**SA WG3 Meeting S3#115-Adhoc S3-241211r1**

**April 15 – 19, 2024, e-meeting**

**Source: Nokia, Nokia Shanghai Bell, CableLabs**

**Title: new solution to support Third Party User Identities in IMS using STIR/SHAKEN**

**Document for: Approval**

**Agenda Item: 5.2**

**Work Item / Release: FS\_NG\_RTC\_Ph2/Rel19**

# 1 Decision/action requested

***Approve the solution added to TR 33.790***

# 2 References

[1] 3GPP TR 23.700-77 Study on system architecture for next generation real time communication services Phase 2

[2] 3GPP TR 33.790 Study on the security support for the Next Generation Real Time Communication services phase 2

# 3 Rationale

The contribution proposes a new solution to support Third Party User Identities in IMS using STIR/SHAKEN.

# 4 Detailed proposal

All content in the change part is new.

\* \* \* \* First change\* \* \* \*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[x] 3GPP TS 24.229: "IP Multimedia Call Control based on SIP and SDP; Stage 3".

[y] ATIS-1000074: "Signature-based Handling of Asserted information using Tokens (SHAKEN)".

[z] IETF draft-ietf-stir-passport-rcd-26: "PASSporT Extension for Rich Call Data".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[xx] IETF draft-ietf-sipcore-callinfo-rcd-09: "SIP Call-Info Parameters for Rich Call Data".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[yy] 3GPP TS 23.700-77: "Study on system architecture for next generation real time communication services Phase 2".

\* \* \* \* Next change \* \* \* \*

## 6.x Solution #x: Support of Third Party specific User Identities in IMS using STIR/SHAKEN

### 6.x.1 Introduction

The solution addressed Key issue #1: Third party specific user identities.

The Ms reference point as described in TS 24.229 [10], Annex V.2, is used to request signing of an Identity header field or request verification of a signed assertion in an Identity header field. This enables calling number verification using signature verification and attestation information based on the STIR/SHAKEN framework.

This solution proposes to use the existing Ms reference point and procedures for signing and verifying other identities than for example the ones in the P-Asserted-Identity header field which are mainly in the format of a SIP URI or Tel URL. For verification of the calling line identity the IBCF or an IMS AS of the originating network sends a HTTP signing request to the signing AS which in turn replies with a Personal Assertion Token (PASSporT). At the terminating network side, the IBCF or an IMS AS sends a HTTP verification request to the signing AS including the PASSporT which in turn replies with a verification success or failure message. The Ms reference point involves an AS for signing of the Identity at the originating side and another AS for verification of the signed token at the terminating side. It can be extended to enable signing and verification of different kind of identities.

The draft-ietf-stir-passport-rcd-26 [18] describes an optional mechanism for PASSporT and the associated STIR procedures allowing to sign and verify additional data elements including for example:

- Name of the calling person or of an entity.

- Caller ID along with related display information that would be rendered to the called party during alerting.

- Hyperlinks to images, logos, pictures of faces, Avatar representations, or to similar external profile information.

- Information related to the official address of the caller.

- Information related to an organization, or categories/departments of organizations and institutions.

- Possibly other Rich Call Data (RCD) information elements.

The solution assumes that the types of Third Party specific User Identities used in IMS are aligned with the definitions in draft-ietf-sipcore-callinfo-rcd-09 [19]. Other possible user identity information, e.g Avatar ID can also be added and used for signing and verification. The concrete list of Third Party specific User identities is determined during normative phase in alignment with stage 3 and IETF.

Example of a Call-Info header field according draft-ietf-sipcore-callinfo-rcd-09 [19]:

Call-Info: <https://example.com/qbranch.json>;purpose=jcard.

Example contents of a URL linked jCard JSON file:

["vcard",

 [

 ["version",{},"text","4.0"],

 ["fn",{},"text","SA2 WG"],

 ["org",{},"text","3GPP;SA2 WG delegate"],

 ["photo",{},"uri","https://example.com/photos/sa2-256x256.png"],

 ["logo",{},"uri","https://example.com/logos/3gpp-256x256.jpg"],

 ["logo",{},"uri","https://example.com/logos/3gpp-64x64.jpg"]

 ]

]

Example "rcd" PASSporTs with URL linked jCard JSON file:

{

"orig": {"tn": "12025551000"},

"dest": {"tn": ["12155551001"]},

"iat": 1443208345,

"rcd": {

"nam": "Q Branch Spy Gadgets",

"jcl": "https://example.com/qbranch.json"

},

"rcdi": {

"/jcl":"sha256-qCn4pEH6BJu7zXndLFuAP6DwlTv5fRmJ1AFkqftwnCs",

"/jcl/1/3/3":"sha256-RojgWwU6xUtI4q82+kHPyHm1JKbm7+663bMvzymhkl4",

"/jcl/1/4/3":"sha256-jL4f47fF82LuwcrOrSyckA4SWrlElfARHkW6kYo1JdI",

"/jcl/1/5/3":"sha256-GKNxxqlLRarbyBNh7hc/4lbZAdK6B0kMRf1AMRWPkSo"

}

}

The overall reference architecture is depicted in Figure 6.x.1-1. The Third Party network can be connected to the serving IMS network via UNI or NNI interfaces. The serving IMS network handles outbound SIP calls from the Third Party network.



