URI for emergency service identifiers.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method matches one of the emergency service identifiers in the associated lists, the P-CSCF shall:

1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]:

a) if the received Request-URI matches an emergency service URN, as received from the UE in the Request-URI; and

b) if the received Request-URI does not match an emergency service URN, as deduced from the Request-URI received from the UE.

NOTE 1: Bullet b) can happen if a request is received from a UE not following the procedures in the present document.

1A) if the operator policy requires that emergency service requests are forwarded to the S-CSCF and the P-CSCF determines that the network to which the originating user is attached (see the IP-CAN specific annexes for the detailed procedure) is the network the P-CSCF is in and if the user is not roaming, then:

NOTE 2: The P-CSCF can know if the user is roaming by comparing the home network domain name of the user received in the Request-URI in the REGISTER request with its own domain name. If they are different the user is a roaming user.

a) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for routing to IBCF;

b) before the request is forwarded in the referenced procedures, include a bottom most Route header field set to the URI associated with an E-CSCF;

NOTE 3: It is implementation dependent as to how the P-CSCF obtains the list of E-CSCFs.

c) afterwards upon receipt of a target refresh request or a subsequent request other than a target refresh request (including requests relating to an existing dialog where the method is unknown) for a dialog from the UE, execute the procedure described in subclause 5.2.6.3.5 and subclause 5.2.6.3.9; and

d) afterwards upon receipt of any response from the UE to a target refresh request or a subsequent request other than a target refresh request (including requests relating to an existing dialog where the method is unknown) for a dialog, execute the procedure described in subclause 5.2.6.4.6 and subclause 5.2.6.4.10;

1B) if the condition for 1A) is not fulfilled then:

a) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for:

- verifying the preloaded route against the received Service-Route header field;

- routing to IBCF; and

- inserting a type 1 "orig-ioi" header field parameter in the P-Charging-Vector header field;

b) before the request is forwarded in the referenced procedures, remove all Route header fields and include a Route header field set to the URI associated with an E-CSCF;

NOTE 4: It is implementation dependent as to how the P-CSCF obtains the list of E-CSCFs.

c) afterwards upon receipt of a target refresh request or a subsequent request other than a target refresh request (including requests relating to an existing dialog where the method is unknown) for a dialog from the UE, execute the procedure described in subclause 5.2.6.3.5 and subclause 5.2.6.3.9, except for inserting a type 1 "orig-ioi" header field parameter in the P-Charging-Vector header field; and

d) afterwards upon receipt of any response from the UE to a target refresh request or a subsequent request other than a target refresh request (including requests relating to an existing dialog where the method is unknown) for a dialog, execute the procedure described in subclause 5.2.6.4.6 and subclause 5.2.6.4.10, except for inserting type 1 "orig-ioi" and "term-ioi" header field parameters in the P-Charging-Vector header field;

1C) if the request is from a UE that is not considered as privileged sender and if the alternative identity of the originator of the request was not identified (see subclause 5.2.6.3.1):

i) if the P-Asserted-Identity header field in the request to be sent contains a SIP URI and if a tel URI belongs to the set of implicitly registered public user identities that contains the SIP URI, add a second P-Asserted-Identity header field that contains the first tel URI of the implicitly registered public user identities; and

ii) if the P-Asserted-Identity header field in the request to be sent contains a tel URI, add a second P-Asserted-Identity header field that contains the first SIP URI of the implicitly registered public user identities that contains the tel URI;

2) if the request contains a Contact header field containing a GRUU the P-CSCF shall save the GRUU received in the Contact header field of the request and associate it with the UE IP address and UE port such that the P-CSCF is able to route target refresh request containing that GRUU in the Request-URI. The UE port used for the association is determined as follows:

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the UE unprotected port on which the request was received;

3) where the network uses the Resource-Priority header field to control the priority of emergency calls, add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197]; and

4) if the P-CSCF supports calling number verification using signature verification and attestation information as specified in subclause 3.1 and if required by operator policy, the P-CSCF shall perform attestation of the user identity by inserting:

- a "verstat" tel URI parameter, specified in subclause 7.2A.20, to the tel URI or SIP URI with a user=phone parameter in the From header field or the P-Asserted-Identity header field;

- an Attestation-Info header field specified in subclause 7.2.18; and

- an Origination-Id header field, specified in subclause 7.2.19, set to a UUID identifying the P-CSCF which is configured based on local policy;

If the P-CSCF does not receive any response to an initial request for a dialog or standalone transaction or an unknown method sent to an E-CSCF (including its retransmissions); or receives a 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method sent to an E-CSCF, the P-CSCF shall include a URI, associated with a different E-CSCF, in the topmost Route header field and forward the request.

