**3GPP TSG-SA3 Meeting #108e-AdHoc *S3-222836***

**e-meeting, 10 - 14 October 2022**

**Source: Ericsson**

**Title: Update solution#1**

**Document for: Approval**

**Agenda Item: 5.15**

# 1 Decision/action requested

***Approve the pCR to TR 33.890.***

# 2 References

[1] 3GPP TR 23.700-87: " Study on system architecture enhancement for next generation real time communication; phase 2"

[2] 3GPP TR 33.890: "Study on security support for Next Generation Real Time Communication services”

# 3 Rationale

This contribution proposes update to solution#1 by clarifying the Database in Prerequisites, updating the figures and flows for more accurate description.

# 4 Detailed proposal

Approve the following changes to TR 33.890 [2].

\*\*\* Start of changes \*\*\*

# 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*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-87: "Study on system architecture enhancement for next generation real time communication".

[3] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[4] 3GPP TS 24.229: IP Multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

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

[6] IETF draft-ietf-stir-passport-rcd-18, "PASSporT Extension for Rich Call Data"

[7] draft-ietf-sipcore-callinfo-rcd-03: "SIP Call-Info Parameters for Rich Call Data".

[8] IETF RFC 8224: "Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[XX] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2”

\*\*\* End of 1st Change \*\*\*

\*\*\* Start of 2nd Change \*\*\*

## 6.1 Solution #1: How the Originating IMS network signs the 3rd party IDs and terminating IMS network verifies the 3rd party IDs

### 6.1.1 Introduction

This solution addresses the key issue #1 (Third party specific user identities). As stated in the key issue details, there are scenarios that the 3rd party subscribers (e.g., employees) use third party IDs (e.g., enterprise employee ID). The IMS network can present the 3rd party ID (3P ID) to the callee during subsequent calling process. From the security point of view, the enhanced IMS network needs to be able to support the identity verification and authorization of 3rd party user during an IMS call.

This solution proposes to use the existing Ms reference point and procedures as described in TS 24.229 [4] and STIR/SHAKEN framework [5] while adopting draft-ietf-stir-passport-rcd-18 [6].

### 6.1.2 Solution details

#### 6.1.2.1 Solution Description

The Ms reference point as described in TS 24.229 [4] is used to request signing of a SIP Identity header field and verification of a signed assertion in a SIP Identity header field. This enables calling number verification using signature verification and attestation information based on the STIR/SHAKEN framework.



Figure 6.1.2.1-1: Ms reference point operation (see TS 24.229 [XX], Annex V.2)

Here is the SHAKEN Reference Architecture in ATIS-1000074 [5].

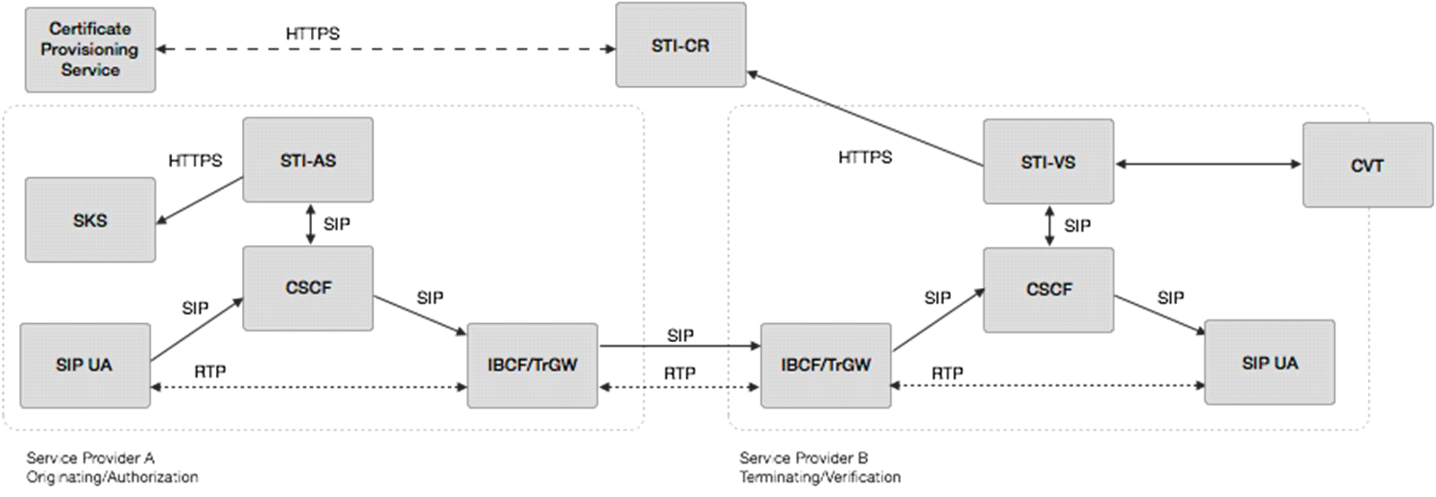


Figure 6.1.2.1-2: SHAKEN Reference Architecture

However, securing the display name of a caller was outside the scope of Secure Telephone Identity Revisited (STIR) while draft-ietf-stir-passport-rcd-18 [6] documents an optional mechanism for PASSporT and the associated STIR procedures allowing to sign and verify additional data elements including for example:

- the name of the calling person or of an entity;

- the traditional caller ID along with related display information that would be rendered to the called party during alerting;

- hyperlinks to images, such as logos or pictures of faces, or to similar external profile information;

- information related to the location of the caller;

- information related to an organization the caller is associated with, or categories/departments of organizations and institutions;

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

The types of 3rd party user identities as used in IMS need to be aligned with the definitions in [6] and include the calling person's name and job title, information related to the organization the caller is associated with and information related to the caller's location. The overall reference architecture is depicted in Figure 6.X.2.1-1. The 3rd party (Enterprise) 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.

There are several options how and where the 3rd party user identities are signed and verified. These options allow for different deployment scenarios, e.g., using UNI or NNI interface between 3rd Party and IMS network, with different levels of impact to the 3rd Party network and the IMS network provider and with different levels of trust relationship between both.

This solution proposes that the originating IMS network invokes the signing on behalf of 3rd Party. In this case the signing AS in Figure 6.1.2.1-1 is invoked by the originating IMS network and the verification of the signature is invoked in the terminating IMS network.

Prerequisites:

1. The 3rd Party specific user identities that are subject for signing in the originating IMS network and the corresponding rich call data information related to each 3rd Party specific user identity are associated to the corresponding IMS identities in a Database. Who owns and how this Database is administered/provisioned is out of scope of the present solution.

NOTE 1: In the PBX case, it is assumed that this Database is under control of the 3rd Party (Enterprise) as the enterprise is responsible for assigning the IMS identities which are provided by the IMS operator to their employees and therefore also maintaining the corresponding Rich Call Data information. In the single UE case, the Database could be provided by the originating IMS operator and allow certain access to the calling UE via a UE self-management portal. The access to the UE self-management portal is assumed to be secured. How this is done is out of scope of the present solution.

2. Originating IMS network is assumed to have a secure channel to the Database which includes Rich Call Data information. How this secure channel is set-up is out of scope of the present solution.

NOTE 2: When the Database is located outside the IMS operator domain, the access to the Database can be secured in the same way as the SIP trunk link between the IMS network and the PBX; i.e., using mutual TLS as defined in Clause S.2.2 of TS 23.228 [XX].

Editor's Note: How to resolve the case when UE has multiple 3rd party ID is ffs.

Editor's Note: How to resolve the case when the users of the 3rd party will dynamically change (e.g., employees leaving or joining an enterprise) is ffs.

#### 6.1.2.2 How Originating IMS network invokes the signing on behalf of 3rd party (SIP trunk)



Figure 6.1.2.2-1: How Originating IMS network invokes the signing on behalf of 3rd party (SIP trunk)

1. The 3rd party PBX sends a SIP INVITE that contains the IMS Identity of the calling UE and that may or may not contain the third party ID on behalf of 3rd party subscriber to IBCF.

2. The IBCF forwards the SIP request to the IMS subsystem entity. The IMS subsystems include I/S-CSCF, MMtel AS and etc. (details not shown in the figure)

3. The originating IMS subsystem checks whether the IMS subscription of the calling PBX is authorized to use 3P IDs. If the PBX is not authorized to use 3P IDs, then the originating IMS subsystem ignores the 3P ID within the SIP INVITE (if present) and do not execute the rest of 3P ID related steps during the call set-up. The call continues without presenting 3P ID to the called endpoint.

If the PBX is authorized to use 3P IDs, the originating IMS subsystem gets Rich Call Data of 3rd party subscriber from the Database based on the received IMS identity. If no RCD data exists for this user (IMS identity), the rest of 3P ID related steps are not executed during the call set-up. The call continues without presenting 3P ID to the called endpoint.

NOTE: If no 3P ID is received in the SIP INVITE from the PBX, suppression of a Database lookup can be optionally applied based on a local policy. If there is a mismatch between the received 3P ID in the SIP INVITE and data retrieved from the Database based on the IMS identity, it is governed by a local policy of the originating IMS subsystem how the population of the Rich Call Data into the SIP Identity header will be done.

4. The originating IMS subsystem adds a P-Asserted-Identity header field asserting the telephone number and Rich Call Data of the 3rd party subscriber and invokes the STI-AS to sign the Identity header based on Figure 6.12.1-2: SHAKEN Reference Architecture and TS 24.229 [4].

