|  |  |
| --- | --- |
| 3GPP TR 33.790 V0.2.0 (2024-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on the security support for the next generation real time communication services phase 2  (Release 19) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Assumptions 7

4.1 General 7

4.2 Architectural Assumptions and Principles 7

5 Key issues 8

5.1 Key issue #1: Third party specific user identities 8

5.1.1 Key issue details 8

5.1.2 Threats 8

5.1.3 Potential security requirements 8

5.2 Key issue #2: Security of IMS based Avatar Communication 8

5.2.1 Key issue details 8

5.2.2 Threats 8

5.2.3 Potential security requirements 9

5.3 Key Issue #3: Security and privacy aspects of IMS DC capability exposure 9

5.3.1 Key issue details 9

5.3.2 Security threats 9

5.3.3 Potential security requirements 9

6 Solutions 10

6.0 Mapping between key issues and solutions 10

6.1 Solution #1: Signing/verification of third party ID information 10

6.1.1 Introduction 10

6.1.2 Solution details 10

6.1.3 Evaluation 12

6.2 Solution #2: Security of 3rd party specific identities 12

6.2.1 Introduction 12

6.2.2 Solution details 12

6.2.2.1 Solution Description 12

6.2.2.2 How the Originating IMS network invokes the signing on behalf of 3rd party (SIP trunk) 14

6.2.2.3 How the Originating IMS network invokes the signing on behalf of 3rd party (Single SIP registration) 15

6.2.3 Evaluation 17

6.3 Solution #3: Support of Third Party specific User Identities in IMS using STIR/SHAKEN 17

6.3.1 Introduction 17

6.3.2 Solution detail 19

6.3.3 Evaluation 20

7 Conclusions 21

Annex A (informative): Change history 22

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

Editor's Note: The introduction clause content is left for future consideration.

# 1 Scope

The present document studies security impacts of the new features of the next generation real time communication studied in TR 23.700-77[2], specifically, the security aspects that are to be covered in the present document are as follows:

- IMS third party identity security handling

- The security handling of the enhancements to support the use cases of IMS based Metaverse services

- The security and privacy issues and solutions related to the IMS data channel exposure.

Editor’s Note: New objectives may be added to address security aspects of other key issues introduced in SA2 after further progress made in SA2.

# 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 23.700-77: ""Study on system architecture for next generation real time communication services; Phase 2".

[3] 3GPP TR 33.890: "Study on security support for next generation real time communication services".

[4] 3GPP TR 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-26: "PASSporT Extension for Rich Call Data"

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

[7] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2"

[8] 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.

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or abbreviations.

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Assumptions

## 4.1 General

The following clauses include information about the previous security study results documented in TR 33.890 [3] and the related work documented in TR 23.700-77 [2].

## 4.2 Architectural Assumptions and Principles

The following architectural assumptions and principles are considered during the study:

- The third party specific user identity handling work in TR 33.890 [3] and TR 23.700-77 [2] is taken into account if applicable. The existing Ms reference point and procedures as described in TS 24.229 [4] are to be reused.

- The security study of the IMS enhancements to support media handling of avatar calls considers alignment with the study in TR 23.700-77 [2].



Figure 4.2-1: Usage of Ms reference point (see TS 24.229 [4], Annex V.2)

# 5 Key issues

## 5.1 Key issue #1: Third party specific user identities

### 5.1.1 Key issue details

According to TR 23.700-77 [2], there are scenarios that the third party subscribers use third party IDs (e.g., enterprise employee ID). The IMS network can present the third party ID to the callee during subsequent calling process. The third party subscriber can access the IMS network directly or via a SIP trunk as well.

From the security point of view, the enhanced IMS network shall be able to support the identity verification and authorization of third-party user during an IMS call.

### 5.1.2 Threats

A malicious UE can use IDs belonging to others or forged IDs to initiate IMS calls in the IMS network;

A malicious UE can use an ID that no longer belongs to it to initiate IMS calls in the IMS network (e.g., the user use the ID allocated by a particular company even after leaving it).

