**3GPP TSG-CT WG1 Meeting #131-eC1-214060**

**E-meeting, 19-27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.229** | **CR** | **6528** | **rev** | **1** | **Current version:** | **17.3.1** |  |
|  | | | | | | | | |
| *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:*** | 24.229 RPH signing for MPS | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Peraton Labs, CISA ECD, AT&T, T-Mobile USA, Verizon | | | | | | | | | |
| ***Source to TSG:*** | CT1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17\_SAPES | | | | |  | ***Date:*** | | | 2021-08-06 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **C** |  | | | | | ***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 can be 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:*** | | |  | | --- | | Changes to TS 24.229 are needed to support the following SA2 requirements:  In TS 23.228 clause 4.14:  - For an originating session leaving an IBCF, the IBCF of the originating network, if configured through operator policies, invokes an AS for the signing of Resource-Priority header field related information, if available in the incoming request. The IBCF includes the signed Resource-Priority header field related information in the outgoing request.  - For a terminating session entering the IBCF with signed Resource-Priority header field information, the IBCF, if configured through policies, invokes an AS for signature verification.  In TS 23.228 clause 4.16.3:  If configured through policies, the telephony AS, or any other AS, may perform for originating IMS priority sessions, assertion of authorization for the Resource-Priority header field information.  In addition, and if configured through policies, the telephony AS, or any other AS, may perform for terminating requests signature verifications, if one or more signatures is included.  Additionally, RPH signing does not require caller ID signing, the two types of signing should be de-coupled in the TS. | | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | First change:  Changes the header field value "psap-callback" to "optionally" in the definition of "Priority verification using assertion of priority information" so that "Priority verification using assertion of priority information" can be used for cases where only RPH signing is required and header field value "psap-callback" signing is not required.  Second change:  RPH signing does not also require caller id signing, make it optional in clause 4.11.    Third change:  Adds RPH signing specific procedures to the originating AS procedures  Fourth change:  Adds RPH verifying specific procedures to the terminating AS procedures  Fifth change:  Adds RPH signing to general list of actions by the IBCF. Deletes duplicate sentence.  Sixth change:  Editorial change "is" to "are".  Seventh change:  Added a note to explain that either the AS or the IBCF can invoke AS for signing.    Eighth change:  The Priority header is made optional, it's not needed for non-emergency sessions. Added a note to explain that either the AS or the IBCF can invoke AS for signing. Added a note that how the authenticity is asserted is out of scope.  Ninth change:  The description of Priority-Verstat is modified to make "psap-callback" optional so that Priority-Verstat can be used for standalone RPH signing.  Tenth change:  Align name of AS for signing with rest of clause.  Eleventh change:  Align name of AS for signing with rest of clause.  Twelfth change:  There can be more than one claim per Ms interface invocation, the verbiage is fixed to allow more than one in clause V.2.6.1, to agree with other clauses.  Thirteenth change:  Changes the mandatory identityHeader to be either the identity header of the originating identity or the identity header for the RPH because for standalone RPH, there won't be an identity header for the originating identity. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Implementations will be forced to implement caller id signing in order to do RPH signing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 3.1, 4.4.6, 4.11, 5.7.1.25.2, 5.7.1.25.3, 5.10.1, 5.10.10.1, 5.10.10.2, 5.10.10.3, 7.2.21.1, V.2.5.1, 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 \*\*\*\*\*

## 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 [279] and, by extension for emergency sessions, the header field value "psap-callback" provided in the Priority header field as specified in draft-ietf-stir-rph-emergency-services [278]. As specified in RFC 8443 [279] the Identity header field is used for the purpose of authentication of the Resource-Priority header field and, by extension for emergency sessions, 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**

\*\*\*\*\* Second 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 a network has requirements on attestation and signing of priority IMS sessions (e.g., MPS sessions) the Priority verification using assertion of priority information feature described in subclause 3.1 shall be supported and the Calling number verification using signature verification and attestation information feature described in subclause 3.1 may be supported.

Where the network has requirements on attestation and signing of originating calling identification information for emergency and emergency callback 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.

\*\*\*\*\* Third change \*\*\*\*\*

##### 5.7.1.25.2 Originating procedures

An originating AS supporting the calling number verification using signature verification and attestation information, as defined in subclause 3.1:

1) may based on local policy insert an Identity header field as specified in RFC 8224 [252] for all initial INVITE requests and MESSAGE requests and shall for this purpose use the identity in the P-Asserted-Identity header field or the From header field; or

NOTE 1: This option is kept from the original release-14 functionality. If the AS knows the IBCF supports invoking an AS for providing an Identity header field the below actions are more efficient.

2) may based on local policy perform attestation of the identity of the served user by:

a) inserting a "verstat" tel URI parameter, specified in subclause 7.2A.20; in the From header field or the P-Asserted-Identity header field if not already present; and

b) insert an Origination-Id header field as specified in subclause 7.2.19 and an Attestation-Info header field specified in subclause 7.2.18, if not alredy present.

If the AS performs originating services on behalf of a diverting user, the AS may assert the identity of the diverting user by inserting a "verstat" tel URI parameter, specified in subclause 7.2A.20, in the History-Info hi-entry representing the diverting user.

If the AS supports priority verification using assertion of priority information as specified in subclause 3.1 and if allowed by local operator policy, the AS may insert an Identity header field as described in RFC 8443 [279] and RFC 9027 [278], and shall for this purpose use the resource priority of the Resource-Priority header field in the received initial INVITE or re-INVITE request.