Figure 6.x.1-1: Third Party network connected to the serving IMS network

### 6.x.2 Solution detail

There are several options how and where Third Party specific user identities are signed and verified, which allow for different deployment scenarios, e.g. using UNI or NNI interface between Third Party and IMS network, with different levels of impact to the Third Party network and the IMS network and with different levels of trust relationship between both.

Generally, the HSS stores one or several URL(s) pointing to resources on Web servers where Third Party specific user identities and data are stored. This includes URL(s) pointing to Rich Call Data (RCD URL) as described above or pointing to any other user or Third Party specific data. Storing just URL(s) in the HSS avoids potential misusing a Third Party specific user identities that no longer belongs to an UE to initiate IMS calls (e.g., the user uses the identities allocated by a particular company even after leaving it), and possibly frequent updates to the data based on request from the Third Party network and avoids defining Third Party specific data formats in HSS. Nevertheless, the HSS may also store additional data in the subscription of a Third Party subscriber like caller name, organization information, job title, and location information. The URL(s) and possibly other data are fetched from the HSS by the CSCF or IMS AS depending which entity invokes the signing. Optionally, the IMS AS may use the RCD URL received from the HSS to fetch Rich Call Data from a server that can be in the operator domain or external in the Third Party network and provide these data or the RCD URL in SIP signalling (SIP INVITE) towards the terminating party. The fetched Rich Call Data information is used by the Signing AS for signing the RCD PASSporT and by the Verification AS to verify the signed RCD PASSporT.

The SIP header extensions (e.g. Call-Info header) required to transfer Third Party specific user identity information are defined by stage 3.

Editor's Note: In case RCD is stored in HSS and URLs are included in the RCD, e.g. URIs of photo and/or logo are data elements of the RCD, whether the data is fetched by source IMS or target IMS based on the URIs is FFS.

The procedures to sign and verify PASSporT tokens follow the descriptions in TS 24.229 [10] with the main difference that besides telephone numbers also other information as described in draft-ietf-sipcore-callinfo-rcd-09 [19] and draft-ietf-stir-passport-rcd-26 [18] can be used for signing and verification.



Figure 6.x.2-1: Third Party Identity signing and verification workflow

1. The originating UE sends a SIP INVITE that contains the IMPU of the calling UE and optional Third Party specific user identity (or third party identity).

2. The CSCF forwards the SIP request to the IMS AS.

3. The IMS AS checks with HSS if the calling user (IMPI or IMPU based) is authorized to use the third party identity based on subscription.

4a. The IMS AS/CSCF retrieves Rich Call Data (RCD) information of the third party identity from HSS. HSS may return RCD URL pointing to the RCD on Web servers or concrete RCD, like caller name, job title, organization, and location information, etc., based on deployment option.

NOTE: If HSS returns concrete RCD to the IMS AS in this step, HSS should fetch the RCD from the third party database in advance based on RCD URL/third party identity associated to the IMPU/IMPI.

4b. Optionally, the IMS AS/CSCF may retrieve RCD of the third party identity from third party database based on the third party identity or RCD URL.

5. The IMS AS/CSCF calls STI-AS to sign the SIP header, e.g. call-info, which including RCD URL or RCD of the third party identity.

6. The STI-AS returns the signed SIP header back to the IMS AS/CSCF.

7. The IMS-AS/CSCF forward the SIP INVITE to the terminating IMS subsystem which including signed RCD URL or RCD of the third party identity.

8. The terminating IMS subsystem invokes the STI-VS to verify the signed RCD URL or RCD.

9. If verification is successful, . .

10. The terminating IMS subsystem sends SIP INVITE to terminating UE which including the RCD if verification is successful in step 8. Otherwise, terminating IMS subsystem may send SIP INVITE to terminating UE without including RCD.

11. The terminating UE sends 18X/200 to originating IMS subsystem and to the originating UE.

### 6.x.3 Evaluation

TBD

\* \* \* \* End of changes \* \* \* \*