The ID's transfer between IMS networks may be manipulated by intermediary network entities. Consequently, the callee may receive a wrong ID.

### 5.1.3 Potential security requirements

The IMS system shall be able to coordinate with the third party to verify and authorize the third-party specific user identities.

The IMS network shall be able to support the integrity protection of the third-party specific user identities on the originating side and terminating side.

Editor’s Note: The KI may be updated according to SA2’s progress.

## 5.2 Key issue #2: Security of IMS based Avatar Communication

### 5.2.1 Key issue details

According to TR 23.700-77 [2], there are scenarios that a UE uses an Avatar-ID to initiate an IMS based Avatar Communication. Then the Avatar-ID is used to fetch objects such as an Avatar representation which may include Avatar metadata and Avatar media.

The IMS network can present the Avatar to the callee during the subsequent calling process. The UE can access the IMS network directly or via a SIP trunk as well.

From a security point of view, the enhanced IMS network needs to be able to support the Avatar-ID authentication and authorization during an IMS Avatar call. Also, Avatar objects such as Avatar representations could be used by malicious users to impersonate other users. Therefore, it is essential to ensure that the Avatar objects are secure and cannot be tampered with or accessed by unauthorized entities.

### 5.2.2 Threats

A malicious UE can use Avatar-IDs belonging to other UEs or forged Avatar-IDs to initiate IMS avatar communication in the IMS network and therefore impersonate other UEs.

The potential transfer of the Avatar-IDs between IMS networks can potentially be tampered by intermediary network entities.

The potential transfer of the Avatar metadata between IMS networks can potentially be manipulated by intermediary network entities.

The potential transfer of the Avatar media between IMS networks can potentially be manipulated by intermediary network entities.

Avatar objects could be used for impersonating a IMS caller.

### 5.2.3 Potential security requirements

The 3GPP system shall support means to ensure that stored Avatar objects and Avatar-IDs are accessed only by authenticated and authorized entities, i.e. UEs and IMS network nodes. .

The IMS network shall support the integrity protection of the Avatar-ID on the originating side and terminating side.

The IMS network shall support the integrity protection of the Avatar objects such as the Avatar representation on the originating network and terminating network.

## 5.3 Key Issue #3: Security and privacy aspects of IMS DC capability exposure

### 5.3.1 Key issue details

SA2 has been studied the key issue of Impact on IMS architecture, interfaces, and procedures to support IMS capability exposure in the context of IMS data channel session in TR 23.700-77[1].

During the procedure of IMS capability exposure, without proper security control, the IMS DC services can be maliciously used by malicious application function/server (AF/AS), e.g.:

- First, the malicious AF can eavesdrop or manipulate IMS DCs.

- Event of DC establish, terminate, DC application download, etc., can be exposed to untrusted 3rd party DC AS without aware of the end user.

- The malicious AF can manipulate DC to push unwanted services to the user, e.g. AF manipulates the bootstrap DC to download unwanted applications without awareness of the user/UE.

- Second, the malicious AF can launch DoS attack with updating/terminating an ongoing DC, and cause interruption on the IMS communication of an end user.

- Third, there are potential privacy compromise of the user. i.e.

- Caller/Callee Id of a DC session is disclosed to untrusted 3rd party AF/AS.

- Subscriber's favorite (applications) and habit is disclosed to and inferred by untrusted 3rd party AF/AS.

Editor's Note: Whether exposure events reveal subscriber habits and whether these habits are privacy issue is FFS.

### 5.3.2 Security threats

User private information like Caller/Called ID, DC events, etc. can be disclosed to untrusted 3rd party ASes.

A malicious AF can manipulate an ongoing DC, to interrupt the communication or push unwanted services, which potentially lead to further DoS attacks.

### 5.3.3 Potential security requirements

The 5G system shall support privacy protection during the IMS capability exposure procedures.

The 5G system shall support authentication and authorization of data channel application server during the IMS capability exposure procedures.

