**3GPP TSG-CT WG1 Meeting #135-eC1-223063**

**E-Meeting, 6th – 12th April 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.229** | **CR** | **6555** | **rev** | **2** | **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 Signing and Verification Modifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Neustar, Comcast, Oracle, Genband Ireland | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SPECTRE\_Ph3 | | | | |  | ***Date:*** | | | 2022-03-21 |
|  |  | | | |  | |  | | |  |
| ***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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Implementation experience gained from signing and verifying billions of calls per day has revealed several modifications that will improve the AS for signing and AS for verification. This CR updates the Ms reference point with these modifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The changes include the following:  - Enable a single signing resource for any PASSporT type, therefore simplifying implementations for clients, and enabling the addition of future PASSporT types without the need to define new signing resources; and  - Update the verification response so that it conveys information about all errors encountered during the verification process and facilitates correlating each error to the corresponding PASSporT. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Clients and signing services will not gain the benefits of a simplified signing resource. The client will not gain the benefit of obtaining PASSporT failure information. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 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:*** | | Notes to 24.229 editor:  Table V.2.6.2-3 is updated by this CR, and by CR 6556. 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 this CR. Because of this, the final version of Table V.2.6.2-3 shown in this CR contains two items that are defined in CR 6556:   * The "validClaims" value of the verifyResult parameter; * Table V.2.6.2-5 referenced in the Notes of Table V.2.6.2-3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Revision 1 (from C1-222705)   1. Corrected “singing” typo 2. In response to comments, added Table V.2.6.2-3 to just this CR 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. Described when verification result of “none” is generated 5. In response to comments, moved the optional verification response parameters for failures to a separate Table V.2.6.2-4.   Revision 2 (from C1-223008)   1. Moved notes out of tables V.2.5.2-1 and V.2.6.2-3 to normal text following each table 2. Changed 1st letter in bullets to lower-case. 3. Clarified text and added reference to subclause V.2.2 in bullets following Table V.2.5.2-1. | | | | | | | | |

\* \* \* First 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 |

\* \* \* Next 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. The verificationResponse may also contain verification results information for each verified PASSporT, as follows:

- if verification failed, then verificationResponse contains information describing the reason for the failure.

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 |

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 [verifyResult, ] as defined in table V.2.6.2-3 | 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.2.6.2-3 specifies the data types of the mandatory verifyResult parameter included in the verification response.

Table V.2.6.2-3: Data types for mandatory verifyResult parameters

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| verifyResult | structured data type containing  div,  verstatValue | M | Contains the verification results of a single Identity header field contained in the identityHeader parameter or an entry of the IdentityHeaders array of the verification request. |

Table V.2.6.2-4 specifies the additional data types included in the verification response when the verifyResult parameter contains a value of "TN-Validation-Failed".

Table V.2.6.2-4 specifies the data types of the optional verifyResults parameters included in the verification response.

Table V.2.6.2-4: Data types of optional verifyResult parameters when verstatValue is set to "TN-Validation-Failed"

|  |  |  |  |
| --- | --- | --- | --- |
| Parameter | Type; Value | Presence | Description |
| reasonCode | integer | O | Identifies the 4xx failure reason code of the failing PASSporT, as defined in RFC 8224 [252]. |

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