NOTE 2: For sessions terminating in another domain, only one of the following entities needs to be configured to provide an Identity header field for the resource priority: the IBCF or the AS. Which functional entity provides the Identity header field is subject to network configuration and local policy.

NOTE 3: How the AS asserts the authenticity of the Resource-Priority header field value is out of scope of the present document.

\*\*\*\*\* Fourth change \*\*\*\*\*

##### 5.7.1.25.3 Terminating procedures

Upon receiving an initial INVITE request or a MESSAGE request containing one or more Identity header fields, an AS supporting the calling number verification using signature verification and attestation information, as defined in subclause 3.1, shall if the network indicated support for the calling number verification during registration:

- if no "verstat" tel URI parameter is present for the identity to be verified in the From or P-Asserted-Identity header field, perform user identity verification of the originating user identity using the Identity header field containing a PASSporT SHAKEN JSON Web Token, specified in RFC 8588 [261] and based on local policy all Identity header fields containing a PASSporT div JSON Web Token, specified in RFC 8946 [265], in the received request.Based on the outcome of the verification insert a "verstat" tel URI parameter, specified in subclause 7.2A.20, with a value representing the outcome of the verification in the tel URI or SIP URI with the user=phone parameter of each P-Asserted-Identity header field or From header field where the URI contains the calling number that was tested for verification and based on local policy in all verified identities in the History-Info header field.

If no Identity header field is present in the received INVITE or MESSAGE request, but an Origination-Id header field along with an Attestation-Info header field set either to "B" or "C" is present, the AS shall set the verstat tel URI parameter to the value "No-TN-Validation".

If the AS supports priority verification using assertion of priority information as specified in subclause 3.1 and if allowed by local operator policy, the AS may verify the Resource-Priority header field. To do so, the AS decodes the Identity header fields containing a PASSporT rph JSON Web Token as specified in RFC 8443 [279], if included in the initial INVITE or re-INVITE request.

NOTE: For sessions originating in another domain, only one of the following entities needs to be configured to verify the Identity header field for the resource priority: the IBCF or the AS. Which functional entity provides the Identity header field verification is subject to network configuration and local policy.

\*\*\*\*\* Fifth 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.

\*\*\*\*\* Sixth change \*\*\*\*\*

#### 5.10.10.1 General

General procedures over the Ms reference point are specified in clause V.2.

\*\*\*\*\* Seventh change \*\*\*\*\*

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

When receiving an initial INVITE, re-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 and/or a PASSporT rph JSON Web Token with an optional PASSporT sph 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.

NOTE: For sessions originating in another domain, only one of the following entities needs to be configured to verify the Identity header field for the resource priority: the IBCF or the AS. Which functional entity provides the Identity header field verification is subject to network configuration and local policy.

\*\*\*\*\* Eighth 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 a signingRequest, over the Ms reference point, as specified in annex V, for the resource priority and optionally, the Priority header fields. 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.

When receiving a re-INVITE request containing the Resource-Priority header field, the IBCF sends a signingRequest, over the Ms reference point, as specified in annex V, for the resource priority. 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 re-INVITE request.

NOTE 3: For sessions terminating in another domain, only one of the following entities needs to be configured to provide an Identity header field for the resource priority: the IBCF or the AS. Which functional entity provides the Identity header field is subject to network configuration and local policy.

NOTE 4: How the IBCF asserts the authenticity of the Resource-Priority header field value is out of scope of the present document.

\*\*\*\*\* Ninth change \*\*\*\*\*

#### 7.2.21.1 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 verification of a Resource-Priority header field and of a header field value "psap-callback" of a Priority header field (if present) 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 (if present) 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 (if the Priority header field was present) whether the call should be treated as emergency call back.

\*\*\*\*\* Tenth change \*\*\*\*\*

### V.2.5.1 General

To get an asserted identity signed the client sends an HTTP POST request towards the AS for signing containing a PASSporT SHAKEN object, specified in RFC 8588 [261]; a PASSporT rph object, specified in RFC 8443 [279]; a PASSporT sph object, RFC 9027 [278]; or a PASSporT div object, specified in RFC 8946 [265]. The received signingResponse contains for successful requests the signed Identity header field value in a JSON object. Unsuccessful requests are responded with an HTTP 4xx or 5xx response.

\*\*\*\*\* Eleventh 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 [279] and optionally a PASSporT sph JSON Web Token specified in RFC 9027 [278].

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 [279]. |
| sph | string "psap-callback" | O | Contains header field value "psap-callback" of the SIP Priority header field as specified in RFC 9027 [278]. |

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 AS for signing 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 |

\*\*\*\*\* Twelfth change \*\*\*\*\*

### V.2.6.1 General

To get a received identity claim verified, the client sends an HTTP POST request towards the AS for verification containing a PASSporT object, including one or more claims 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 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 7.2.21. Unsuccessful requests are responded with an HTTP 4xx or 5xx response.

\*\*\*\*\* Thirteenth 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 | O | Parameter informing of the result of the verification of originating identity. To be used in the verstat parameter added to the verified identity. The parameter is mandatory if the request contained a PASSporT SHAKEN JSON Web Token. |
| verstatPriority | string; set to a value defined in table 7.2.21-1 | 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 \*\*\*\*\*