**3GPP SA3LI#86-b S3i220416**

**Sophia Antipolis, France, 30 August 2022 – 2 September 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.128** | **CR** | **387** | **rev** | **1** | **Current version:** | **18.0.0** |  |
|  | | | | | | | | |
| *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:*** | STIR/SHAKEN: Enhancements to stage 3 LI descriptions (LI\_X2) | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | SA3-LI (Nokia, Nokia Shanghai Bell, Ministère Economie et Finances) | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | LI17 | | | | |  | ***Date:*** | | | 2022-09-01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | ***F*** |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | STIR/SHAKEN related stage 3 descriptions do not address the redirected call scenarios. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | xIRI generation algorithms are enhanced. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Erratic implementation of STIR/SHAKEN related LI functions | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7.11.2.2, 7.11.2.3, 7.11.2.x1 (new), 7.11.2.x2 (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | S3i220416 | | | | | | | | |

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

#### 7.11.2.2 Signature generation

The IRI-POI present in the Telephony AS or IBCF, shall generate an xIRI containing a STIRSHAKENSignatureGeneration record under the following conditions:

- Telephony AS or IBCF is interacting with the SIGNING 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 7.11.2.4.

- When P-Asserted Identity or From header of SIP INVITE or SIP MESSAGE request received from S-CSCF is a target identity with the conditions mentioned below:

- The identities in one or both of those headers are used to interact with the SIGNING AS.

- The "shaken" PASSporT is not received in the SIP INVITE request from the S-CSCF.

- The "shaken" PASSporT is received from the SIGNING AS.

- The "shaken" PASSporT is included in the outgoing SIP INVITE or SIP MESSAGE.

- When the "ReportDiversionPASSporTInfo" parameter is set to "True" in the ActivateTask with P-Asserted Identity or From header of SIP INVITE or SIP MESSAGE request received from S-CSCF is a target identity with the conditions mentioned below:

- The identities in one or both of those headers are used to interact with the SIGNING AS.

- A "shaken" PASSporT or a "div" PASSporT with those identities are included in the "orig" claim of "shaken" or "div" PASSporT received from the SIGNING AS .

- The "shaken" PASSporT or a "div" PASSporT with those identities are included in the "orig" claim of "shaken" or "div" PASSporT in the outgoing SIP INVITE or SIP MESSAGE.

- When Diversion header or the History Info of SIP INVITE request received from the S-CSCF includes a target identity with the conditions mentioned below:

- The identities in one or both of those headers are used to interact with the SIGNING AS.

- The "div" PASSporT with those identities in the "div" claim is not received in the SIP INVITE request from the S-CSCF.

- The "div" PASSporT with those identities in the "div" claim is received from the SIGNING AS.

- The "div" PASSporT with those identities in the "div" claim is included in the outgoing SIP INVITE.

* When the "ReportDiversionPASSporTInfo" parameter is set to "True" in the ActivateTask with Diversion or HistoryInfo header of SIP INVITE request received from S-CSCF includes the target identity with the conditions mentioned below:
* The identities in P-Asserted Identity or From of SIP INVITE received from the S-CSCF are used to interact with the SIGNING AS.
* A "div" PASSporT with the identities in P-Asserted Identity or From of SIP INVITE request received from S-CSCF are included in the "orig" claim of "div" PASSporT received from the SIGNING AS .
* The "div" PASSporT with the identities in P-Asserted Identity or From of SIP INVITE request received from S-CSCF are included in the "orig" claim of "div" PASSporT in the outgoing SIP INVITE.
* When Request URI of outgoing SIP INVITE is a target non-local ID and is present in the "dest" claim of "shaken" or "div" PASSporT received from the SIGNING AS and the same is included in the outgoing SIP INVITE.
* When Request URI of outgoing SIP MESSAGE is a target non-local ID and is present in the "dest" claim of "shaken" PASSporT received from the SIGNING AS and the same is included in the outgoing SIP MESSAGE.