If the P-CSCF does not receive any response to an initial request for a dialog or standalone transaction or an unknown method sent to a S-CSCF (including its retransmissions); or receives a 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method sent to a S-CSCF, the P-CSCF shall include a URI, associated with a different E-CSCF, in the topmost Route header field of the initial request for a dialog or standalone transaction or an unknown method, and forward the request.

When the P-CSCF received a subsequent request in the dialog from the UE, and the network uses the Resource-Priority header field to control the priority of emergency calls, the P-CSCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

When the P-CSCF receives a target refresh request for a dialog with the Request-URI containing a GRUU the P-CSCF shall:

- obtain the UE IP address and UE port associated to the GRUU contained in the Request-URI and rewrite the Request-URI with that UE IP address and UE port; and

- perform the steps in subclause 5.2.6.4.5 for when the P-CSCF receives, destined for the UE, a target refresh request for a dialog.

\*\*\* Next Change \*\*\*

#### 5.7.1.14 Emergency transactions

Identification of emergency transactions for termination in the public network by an AS are outside the scope of this document, and are dependent on many application specific considerations.

Where an AS decides to generate an emergency request on behalf of its served user, the AS shall meet the following conditions:

1) the UE is in the same network as the S-CSCF (i.e. that the UE is not roaming).

NOTE 1: How the above is determined is outside the scope of this document and will depend on the application supported. Possible mechanisms could be: 1) that the AS only receives requests that are from non-roaming UEs; 2) analysis of the P-Access-Network-Info header field in a received request from the UE.

The AS generate the request with the following contents:

1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

2) a Route header field with the topmost Route header field set to the URI associated with an E-CSCF;

3) if the AS is part of the trust domain of the network, a P-Asserted-Identity header field containing the identity of the UE served by the AS;

4) if the AS is not part of the trust domain of the network, a P-Preferred-Identity header field containing the identity of the UE served by the AS;

5) if a GRUU is available for the UE served by the AS, provide the GRUU as part of a Contact header field;

NOTE 2: If the AS is not already aware of the GRUU of the UE due to previously receiving it in a Contact header, and the UE is registered, the GRUU can be obtained using either the subscription to the reg events package or using the third-party registration procedure with the REGISTER request including a "message/sip" MIME body of the 200 (OK) response for the REGISTER request as described in subclause 5.7.1.1.

6) if a location is available at the AS in any form, include a Geolocation header field with that location;

7) a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];

8) if the AS supports calling number verification using signature verification and attestation information as specified in subclause 3.1 and if required by operator policy, the AS shall perform attestation of the user identity by inserting:

- a "verstat" tel URI parameter, specified in subclause 7.2A.20, to the tel URI or SIP URI with a user=phone parameter in the From header field or the P-Asserted-Identity header field;

- an Attestation-Info header field, specified in subclause 7.2.18; and

 an Origination-Id header field, specified in subclause 7.2.19, set to a UUID identifying the AS which is configured based on local policy and requirements from national regulation; and

9) if the AS supports priority verification using assertion of priority information as specified in subclause 3.1 and if required by operator policy, the AS shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

If the AS does not receive any response to the INVITE request (including its retransmissions); or receives a 3xx response or 480 (Temporarily Unavailable) response to an INVITE request, the AS shall select a new E-CSCF and forward the INVITE request.

\*\*\* Next Change \*\*\*

#### 5.7.1.25 Assertion verification using the Identity header field

##### 5.7.1.25.1 General

RFC 8224 [252] describes a mechanism where an authentication service after verifying the calling number identity inserts a signature over selected header fields. A verification service can then use this signature to trust the correctness of the identity.

RFC 8946 [265] describes a mechanism where an authentication service after verifying the diverting number identity inserts a signature over selected header fields. A verification service can then use this signature to trust the correctness of the diverting identity.