NOTE: Existing 3GPP defined authentication, authorization and privacy protection features should be reused as much as possible if applicable.

Editor's Note: Security and privacy threats and solutions depend on SA2 architecture and procedures.

# 6 Solutions

## 6.0 Mapping between key issues and solutions

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |
| --- | --- | --- |
| Solutions | KI#1 | KI#2 |
| Solution #1: Signing and verification of third party ID information | X |  |
| Solution #2: Security of 3rd party specific identities | X |  |
| Solution #3: Support of Third Party specific User Identities in IMS using STIR/SHAKEN | X |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 6.1 Solution #1: Signing/verification of third party ID information

### 6.1.1 Introduction

This solution addresses key issue #1.

### 6.1.2 Solution details

This solution enhances the STIR/SHAKEN framework that has been adopted in 3GPP (see TS 24.229 [4]) to all third party ID information. The third party ID information is related to an IMPU and is either provided to the HSS or IMS-AS (as described below). In the latter case the HSS provides a URI to the IMS AS so the third party ID information can be requested. The IMPU and third party ID information or URI to fetch that information is provisioned in the HSS before the SIP INVITE is sent.

NOTE: The UE is provisioned with multiple IMPU in the case that the UE can use multiple 3rd party IDs.

Editor's Note: Whether the HSS stores third party ID information pointer or actual third party ID information is to be aligned with SA2.

Figures 6.1.2-1 and 6.1.2-2 (given below) show the procedures for the originating and terminating networks respectively.



Figure 6.1.2-1: Originating network procedures for authorising/verifying the third party ID information

1. UE-A sends a SIP INVITE with an IMPU that has been subscribed for the delivery of third party user identity information.

2. The CSCF forwards the SIP INVITE to IMS AS for processing of third party user identity service based on the included IMPU.

3. The IMS AS sends a request to HSS to retrieve the third party ID information.

4. If needed, the HSS fetches the third party ID information.

5. The HSS returns either the third party ID information ID or a URI to fetch the third party information ID to the IMS AS.

6. If the IMS AS received the URI from the HSS, the IMA AS retrieves the third party ID information from the repository linked to the URI.

7-8. IMS AS sends the third party ID information to the Signing Server and receives a Personal Assertion Token (PASSporT) in the response.

9. The IMS AS send the signed third party ID information (including the third party ID information and the PASSporT to the CSCF).

10a. The CSCF forwards the SIP INVITE to the terminating network.



Figure 6.1.2-2: Terminating network procedures for authorising/verifying the third party ID information

10b. The CSCF in the terminating network receive the forwarded the SIP INVITE.

11. The SCSF sends the SIP INVITE to IMS AS based on UE subscription data and network policy.

12-13. The IMS AS in the terminating network sends the third party ID information and associated PASSporT to the Verification Server, then receives the message of verification success in the response.

14. The IMS AS send the SIP INVITE to the CSCF including the verified third party ID information.

15. The CSCF forwards the SIP INVITE (including the verified third party ID information).onto UE-B for rendering and presentation to the user.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Security of 3rd party specific identities

### 6.2.1 Introduction

This solution addresses the Key issue #1 "Third party specific user identities".

As stated in the Key issue #1 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 specific identities (3P ID or Rich Call data/RCD) to the callee during the subsequent calling process. From a 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-26 [6].

### 6.2.2 Solution details

#### 6.2.2.1 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 as shown in Figure 4.2-1. This enables calling number verification using signature verification and attestation information based on the STIR/SHAKEN framework.

This solution proposes that the originating IMS network verifies that the use of 3rd party ID data is allowed and the validity of the incoming 3rd party ID data (e.g. the display name in From header or other header info) of the calling party before adding Rich Call Data (RCD) that is associated with the 3rd party ID data and invoking the signing on behalf of the 3rd Party.

The main user identity information involved in this solution includes:

1) The IMS identity (IMPU) of the calling party (typically fetched from P-Asserted-Identity header). This is used to fetch the RCD from the 3P ID server (details below).