- When Telephony AS is interacting with the SIGNING AS, and when Request URI of SIP INVITE received from the S-CSCF is a target identity with the conditions mentioned below:

- The identity is used to interact with the SIGNING AS.

- The "div" PASSporT with that identity in the "div" claim is received from the SIGNING AS.

- The "div" PASSporT with that identity in the "div" claim is included in the outgoing SIP INVITE

When the target is not a non-local ID, the STIRSHAKENSignatureGeneration includes only the PASSporT received in the SIGING AS response with the following rules:

* When the "ReportDiversionPASSporTInfo" parameter is set to "True" in the ActivateTask, all of the PASSporT received from the SIGNING AS.
* When the "ReportDiversionPASSporTInfo" parameter is set to "False" in the ActivateTask:
* If P-Asserted Identity or From header in the SIP INVITE or SIP MESSAGE received from the S-CSCF is a target identity, then only "shaken" PASSporT received from the SIGNING AS with those identities in the "orig" claim of the "shaken" PASSporT.
* If Diversion or HistoryInfo header in the SIP INVITE received from the S-CSCF is a target identity, then only the "div" PASSporT received from the SIGNING AS with those identities in the "div" claim of "div" PASSporT.
* If REQUEST URI or To header in the SIP INVITE received from the S-CSCF is a target identity, then only the "div" PASSporT received from the SIGNING AS with those identities in the "div" claim of "div" PASSporT.

When the target is non-local ID, STIRSHAKENSignatureGeneration includes all of the PASSporT included in the outgoing SIP message.

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

Table 7.11.2.2-1: Payload for STIRSHAKENSignatureGeneration record

|  |  |  |
| --- | --- | --- |
| Field name | Description | M/C/O |
| pASSporTs | Identifies the content of the SIP Identity headers added by the originating network and transit networks. This is a set of PASSporT parameter. See table 7.11.2.2-2. | M |
| encapsulatedSIPMessage | Encapsulated SIP INVITE or SIP MESSAGE request that includes SIP Identity header carrying the PASSporT (Outgoing SIP request) based on the structure defined in table 7.12.4.2-2 (see NOTE below). | M |
| NOTE 1: For the backward compatibility purposes the parameter is coded as OPTIONAL in the ASN.1 schema (Annex A.).  NOTE 2: The same SIP message may be encapsulated in the xIRI IMSMessage as well. | | |

Table 7.11.22-2: Details for PASSporT parameter

|  |  |  |
| --- | --- | --- |
| Field name | Description | M/C/O |
| pASSporTHeader | PASSporT Header as defined in RFC 8224 [70] clause 4 for "shaken” PASSporT, in RFC 8946 [76] clause 3 for "div” PASSportT and in TS 24.229 [74]. See table 7.11.2.2-3. | M |
| pASSporTPayload | PASSporT Payload as defined in RFC 8224 [70] clause 4 for "shaken” PASS, in RFC 8946 [76] clause 3 for "div” PASSporTand in TS 24.229 [74]. See table 7.11.2.2-4. | M |
| pASSporTSignature | PASSporT Signature as defined in RFC 8224 [70] clause 4 for "shaken” PASSporT, in RFC 8946 [76] clause 3 for "div” PASSporTand in TS 24.229 [74]. | M |

Table 7.11.2.2-3: Details for pASSporTHeader parameter

|  |  |  |
| --- | --- | --- |
| Field name | Description | M/C/O |
| type | Shall be populated with the type contained in the PASSporT Header as defined in RFC 8225 [69] clause 4.1 for "shaken” PASSporT and in RFC 8946 [76] clause 3 for "div” PASSporT.. | M |
| algorithm | Shall be derived from the value of the 'alg' parameter of the PASSporT Header as defined in RFC 8225 [69] clause 4.2 for "shaken” PASSporT and in RFC 8946 [76] clause 3 for “div” PASSporT. | M |
| ppt | Shall be derived from the value of the 'ppt' parameter of the PASSporT Header as defined in RFC 8225 [69] clause 8.1 for “shaken” PASSporT if the PASSporT Header contains a ppt parameter and in RFC 8946 [76] clause 3 for “div” PASSporT. | C |
| x5u | Shall be populated with the URI contained in the 'x5u' parameter of the PASSporT Header as defined in RFC 8225 [69] clause 4.3 for “shaken” PASSporT and in RFC 8946 [76] clause 3 for "div” PASSporT.. | M |