RFC 8443 [nn1] describes a mechanism where an authentication service after verifying the Resource-Priority header field inserts a signature over the Resource-Priority header field. A verification service can then use this signature to trust the correctness of the Resource-Priority header field.

draft-ietf-stir-rph-emergency-services [nn2] extends a mechanism defined in RFC 8443 [nn1] to enable authentication of the header field value "psap-callback" of the Priority header field and inserts a signature over the Resource-Priority header field and the header field value "psap-callback" provided in the Priority header field. A verification service can then use this signature to trust the correctness of the Resource-Priority header field and header field value "psap-callback" of the Priority header field.

\*\*\* Next Change \*\*\*

### 5.10.1 General

As specified in 3GPP TS 23.228 [7] border control functions may be applied between two IM CN subsystems or between an IM CN subsystem and other SIP-based multimedia networks based on operator preference. The IBCF may act both as an entry point and as an exit point for a network. If it processes a SIP request received from other network it functions as an entry point (see subclause 5.10.3) and it acts as an exit point whenever it processes a SIP request sent to other network (see subclause 5.10.2).

The functionalities of the IBCF are entry and exit point procedures as defined in subclause 5.10.2 and subclause 5.10.3 and additionally can include:

- network configuration hiding (as defined in subclause 5.10.4);

- application level gateway (as defined in subclause 5.10.5);

- transport plane control, i.e. QoS control (as defined in subclause 5.10.5);

- screening of SIP signalling (as defined in subclause 5.10.6);

- inclusion of an IWF if appropriate;

- media transcoding control (as defined in suclause 5.10.7);

- privacy protection (as defined in subclause 5.10.8);

- additional routeing functionality (as defined in Annex I); and

- invocation of an AS over the Ms reference point (as defined in subclause 5.10.10).

NOTE 1: The functionalities performed by the IBCF are configured by the operator, and it is network specific.

The IBCF shall log all SIP requests and responses that contain a "logme" header field parameter in the SIP Session-ID header field if required by local policy.

When an IBCF acting as an exit or an entry point receives a SIP request, the IBCF may reject the SIP request based on local policy by sending an appropriate SIP 4xx response.

NOTE 2: The local policy can take bilateral agreements between operators into consideration.

NOTE 3: Some SIP requests can be rejected by an AS instead of the IBCF according to local policy.

The IBCF, acting as B2BUA, which is located between visited network and home network shall preserve the dialog identifier, i.e. shall not change the Call-Id header field value, the "tag" header field parameter value of the From header field in any SIP INVITE request and any SIP response to the SIP INVITE request, and shall preserve the "tag" header field parameter value of the To header field, in any SIP response to the SIP INVITE request.

NOTE 4: The IBCF can identify whether it is located between visited network and home network based on local configuration or, if IBCF supports indicating traffic leg associated with a URI as specified in RFC 7549 [225], based on the value of the "iotl" SIP URI parameter.

If the IBCF has verified that an initial INVITE request is for a PSAP callback, then depending on local policy it may include a Priority header field with a "psap-callback" header field value in the INVITE request. If the IBCF included the Priority header field with a "psap-callback" header field value, if the IBCF supports priority verification using assertion of priority information as specified in subclause 3.1 and if required by operator policy, the IBCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197] if not already present.

NOTE 5: The means for the IBCF to verify that a request is for a PSAP callback is outside the scope of this specification.

When receiving a dialog creating SIP request or a SIP stand-alone request and if an IBCF acting as an entry or exit point supports indicating the traffic leg as specified in RFC 7549 [225], the IBCF can identify the II-NNI traversal scenario as described in subclause 4.13 and make policy decisions based on the II-NNI traversal scenario type. If a received request contains more than one "iotl" SIP URI parameter the IBCF shall select one of the "iotl" SIP parameters in the received request in accordance with the RFC 7549 [225].

When sending a failure response to any received request, depending on operator policy, the IBCF may insert a Response-Source header field with an "fe" header field parameter constructed with the URN namespace "urn:3gpp:fe", the fe-id part of the URN set to "ibcf" and optionally an appropriate fe-param part of the URN set in accordance with subclause 7.2.17.