2) The 3rd Party ID data optionally included in the SIP INVITE from the UE (or PBX) to the Originating IMS network. This is a pointer to an RCD record in case more than one RCD record is fetched and it points to the one to be used. If there is only one RCD record expected to be fetched, then nothing is inserted by the UE. The enables flexibility for users with more than one identity, to select the identity, to be presented to the caller.

NOTE 1: When the 3rd party ID data is not included, default Rich Call Data can optionally be added by the originating IMS network based on policy.

3) The Rich Call Data which may be embedded, signed and verified in the SIP INVITE by the originating IMS network.

Examples of Rich Call Data are:

- 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 IETF draft-ietf-stir-passport-rcd-26 [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 4.2-1. The 3rd party (Enterprise) network can be connected to the serving IMS network via UNI (UE to Network Interface) or NNI (Network to Network) interfaces. The serving IMS network handles outbound SIP calls from the Third Party.

There are several options how and where the RCD data of a 3rd party user is 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.

A 3rd party ID Server (3P ID Server) stores the associations between the 3P Caller IMPU, 3rd Party ID data and the corresponding Rich Call Data (RCD) information. The Rich Call Data information is subject to signing in the originating IMS network. The address of the applicable 3rd Party ID Server for the user can be included in HSS.

Prerequisites:

1. The 3rd Party specific user identity data (3P ID data) and the corresponding Rich Call Data information (related to each 3rd party and identified by the 3rd Party specific user identity data) that are subject for signing in the originating IMS network are associated to the corresponding IMS identities in a 3rd party ID server (3P ID Server). The address of the applicable 3P ID Server for the user can be stored in HSS. The ownership, administration and provisioning of the 3P ID Server is out of scope of the present solution.

NOTE 1: In the PBX case, it is assumed that this 3P ID Server 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. Otherwise, the 3P ID Server could be provided by the originating IMS operator which could allow certain access to the calling UE via a UE self-management portal. The access to the enterprise administrator (in the PBX case) or the UE (in the single UE case) self-management portal is assumed to be secured and out of scope of the present solution.

2. The Originating IMS network is assumed to have a secure channel to the 3P ID Server which includes the Rich Call Data information. The setup of this secure channel is out of scope of the present solution.

NOTE 2: When the 3P ID Server is located outside the IMS operator domain, the access to the 3P ID Server 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 [7].

NOTE 3: If the user has multiple 3rd party ID data, the RCD data that matches the provided 3rd  party ID data for the IMS identity will be selected. If no match is found, a default RCD data record or no RCD data for the IMS identity will be selected depending on the operator policy.

Editor's Note: For the solution options below which SIP header includes the RCD is FFS

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

****

Figure 6.2.2.2-1: The 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 Caller IMPU and optionally the 3P ID data to the IBCF

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

3. The originating IMS system 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 system ignores the 3P ID data within the SIP INVITE (if present) and does not execute the rest of 3P ID related steps during the call set-up. The call continues without presenting any RCD to the called endpoint.

If the PBX is authorized to use 3P IDs, the originating IMS system retrieves the Rich Call Data of 3rd party subscriber from the 3P ID Server 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 RCD to the called endpoint.

NOTE 1: If no 3P ID data is received in the SIP INVITE from the PBX, suppression of a 3P ID Server lookup can be optionally applied based on a local policy. If there is a mismatch between the received 3P ID data in the SIP INVITE and data retrieved from the 3P ID Server based on the IMS identity, it is governed by a local policy of the originating IMS system how the population of the Rich Call Data into the SIP Identity header will be done.

4. The originating IMS system 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 4.2-1.

5. The STI-AS signs the SIP identity header according to STIR/SHAKEN framework and draft-ietf-stir-passport-rcd-26[6].

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

7. The originating IMS system routes the call to the egress IBCF. Then the 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 the terminating IMS systems.

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

9. The STI-VS validates the certificate, extracts the public key and verifies the signature in the Identity header field, which validates the Caller ID and Rich Call Data signed in the INVITE message on the originating STI-AS based on Figure 4.2-1.