Table 7.11.2.2-4: Details for pASSporTPayload parameter

|  |  |  |
| --- | --- | --- |
| Field name | Description | M/C/O |
| issuedAtTime | Shall be populated with the GenrealizedTime format timestamp converted from the NumericDate contained in the 'iat' parameter of the PASSporT Payload as defined in RFC 8225 [69] clause 5.1.1 and in RFC 8946 [76] clause 3... | M |
| originator | Shall be populated with the value of the "orig" claim of the PASSporT Payload as defined in RFC 8225 [69] clause 5.2.1 and in RFC 8946 [76] clause 3. | M |
| destination | Shall contain the list of destinations contained in the "dest" claim of the PASSporT Payload as defined in RFC 8225 [69] clause 5.2.1 and in RFC 8946 [76] clause 3. | M |
| diversion | Shall be populated with the "div" claim of the "div" PASSporT payload. For first diversion this contains the original identifier of the destination as defined in RFC 8946 [76] clause 3 for “div" PASSporT. | C |
| attestation | Indicates the attestation level as defined in RFC 8588 [71] clause 4 for the "shaken” PASSporT. The different values of attestation level are A = Full Attestation, B= Partial Attestation, C = Gateway Attestation (See NOTE 3 below). | M |
| origID | Shall be populated with the value of the origID contained in the 'origid' parameter of the PASSporT Payload as defined in RFC 8588 [71] clause 5 for the “shaken” PASSporT (See NOTE 4 below). | M |
| NOTE 3: For the backward compatibility purposes the parameter is coded as MANDATORY in the ASN.1 schema (Annex A.). 'attestation' is mandatory for "shaken" PASSporT and absent for "div" PASSporT. Therefore, for div PASSporT, since "attestation" is not available, the placeholder value “Not available” shall be used.  NOTE 4: For the backward compatibility purposes the parameter is coded as MANDATORY in the ASN.1 schema (Annex A.). This parameter is mandatory for "shaken" PASSporT and absent for the "div" PASSporT. Therefore, for div PASSporT, since "origId" is not available, the placeholder value “Not available” shall be used. | |  |

### \*\* Next 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.

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

#### 7.11.2.x1 IMS Network Function that interacts with signing AS

The Telephony AS interacts with the SIGNING AS when any of the following is true:

* RCD is supported.
* Intra-CSP session signing is required.
* CSP choice for signing is AS.

The IBCF interacts with the SIGNING AS when all of the following are true:

* RCD is not supported.
* Intra-CSP session signing is not required.
* CSP choice for signing is IBCF.

The IBCF also interacts with the SIGNING AS for an IMS emergency session.

The presence of RCD is on a per call basis. The same rules also apply for SMS over IP with MSISDN-less destination number (i.e. SM-SC is not on the message transfer path).

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

#### 7.11.2.x2 IMS Network Function that interacts with the verification AS

The Telephony AS interacts with the VERIFICATION AS when any of the following is true:

* Intra-CSP session verification is required.
* CSP choice for verification is AS.
* CSP choice for emergency session callback verification is AS.

The IBCF interacts with the VERIFICATION AS when all of the following are true:

* Intra-CSP session verfication is not required.
* CSP choice for verification is IBCF.

The IBCF also interacts with the VERIFICATION AS for an IMS emergency session callback when the CSP choice for verification for emergency callback session is IBCF.

The same rules also apply SMS over IP with MSISDN-less destination number (i.e.SM-SC is not on the message transfer path).

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