\*\*\* Next Change \*\*\*

#### 5.10.10.2 Procedures for an IBCF acting as an entry point

When receiving an initial INVITE or MESSAGE request containing one or more SIP Identity header fields, the IBCF shall determine the information (originating identity, diverting identities, contents of the Resource-Priority and Priority header fields) to be verified by decoding the Identity header fields containing a PASSporT SHAKEN JSON Web Token. The IBCF uses the Identity header fields to:

1) build and send a verificationRequest, specified in annex V, to an AS for verification over the Ms reference point; and

2) shall upon receiving an HTTP 200 (OK) response to the above request, use:

- the verstat claim from this response to populate the "verstat" tel URI parameter for the Identity header field associated with the originating identity and add this parameter to the verified identity in the SIP From header field or the SIP P-Asserted-Identity header field in the forwarded SIP request. Additionally, if the HTTP 200 (OK) response included verification results for the diverting identities, the IBCF shall based on local policy add the "verstat" tel URI parameter to the verified diverting identities in the History-Info header field if this field is available; and

- the verstatPriority claim from this response to populate the Priority-Verstat header field for the Identity header field associated with the Resource-Priority header field and with the header field value "psap-callback" of the Priority header field (if present) and include the Priority-Verstat header field in the forwarded SIP request.

\*\*\* Next Change \*\*\*

#### 5.10.10.3 Procedures for an IBCF acting as an exit point

When receiving an initial INVITE or MESSAGE request containing:

NOTE 1: As part of the border control procedures the IBCF can apply privacy procedures and in these cases this procedure is not needed.

1) a "verstat" tel URI parameter in at least one of the SIP From header field or the SIP P-Asserted-Identity header field;

2) a SIP Attestation-Info header field as defined in subclause 7.2.18; and

3) a SIP Origination-Id header field as defined in subclause 7.2.19;

and if no Identity header field exists, the IBCF sends a signingRequest, specified in annex V, over the Ms reference point. When the HTTP 200 (OK) response to this request is received, the IBCF shall include value of the "identity" claim in an Identity header field in the forwarded SIP request.

When receiving an initial INVITE or MESSAGE request containing at least one Identity header field and a "verstat" tel URI parameter in a tel URI or a SIP URI with a user=phone parameter in one or more History-Info header field(s) or using other not specified means to determine that a diversion has occurred, then the IBCF sends a signingRequest, specified in annex V, over the Ms reference point for each of the identities to be signed. When the HTTP 200 (OK) response for any of these requests is received, the IBCF shall include the value of the "identity" claim in an Identity header field in the forwarded SIP request.

NOTE 2: As part of the border control procedures the IBCF can apply privacy procedures and in these cases this procedure is not needed.

When receiving an initial INVITE request containing the Resource-Priority header field and optionally the Priority header field with a "psap-callback" header field value or if the IBCF included the Priority header field with a "psap-callback" header field value and the Resource-Priority header field (as specified in subclause 5.10.1), the IBCF sends for the Resource-Priority and Priority header fields a signingRequest, specified in annex V, over the Ms reference point. When the HTTP 200 (OK) response to this request is received, the IBCF shall include the value of the "identity" claim in an Identity header field in the forwarded initial INVITE request.

\*\*\* Next Change \*\*\*

### 7.2.x Definition of Priority-Verstat header field

Editor's note: [WI: TEI17\_SAPES, CR #6518] as per RFC 5727 an IETF expert review is needed in order to obtain the IANA registration of this header field.

#### 7.2.x.1 Introduction

IANA registry: Header Fields registry for the Session Initiation Protocol (SIP)

Header field name: Priority-Verstat

Usage: The Priority-Verstat header field is used only for informative purposes.

Header field specification reference: 3GPP TS 24.229, http://www.3gpp.org/ftp/Specs/archive/24\_series/24.229/

When a node has performed authentication of a Resource-Priority header field and a header field value "psap-callback" of a Priority header field in an incoming request, the node can inform a downstream node whether the Resource-Priority header field and the header field value "psap-callback" of the Priority header field was populated by an authorized entity and can be trusted. A downstream node can use use this information to determine whether the call should be treated according to the priority level indicated in the Resource-Priority header field and whether the call should be treated as emergency call back.

#### 7.2.x.2 Applicability statement for the Priority-Verstat header field

The Priority-Verstat header field is applicable within a single private administrative domain or between different administrative domains.

The Priority-Verstat header field is applicable when a node has performed authentication of a Resource-Priority header field and a header field value "psap-callback" of a Priority header field in an incoming request.

