**3GPP TSG-CT WG1 Meeting #135-eC1-223513**

**E-Meeting, 6th – 12th April 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.229** | **CR** |  | **rev** | **4** | **Current version:** | **17.6.1** |  |
|  | | | | | | | | |
| *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:*** | Annex-V – Verify integrity of SIP header fields based on validated PASSporT claims | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Neustar, Comcast, Oracle, Genband Ireland | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17\_SAPES | | | | |  | ***Date:*** | | | 2022-03-23 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Add functionality described in RFC 8443 and RFC 8224 to improve the capabilities of the verification service.  RFC 8443 describes the following security vulnerabilities associated with the Resource-Priority header field:  "However, the SIP 'Resource-Priority' header field could be spoofed and abused by unauthorized entities, the threat models and use cases of which are described in [RFC7375] and [RFC7340], respectively. Compromise of the SIP 'Resource-Priority' header field [RFC4412] could lead to misuse of network resources (i.e., during congestion scenarios), impacting the application services supported using the SIP 'Resource-Priority' header field."  The "rph" PASSporT protects against this security concern by integrity protecting the Resource-Priority header field with the "rph" claim of the "rph" PASSporT. For example, RFC 8443 contains the following text (*underline/italics* added for emphasis):  “[RFC8225] allows extensions by which an authority on the originating  side verifying the authorization of a particular communication for  the SIP 'Resource-Priority' header field can use a PASSPorT claim to  cryptographically sign the SIP 'Resource-Priority' header field and  convey assertion of the authorization for the SIP 'Resource-Priority'  header field. *A signed SIP 'Resource-Priority' header field will*  *allow a receiving entity (including entities located in different*  *network domains/boundaries) to verify the validity of assertions*  *authorizing the SIP 'Resource-Priority' header field and to act on*  *the information with confidence that the information has not been*  *spoofed or compromised*.”  RFC 8443 describes how the value of the "rph" PASporT "rph" claim is derived as follows (again, *underline/italics* added for emphasis):  “Specifically, the "rph" claim includes an assertion of the priority  level of the user to be used for a given communication session. The  value of the "rph" claim is an object with one or more keys. Each  key is associated with a JSON array. *These arrays contain strings*  *that correspond to the r-values indicated in the SIP 'Resource-*  *Priority' header field*.”  Finally, RFC 8443 describes how the "rph" PASSporT "rph" claim is used to verify that the priority indicated by a Resource-Priority header field is authorized, as follows:  “The verification service MUST extract the value associated with the  "auth" key in a full-form PASSporT with a "ppt" value of "rph". If  the signature validates, then the verification service can use the  value of the "rph" claim as validation that the calling party is  authorized for SIP 'Resource-Priority' header fields as indicated in  the claim. *This value would, in turn, be used for priority treatment*  *in accordance with local policy for the associated communication*  *service.*”  To support the above RFC 8443 requirements, this CR adds the optional capability for the Annex-V verification API to verify the integrity of the contents of the Resource-Priority header field using the value indicated by a validated "rph" claim.  With the currently-defined Annex V verification API, there is no way to compare the validated "rph" claim with the contents of the Resource-Priority header; i.e., there is no single entity that knows both the header field contents and the validated claim contents so that it can perform the integrity check. Specifically, the Resource-Priority header field contents are not passed in the verification request so the AS for verification could perform the integrity check. Likewise, the validated "rph" claim values are not returned in the verification response so the client could perform the integrity check. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The verification request is updated to enable the client to optionally include the Resource-Priority header field contents in the verification request. The verification service can then compare the received header field values with the associated claim values in the "rph" PASSporT, and declare a verification failure if a mismatch is found. Likewise, the verification response is updated to enable the verification service to return the valid claims of a verified "rph" PASSporT to the client. This enables the option where the client performs the integrity check. The API updates are designed to be sufficiently general to support integrity checking of any header field information protected by PASSporT claims. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Malicious entities could modify the Resource-Priority header field, thus preventing an authorized priority user from priority access to network resources. This could negatively impact the ability of the network to support legitimate priority services, or in the worst case, its ability to support normal calls.  For example, RFC 4412 defines the following priority level namespace for WPS calls:  (lowest) wps.4  wps.3  wps.2  wps.1  (highest) wps.0  Say a legitimate WPS user is authorized to obtain priority wps.3. If a malicious entity were to increase the Resource-Priority header field priority level to wps.0, it could potentially block legitimate calls at priority wps.2 or wps.1. Likewise, a malicious entity could lower the priority (or remove the Resource-Priority header field all together) which could potentially block this priority call.  Another example would be the case where a Certification Authority issues a delegate certificate to an untrusted VoIP entity. The delegate certificate contains Claim Constraints that authorize the VoIP entity to sign "rph" PASSporTs only for wps.4 and wps.3. Without the change proposed by this CR, a verification service would be unable to detect when the VoIP entity added a Resource-Priority header field with an unauthorized priority level higher than wps.3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.7.1.25.3, 5.10.10.2, 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:*** | | Notes to 24.229 editor:  Table V.2.6.2-3 is updated by this CR, and by CR 6555. In order to make it clear what the final table should look like, the updates to Table V.2.6.2-3 for both CRs are shown in CR 6555, and not in this CR (specifically, the “validClaims” field of the new verifyResults” parameter is shown in CR 6555).  Also, CR 6559 changes the verification request parameter name "IntegrityHeaders" to "integrityHeaders". The text in this CR following Table V.2.6.2-1 uses the new "integrityHeaders" name. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Revision 1 (from C1-222706):   1. Corrected “TEI17-SAPES” work item code typo 2. In response to comments, added Table V.2.6.2-3 to CR 6555 which includes updates in both CR 6555 and CR 6556 3. In response to comments, re-worded text describing new, optional parameters to avoid describing specific AS behavior 4. Correct reference to SIP Priority header IETF RFC 5. In response to comments, changed “retargets” parameter to “diversions” 6. In response to comments, moved the optional verification response parameters for successes to a separate Table V.2.6.2-5 7. Added reference to SIP Diversion header IETF RFC 8. Corrected several other minor typos on review   Revision 2 (from C1-223009)   1. Moved notes out of tables V.2.6.2-1 and V.2.6.2-5 to normal text following each table 2. Removed all references to the Diversion header field 3. Updated the "reason for change" to clarify why this change is needed. 4. Updated the "Consequences if not approved" to clarify what bad things could happen if this CR is not approved. 5. Updated the text after table V.2.6.2-1 to clarify when integrity protected header information is or is not conveyed in the verification request.   Revision 3 (from C1-223064)   1. Added AS procedures to 5.7.1.25.3, and IBCF procedures to 5.10.10.2 to verify that the SIP request information associated with the verification response validClaims parameter is authorized by the validClaims values. 2. Updated V.2.6.1 to clarify what is passed in the verification request to verify the integrity of message components protected by PASSporT claims.   Revision 3 (from C1-223064)   1. Changed “must” to “shall”.   Revision 4 (from C1-223513)   1. Clarified text in 5.7.1.25.3 (instead of adding a new requirement, integrated changes with existing text). 2. Changed new requirement in 5.10.10.2 from “shall” to “may”. 3. In V.2.6.1, Changed verifyRequest to verification request. Also, clarified that the verification response can return the validated claims. 4. In V.2.6.2, edited the text following Table V.2.6.2-1, eliminating everything but the essentials. | | | | | | | | |

