**3GPP TSG-CT WG1 Meeting #136-eC1-223950**

**E-Meeting, 12th – 20th May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.229** | **CR** | **6559** | **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 Corrections | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Neustar, Comcast, Oracle, Genband Ireland | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2022-05-02 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Update API defintion so that it can correctly sign and verify the various cpmbinations of PASSporT types that are encountered in real-world deployments. Updates fall into four main categories:   * Fix specific errors in parameter definitions; * Remove extraneous resources that aren’t needed in order to simplify implementations; * Add missing information that will help implementors (e.g., missing RFC references); and * Fix typo’s and make editorial clarifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Updated Figure V.2.2-1   * Removed /ecbSigning resource, since "ecb" is not a PASSporT type; and * Removed all verification resources except /verification (i.e., specific verification resources per PASSporT type are not needed since the PASSporT type to be verified is indicated by the protected header "ppt" parameter).   For signing request:   * Clarified text in V.2.5.1 (e.g., original text inadvertently implied that the signing request contains PASSporTs); * Updated Table V.2.5.2-1   + Corrected/clarified "dest" and "div" parameter definitions; and   + Added missing references. * Added Table V.2.5.2-1a to clarify parameter inclusion requirements per PASSporT type; and * Updated Table V.2.5.2-2 to clarify that the API client performs TN canonicalization, not the server.   For verification request:   * Updated Table V.2.6.2-1   + Changed "identityHeader" parameter from mandatory to optional, since this parameter is not needed when verifying an "rph" PASSporT;   + Changed IdentityHeader parameter name to "identityHeaders" (lowercase 'i');   + Changed "dest" parameter from optional to mandatory. It is always needed for replay attack detection; and   + Added notes clarifying the inclusion rules for the identityHeader and identityHeaders parameters of the verification request | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | * The presence of extraneous signing and verification resources increases implementation complextity; * /divSigning could incorrectly mend a broken authority chain if "div" parameter populated from Identity header field; * TN canonicalization may be performed incorrectly (e.g., the server could incorrectly add a ‘1’ prefix to 10-digit international number, making it look like a domestic number); * /verification unable to detect replayed PASSporT when "dest" parameter is missing; and * API ambiguity leads to interoperability issues. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | V.2.2, V.2.3.2, V.2.4.3.1, V.2.5.1, V.2.5.2, 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:*** | | Revision 1 (from C1-223514)   1. Removed “TS” in CR header; 2. Backed out signingRequest parameter name changes to maintain backwards compatibility; and 3. Corrected typos.   Revision 2 (from C1-223950)   1. Added Table V.2.6.2-1a to clarify the verification request inclusion rules for the identityHeader and identityHeaders parameters for the different combinations of PASSporT types being verified. 2. Moved note associated with table V.2.5.2-1a to inside the table itself. 3. Corrected miscellaneous editorials/typos. | | | | | | | | |

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

## V.2.2 Resource structure

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

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

The resource URI structure is:



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

NOTE: v1 is the version number of the API.

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

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

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

### V.2.3.2 Request header requirements

Table V.2.3.2-1 lists request header field requirements.

Table V.2.3.2-1: Header fields included in the requests

|  |  |  |
| --- | --- | --- |
| Header field name | Description | Presence |
| Content-Type | Describes the format of the request body. Shall be set to "application/json" | M |
| Accept | Describes the supported format of the response body. Shall be set to "application/json" if present | O |

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

#### V.2.4.3.1 General

If the server cannot process the request, the server provides an HTTP error response. The error response contains a JSON object specifying the error type.

The server provides a service error when the server is unable to process the request.

The server provides a policy error when the server is able to process the request, but not able to complete the service execution due to a policy restriction.

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

### V.2.5.1 General

To construct a PASSporT SHAKEN object specified in RFC 8588 [261], a PASSporT rph object specified in RFC 8443 [279] and RFC 9027 [278], or a PASSporT div object, specified in RFC 8946 [265], the client sends an HTTP POST request to the AS for signing containing the SIP request information plus any additional claim information to be signed by the target PASSporT type. If the request was successfully processed, then the received signingResponse contains an Identity header field value populated with a signed PASSporT of the requested type along with the appropriate Identity header field parameters.

Unsuccessful requests are responded with an HTTP 4xx or 5xx response.

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

### V.2.5.2 Data types

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

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

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

- a PASSporT rph JSON Web Token specified in RFC 8443 [279] and 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 "shaken" or "rph" PASSporT as specified in RFC 8224 [252], and from the Request-URI after retargeting for a "div" PASSporT as specified in RFC 8946 [265]. |
| div | identity claim JSON object, tn or uri. A hi element should be included. | O | Identifying the diverting user, taken from the Request-URI before retargeting as specified 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] and RFC 9027 [278]. |
| 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.2.5.2-1a specifies the signingRequest parameter inclusion rules per PASSporT type.

Table V.2.5.2-1a: signingRequest parameters per PASSporT Type

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| PASSporT Type | Parameter | | | | | | | |
| attest | dest | div | time | from | origid | rph | sph |
| shaken | M | M | X | M | M | M | X | X |
| div | X | M | M | M | M | X | X | X |
| rph | X | M | X | M | M | X | M | O |
| NOTE: "M" means "mandatory", "O" means "optional", and "X" means "not allowed". | | | | | | | | |

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 shall be canonicalized by the client before it is populated in the signingRequest following the procedure in RFC 8224 [252] 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.2.6.2 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] and RFC 8588 [261]. | O | This parameter contains the "shaken" Identity header field value to be verified (see NOTE-1). |
| identityHeaders | array of string; Identity header field values as specified in RFC 8224 [252], RFC 8443 [279], RFC 8946 [265], RFC 9027 [278]. One identityHeader claim per received Identity header field is sent. | O | This array contains the "div" and "rph" Identity header field values to be verified (see NOTE-2). |
| 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 | M | The destination identity taken from the Request-URI in the incoming request. |
| 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 |
| NOTE-1) For "shaken" PASSporT verification, an identityHeader parameter containing a "shaken" Identity header field shall be included in the verification request. Otherwise, the identityHeader parameter shall not be included in the verification request.  NOTE-2) For "rph" PASSporT verification, an identityHeaders parameter containing an "rph" Identity header field shall be included in the verification request. If the identityHeader parameter contains a "shaken" Identity header field, and/or the identityHeaders parameter contains an "rph" Identity header field, then all "div" Identity header field(s) received in an INVITE request shall be included in the identityHeaders parameter of the verification request. If "rph" PASSporT verification is not to be performed, and if the INVITE request does not contain any "div" Identity header fields, then the identityHeaders parameter shall not be included in the verification request. | | | |

Table V.2.6.2-1a specifies the inclusion rules for the verification request identityHeader and identityHeaders parameters for the different combinations of PASSporT types to be verified.

Table V.2.6.2-1a: Verification request identityHeader and identityHeaders parameter inclusion rules

|  |  |  |
| --- | --- | --- |
| PASSporT type(s) to be verified | Parameter | |
| identityHeader | identityHeaders |
| shaken | M | X |
| shaken, div | M | M |
| rph | X | M |
| rph, div | X | M |
| shaken, rph | M | M |
| shaken, rph, div | M | M |
| NOTE: "M" means "mandatory" and "X" means "not allowed". | | |

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 \* \* \* \*