#### 7.2.x.3 Usage of the Priority-Verstat header field

The Priority-Verstat header field is used to indicate the verification status of the Resource-Priority header field and optionally the header field value "psap-callback" of the Priority header field.

#### 7.2.x.4 Procedures at the UA

There are no specific procedures specified for a UA.

#### 7.2.x.5 Procedures at the proxy

A SIP proxy that supports this extension and receives a request may as part of its procedures insert a Priority-Verstat header field prior to forwarding the request. The header field is populated as specified in table 7.2.x-1.

#### 7.2.x.6 Security considerations

A UE is not expected to receive this information.

#### 7.2.x.7 Syntax

The syntax for Priority-Verstat header field is specified in table 7.2.x-1.

Table 7.2.x-1: Syntax of Priority-Verstat

Priority-Verstat = "Priority-Verstat" HCOLON verstat-value / token

verstat-value = "RPH-Validation-Passed" / "RPH-Validation-Failed" / "No-RPH-Validation" /
 "ECB-RPH-Validation-Passed" / "ECB-RPH-Validation-Failed" / "No-ECB-RPH-Validation" /
 other-value

other-value = token

#### 7.2.x.8 Examples of usage

The Priority-Verstat header field is used in networks which have requirements on authentication of a Resource-Priority header field and a header field value "psap-callback" of a Priority header field to authenticate content of the Resource-Priority header field and the header field value "psap-callback" of the Priority header field.

\*\*\* Next Change \*\*\*

### 7.13.x verstatPriority

The verstatPriority claim is used to transport the verification value of the Resource-Priority header field and optionally the header field value "psap-callback" of the Priority header field.

Claim name: verstatPriority

Claim value: String

Claim description: Indicates the result of the verification of the Resource-Priority header field and optionally the header field value "psap-callback" of the Priority header field.

\*\*\* Next Change \*\*\*

## V.2.1 General

For the Ms reference point HTTP 1.1 as specified in RFC 2616 [196] shall be used.

The Ms reference point is used to request signing of an Identity header field or request verification of a signed assertion in an Identity header field.

HTTP POST method is used for the verification request.

HTTP 200 (OK) is used when the AS for verification has successfully processed the verification request.

HTTP POST method is used for the signing request.

HTTP 200 (OK) is used when the AS for signing has successfully processed the signing request.

HTTP POST method is used for the diversion signing request.

HTTP 200 (OK) is used when the AS for signing has successfully processed the diversion signing request.

HTTP POST method is used for the Resource-Priority header field signing request.

HTTP 200 (OK) is used when the AS for signing has successfully processed the Resource-Priority header field signing request.

HTTP POST method is used for the Resource-Priority and Priority header fields signing request.

HTTP 200 (OK) is used when the AS for signing has successfully processed the Resource-Priority and Priority header field signing request.



Figure V.2.1-1: Usage of the Ms reference point

\*\*\* Next Change \*\*\*

## V.2.2 Resource structure

API resources are defined with respect to a "server root". The server root is a URI:

- {hostname}:{port}/{RoutingPath},

The resource URI structure is:



Figure V.2.2-1: Resource structure for the resource exposed over the Ms reference point

NOTE: v1 is the version number of the API.

Table V.2.2-1: Variables for the server root

|  |  |  |
| --- | --- | --- |
| Variable | Description | Presence |
| hostname | Host name used to reach the resource. | M |
| port | Port where the resource is reached | M |
| RoutingPath | Path identifying the resource | M |

\*\*\* Next Change \*\*\*

### V.2.5.2 Data types

Table V.2.5.2-1 specifies the data types included in the signing request. The signing request contains the claims included in:

- a PASSporT SHAKEN JSON Web Token, specified in RFC 8588 [261];

- a PASSporT div JSON Web Token specified in RFC 8946 [265]; or

- a PASSporT rph JSON Web Token specified in RFC 8443 [nn1] and optionally a PASSporT sph JSON Web Token specified in draft-ietf-stir-rph-emergency-services [nn2].