\* \* \* First 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 that the Priority and Resource-Priority header field values are authorized. To do so, the AS

* verifies the Identity header fields containing a PASSporT rph JSON Web Token as specified in RFC 8443 [279], RFC 8443 [279] and RFC 9027 [278] if included in the initial INVITE or re-INVITE request; and
* verifies that the Priority and Resource-Priority header field values are authorized by valid "rph" PASSporT claims.

The AS shall populate the Priority-Verstat header field associated with the Resource-Priority header field 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 inserts the Identity header field verification is subject to network configuration and local policy.

\* \* \* Next 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 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 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.

Based on local policy, the IBCF may verify that the validated claims returned in the validClaims parameter of the verification response authorize the associated SIP header field values.

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 inserts the Identity header field verification is subject to network configuration and local policy.

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

### V.2.6.1 General

To verify one or more received PASSporTs, the client sends a verification request in the form of an HTTP POST request to the AS for verification containing the Identity header field(s) populated with the PASSporT object(s) to be verified. The verification request also contains the following information:

- SIP request information required to detect replayed PASSporT(s) as specified in RFC 8224 [252] and RFC 8946 [265];

- the originating identity and optionally all the diverting identities; and/or

- the Resource-Priority header field value 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. The verificationResponse can optionally contain the claims of PASSporT(s) that passed verification.

Unsuccessful 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 |
| diversions | array of one or more div parameters defined in table V.2.5.2-1 | O | Contains the retargeting identities (TN or URI) in History-Info header fields defined in RFC 7044 [66]. |
| rph | array of strings corresponding to the r-values contained in the SIP Resource-Priority header field | O | Contains the Resource-Priority header field values as specified in RFC 4412 [116] and RFC 7135 [197]. |
| sph | string; corresponding to the value contained in the Priority header field | O | Contains the SIP Priority header field value as specified in RFC 3261 [26] and RFC 7090 [209]. |
| protectedHeaders | array of string; header field(s) | O | Contains the SIP header field(s) protected by claims in the PASSporT(s) of the IdentityHeaders array. |

Invocation of the verification request results in the verification of the Identity header fields in the identityHeader and identityHeaders parameters. In addition, a verification request invocation may verify the integrity of SIP header fields protected by the "div" and "rph" PASSporTs. When verification of SIP header field integrity is required, the integrity protected SIP header field information shall be conveyed in the verification request to the AS for verification using one of the following mechanisms:

- convey the SIP header field value(s) in the appropriate diversions, rph, and sph parameters; or

- convey the SIP header field(s) in the protectedHeaders parameter.

Header field information that is protected by a PASSporT type is conveyed in the verification request only if that PASSporT type is also conveyed in the identityHeaders array.

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. |

Table V.2.6.2-5 specifies the additional data types included in the verification response when the status parameter contains a value of "pass".

Table V.2.6.2-5: Data types of additional verifyResults parameter for status of "pass"

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| validClaims | JSON object | O | The validClaims parameter contains the payload of the verified PASSporT. |

The validClaims parameter may be used in one of two ways:

- to verify the integrity of SIP header field information associated with the validated claims, where a mismatch results in a verification failure; or

- to ensure that SIP header field contents contain the information authorized by the validated claims, where a mismatch is resolved by updating the SIP header field to match the validated claims.

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