5. STI-AS interacts with SKS (not shown in the figure) and signs the SIP identity header according to STIR/SHAKEN framework and draft-ietf-stir-passport-rcd-18.

6. STI-AS returns the signed SIP identity header back to IMS subsystem.

Editor's Note: Whether the alignment with SA2 is needed is FFS.

7. The originating IMS subsystem, through standard solution, routes the call to the egress IBCF. Then SIP INVITE is routed over the NNI through the standard inter-domain routing configuration. The terminating service provider’s ingress IBCF receives the INVITE over the NNI and forwards to terminating IMS subsystems.

8. The terminating IMS subsystem entity invokes the STI-VS to verify the signed SIP identity header

9. STI-VS interacts with STI-CR to validate the certificate and extracts public key and verify the signature in the Identity header field, which validates the Caller ID and Rich Call Data when signing the INVITE on the originating STI-AS based on Figure 6.X.2.1-2: SHAKEN Reference Architecture and TS 24.229 [4].

10. Depending on the result of the STI validation, STI-VS determines that the call is to be completed with an appropriate indicator and the result is passed back to terminating IMS subsystem which continues to set up the call to the terminating SIP UA. If the Caller ID is validated OK but not the rich call data, the call can continue but without showing name card info to terminating SIP UA.

11. The SIP INVITE with verstat parameter is sent to terminating SIP UA.

12. The terminating SIP UA sends 18X and 200 to originating IMS subsystem.

13. Originating IMS subsystem sends 18X and 200 to originating SIP UA. The call continues following standard solution.

#### 6.1.2.3 How Originating IMS network invokes the signing on behalf of 3rd party (Single SIP registration)



Figure 6.1.2.3-1: How Originating IMS network invokes the signing on behalf of 3rd party (single SIP registration)

1. The 3rd party subscriber sends a SIP INVITE that contains the IMS Identity of the calling UE and may or may not contain the 3P ID.

2. The originating IMS subsystem checks whether the IMS subscription of the calling UE is authorized to use 3P IDs. If the UE is not authorized to use 3P IDs, then the originating IMS subsystem ignores the 3P ID within the SIP INVITE (if present) and do not execute the rest of 3P ID related steps during the call set-up. The call continues without presenting 3P ID to the called endpoint

If the UE is authorized to use 3P IDs, the originating IMS subsystem gets Rich Call Data of 3rd party subscriber from the Database based on the received IMS identity. If no RCD data exist for this user (IMS identity), the rest of 3P ID related steps are not executed during the call set-up. The call continues without presenting 3P ID to the called endpoint.

NOTE: If no third-party ID info is received in the SIP INVITE from the UE, suppression of a Database lookup can be optionally applied based on a local policy. If there is a mismatch between the received 3P ID in the SIP INVITE and data retrieved from the Database based on the IMS identity, it is governed by a local policy of the originating IMS subsystem how the population of the Rich Call Data into the SIP Identity header will be done.

3. The originating IMS subsystem adds a P-Asserted-Identity header field asserting the telephone number and rich call data of the SIP UA and invokes the STI-AS to sign the Identity header based on Figure 6.1.2.1-2: SHAKEN Reference Architecture and TS 24.229 [4].

Editor's Note: Whether the alignment with SA2 is needed is FFS.

4. STI-AS interacts with SKS (not shown in the figure) and signs the SIP identity header according to STIR/SHARKEN framework and draft-ietf-stir-passport-rcd-18.

5. STI-AS returns the signed SIP identity header back to IMS subsystem.

6. The originating IMS subsystems, through standard solution, routes the call to the egress IBCF. Then SIP INVITE is routed over the NNI through the standard inter-domain routing configuration. The terminating service provider’s ingress IBCF receives the INVITE over the NNI and forwards to terminating IMS subsystems.

7. The terminating IMS subsystems invoke the STI-VS to verify the signed SIP identity header.

8. STI-VS interacts with STI-CR to validate the certificate and extracts public key and verify the signature in the Identity header field, which validates the Caller ID and rich call data when signing the INVITE on the originating STI-AS based on Figure 6.X.2.1-2: SHAKEN Reference Architecture and TS 24.229 [4].

9. Depending on the result of the STI validation, STI-VS determines that the call is to be completed with an appropriate indicator and the result is passed back to terminating IMS subsystem which continues to set up the call to the terminating SIP UA. If the Caller ID is validated OK but not the Rich Call Data, the call can continue but without showing name card info to terminating SIP UA.

10. The SIP INVITE with verstat parameter is sent to terminating SIP UA.

11. The terminating SIP UA sends 18X and 200 to originating IMS subsystem.

12. Originating IMS subsystem sends 18X and 200 to originating SIP UA. The call continues following standard solution.

### 6.1.3 Evaluation

TBD

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