Table V.2.5.2-1: Data types for the signingRequest

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| attest | string; "A", "B" or "C" | O | Identifying the relation between the service provider attesting the identity and the subscriber. Specified in RFC 8588 [261]. |
| dest | array of identity claim JSON objects representing destination identities; tn or uri | M | Identifying the called user taken from the To header field for a PASSporT SHAKEN Token, and from the Request-URI for a PASSporT div Token. Specified in RFC 8225 [262]. |
| div | identity claim JSON object, tn or uri. A hi element should be included. | O | Identifying the diverting user, taken from the corresponding Identity header field as pecified in RFC 8946 [265]. |
| iat | integer; time and date of issuance of the PASSporT token | M | Time since 1 January 1970 in Numeric Date format as specified in RFC 7519 [235]. |
| orig | identity claim JSON object; tn or uri | M | Identifying the calling user. Specified in RFC 8225 [262]. |
| origid | String; UUID | O | Specified in RFC 8588 [261] |
| rph | array of strings that correspond to the r-values indicated in the SIP Resource-Priority header field | O | Contains assertion of the priority level of the user to be used for a given communication session as specified in RFC 8443 [nn1]. |
| sph | string "psap-callback" | O | Contains header field value "psap-callback" of the SIP Priority header field as specified in draft-ietf-stir-rph-emergency-services [nn2] |

Table V.2.5.2-2 further specifies the data types contained in the signing request parameters.

Table V.2.5.2-2: Data types for the signingRequest parameters

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| hi | string. An "index" header field parameter as specified in RFC 7044 [66] | O | The "index" header field parameter is included in the entry identifying the diverting user in the History-Info header field. |
| tn | string; allowed characters as for local-number-digits and global-number-digits defined in RFC 3966 [22] | M | The number needs to be canonicalized by the server following the procedure in RFC 8224 section 8.3. |
| uri | string; A SIP URI as specified in RFC 3261 [26] following the generic guidelines in RFC [3986]. | O | Used if the "orig" or "dest" is given in a SIP URI. |

Table V.2.5.2-3 specifies the data types included in the signing response.

Table V.2.5.2-3: Data types for the signingResponse

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| identityHeader | string; Identity header field value as specified in RFC 8224 [252] | M | This string cannot be NULL |

\*\*\* Next Change \*\*\*

### V.2.6.1 General

To get a received identity claim verified the client sends an HTTP POST request towards the verification server containing a PASSporT object, including an identity claim with the contents of the received Identity header field(s) signing:

- the originating identity and optionally all the Identity header fields signing diverting identities; and/or

- the Resource-Priority header field and optionally the header field value "psap-callback" of the Priority header field.

The received verificationResponse contains the outcome of the verification in a verstat claim with values as specified for the verstat tel URI parameter in subclause 7.2A.20 and in a verstatPriority claim with values as specified for the Priority-Verstat header field in subclause 7.2.x. Unsuccesful requests are responded with an HTTP 4xx or 5xx response.

\*\*\* Next Change \*\*\*

### V.2.6.2 Data types

Table V.2.6.2-1 specifies the data types included in the verification request.

Table V.2.6.2-1: Data types for the verificationRequest

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| identityHeader | string; Identity header field value for the originating identity as specified in RFC 8224 [252]. | M | This string cannot be NULL |
| IdentityHeaders | array of string; Identity header field values as specified in RFC 8224 [252]. One identityHeader claim per received Identity header field is sent. | O | Identity headers containing the div, rph or sph claims to be verified. |
| to | String; identity claim JSON object; tn or uri | M | The destination identity taken from the To header field. Used when no div claim is included. |
| dest | string; identity claim JSON object; tn or uri | O | The destination identity taken from the R-URI in the incoming request. Used when div claim is included. |
| time | integer; Numeric date format defined in RFC 7519 [235] | M | Time based on the Date header field in the incoming request. |
| from | string; identity claim JSON object; tn or uri | M | The asserted identity, taken from the P-Asserted-Identity or the From header field of the incoming request |

Table V.2.6.2-2 specifies the data types included in the verification response.

Table V.2.6.2-2: Data types for the verificationResponse

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| divResult | array of one or more [div, verstatValue] tuples | O | Parameter informing of the result of the verification of diverting identities. For each verified identity the verstat parameter is added to the verified identity. |
| verstatValue | string; set to a value defined in table 7.2A.20.3-1 | M | Parameter informing of the result of the verification of originating identity. To be used in the verstat parameter added to the verified identity. |
| verstatPriority | string; set to a value defined in table 7.2.x-1 | O | Parameter informing of the result of the verification of the Resource-Priority header field and optionally the header field value "psap-callback" of the Priority header field. |

\*\*\* End of Changes \*\*\*