**3GPP SA3LI#87-e-a S3i220538**

**Virtual meeting; October 4-6, 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.128** | **CR** | **433** | **rev** | **1** | **Current version:** | **17.6.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Editorial fix in the latest version of the TS 33.128 |
|  |  |
| ***Source to WG:*** | SA3-LI (Nokia, Nokia Shanghai Bell) |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | LI17 |  | ***Date:*** | 2022-10-06 |
|  |  |  |  |  |
| ***Category:*** | ***D*** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | One editorial error. |
|  |  |
| ***Summary of change:*** |  Error is corrected.  |
|  |  |
| ***Consequences if not approved:*** |  Error remains..  |
|  |  |
| ***Clauses affected:*** | 7.11.2.3 |
|  |  |
|  | **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:*** | S3i220538 |

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

#### 7.11.2.3 Signature validation

The IRI-POI present in the Telephony AS or IBCF, shall generate an xIRI containing a STIRSHAKENSignatureValidation record when the following conditions are met:

- Either IBCF or Telephony AS, is interacting with the VERIFICATION AS. Whether it is the Telephony AS or IBCF for sessions is based on network configuration and local policy of the CSP as described in clause 7.11.2.5.

- With one or more of the following are true:

- Request URI and To Headers of SIP INVITE or SIP MESSAGE request received from S-CSCF (in the case of Telephony AS) or from the previous IP network (in the case of IBCF) is a target identity.

- One or more of P-Asserted Identity, From, Diversion, History-Info Headers of SIP INVITE request received from S-CSCF (in the case of Telephony AS) or from the previous IP network (in the case of IBCF) is a target non-local identity without any prior intra-network diversions.

- One or more of P-Asserted Identity, From Headers of SIP MESSAGE request received from S-CSCF (in the case of Telephony AS) or from the previous IP network (in the case of IBCF) is a target non-local identity without any Diversion or History-Info headers.-

 If PASSporTs are received in the SIP INVITE or SIP MESSAGE request, they are submitted by the IBCF to the VERIFICATION AS for validation and the result is included in an outgoing SIP INVITE or SIP MESSAGE request together with possible RCD data or eCNAM data as Call-Info headers.

- If PASSporTs are received in the SIP INVITE or SIP MESSAGE request, they are submitted by the Telephony AS to the VERIFICATION AS for validation and the validation result is received from the Verification AS and the outgoing SIP INVITE or SIP MESSAGE possibly includes RCD data or eCNAM data as Call-Info headers.

NOTE: The IRI-POI may use the Via headers, Record-route headers to determine any prior intra-network diversions.

The IRI-POI present in the Telephony AS shall also generate an xIRI containing a STIRSHAKENSignatureValidation record when it detects the following conditions:

- Session is redirected.

- Request URI header of outgoing SIP INVITE is a target identity.

- Validation result is included in the outgoing SIP INVITE with the possible the RCD data and the eCNAM data as Call-Info headers.

The IRI-POI present in the LMISF-IRI or P-CSCF shall generate an xIRI containing a STIRSHAKENSignatureValidation record when the following conditions are met:

- With one or more of the following are true:

- Request URI or To header of SIP INVITE or SIP MESSAGE request sent to the UE is a target identity.

- One or more of P-Asserted Identity, From, Diversion, History-Info Headers of SIP INVITE request sent to the UE is a target non-local identity.

- One or more of P-Asserted Identity, From Headers of SIP MESSAGE request sent to the UE is a target non-local identity.

- SIP INVITE or SIP MESSAGE request sent to the UE includes SIP Call-Info headers containing possible RCD data or eCNAM data, and the result of the PASSporT verification.

In the above paragraphs, a validation result (i.e. result of all PASSporT verification) is included means a "verstat" parameter within the P-Asserted Identity header is included in the outgoing SIP INVITE or SIP MESSAGE.

The following table contains parameters, with IRITargetIdentifier, generated by the IRI-POI.

Table 7.11.2.3-1: Payload for STIRSHAKENSignatureValidation record

|  |  |  |
| --- | --- | --- |
| Field name | Description | M/C/O |
| pASSporTs | Identifies the content of the SIP Identity headers added by the originating network and transit networks. See TS 24.229 [74] and RFC 8224 [70].This is a set of PASSporT parameter. See table 7.11.2.2-2. | C |
| rCDTerminalDisplayInfo | RCD display information when applicable. See IETF draft-ietf-stir-passport-rcd-12 [73]. | C |
| eCNAMTerminalDisplayInfo | eCNAM display information when applicable. See TS 24.196 [72]. | C |
| sHAKENValidationResult | SHAKEN validation result: TN-Validation-Passed, TN-Validation-Failed, No-TN-Validation. See TS 24.229 [74] and IETF RFC 8588 [71]. | M |
| sHAKENFailureStatusCode | SHAKEN status code when validation fails in the terminating network. See IETF RFC 8224 [70]. | C |
| encapsulatedSIPMessage | Encapsulated SIP INVITE or SIP MESSAGE request that carries P-Asserted Identifier or From header that includes the SHAKEN validation result (Outgoing SIP request) based on the structure defined in table 7.12.4.2-2. (see NOTE below). | C  |
| NOTE: The same SIP message may be encapsulated in the xIRI IMSMessage as well. |

When the termination network performs SHAKEN verification, one of the following values shall be assigned to the SHAKEN validation result parameter as part of the display information: "TN-Validation-Passed", "TN-Validation-Failed", or "No-TN-Validation". In case of TN-Validation-Failed, the SHAKEN failure status code shall be present and coded as an integer. The SHAKEN failure status codes are at least, according to RFC 8224 and to IANA Session Initiation Protocol (SIP) Parameters [75]:

- 403 "Stale Date" response code is sent when the verification service receives a request with a Date header field value that is older than the local policy of the CSP for freshness permits. The same response may be used when the "iat" has a value older than the local policy of the CSP for freshness permits.

- 428 "Use Identity Header" response code is sent when the verification service receives a SIP request that lacks an Identity header. This is to indicate that the request should be re-sent with an Identity header.

- 436 "Bad Identity-Info" response code is used to indicate an inability to acquire the credentials needed by the verification service for validating the signature in an Identity header field.

- 437 "Unsupported Credential" response code is used when the verification service cannot validate the certificate referenced by the URI of the Identity-Info header, for reasons such as failing to trust the issuing certification authority (CA) or failing to support the algorithm with which the credential was signed.

- 438 "Invalid Identity Header" response code is used to indicate that of the set of Identity header fields in a request, no header field with a valid and supported Identity token has been received.

### \*\* End of all Changes \*\*