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 the terminating IMS system which continues to set up the call to the terminating SIP User Agent (UA). If the Caller ID is validated OK but not the Rich Call Data, the call can continue but without showing any name card info to the terminating SIP UA.

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

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

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

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

****

Figure 6.2.2.3-1: The 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 Caller IMPU and optionally the 3P ID data.

2. The originating IMS system 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 system ignores the 3P ID data within the SIP INVITE (if present) and does not execute the rest of 3P ID related steps during the call set-up. The call continues without presenting RCD to the called endpoint.

If the UE is authorized to use 3P IDs, the originating IMS system retrieves the Rich Call Data of the 3rd party subscriber from the 3P ID Server 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 RCD to the called endpoint.

NOTE 1: If no 3P ID data is received in the SIP INVITE from the UE, suppression of a 3P ID Server lookup can be optionally applied based on a local policy. If there is a mismatch between the received 3P ID data in the SIP INVITE and data retrieved from the 3P ID Server based on the IMS identity, it is governed by a local policy of the originating IMS system how the population of the Rich Call Data into the SIP Identity header will be done.

3. The originating IMS system 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 4.2-1.

4. The STI-AS signs the SIP identity header according to STIR/SHAKEN framework and draft-ietf-stir-passport-rcd-26[6].

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

6. The originating IMS system routes the call to the egress IBCF. Then the 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 systems.

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

8. The STI-VS validates the certificate, extracts the public key and verifies the signature in the Identity header field, which validates the Caller ID and Rich Call Data signed in the INVITE message on the originating STI-AS based on Figure 4.2-1.

9. Depending on the result of the STI validation, the STI-VS determines that the call is to be completed with an appropriate indicator and the result is passed back to the terminating IMS system 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 the name card info to the terminating SIP UA.

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

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

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

### 6.2.3 Evaluation

This solution addresses the requirements of KI#1 "Third party specific user identities" and is applicable to both UNI (SIP UA) and NNI (IP PBX) case. The solution reuses the existing STIR/SHAKEN architecture with enhancements that the STI-AS and STI-VS needs to support the signing and verification of the Rich Call Data identity header.

The solution relies on a 3P ID Server which contains the association of the 3P ID data and the corresponding Rich Call Data information with the corresponding IMS identities.

The solution requires no changes on the IP PBX and SIP UA. The solution requires minimal impact on the existing IMS procedures.

## 6.3 Solution #3: Support of Third Party specific User Identities in IMS using STIR/SHAKEN

### 6.3.1 Introduction

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

The Ms reference point as described in TS 24.229 [4], 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 [6] 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 [8]. 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 [8]:

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 6.3.1-1. 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 6.3.1-1: Third Party network connected to the serving IMS network

### 6.3.2 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.

Editor's Note: Whether the HSS stores RCD pointer or actual RCD is to be aligned with SA2.

The procedures to sign and verify PASSporT tokens follow the descriptions in TS 24.229 [4] with the main difference that besides telephone numbers also other information as described in draft-ietf-sipcore-callinfo-rcd-09 [8] and draft-ietf-stir-passport-rcd-26 [6] can be used for signing and verification.

Figure 6.3.2-1: 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. The association between IMPU/IMPI and third party ID/RCD URL is pre-configured in HSS as subscription data.

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.

Editor's Note: Whether the HSS stores RCD pointer or actual RCD is to be aligned with SA2.

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, Optionally. the terminating IMS subsystem may retrieve RCD of the third party identity from third party database if RCD URL pointing to the RCD is received. .

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.

### 6.3.3 Evaluation

TBD

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02-19 | SA3#115 | S3-240761 |  |  |  | TR skeleton | 0.0.0 |
| 2024-03-04 | SA3#115 | S3-240941 |  |  |  | pCRs approved at SA3#115: S3-240761, S3-240942, S3-240943, S3-240944, S3-240945 | 0.1.0 |
| 2024-04-24 | SA3#115Adhoc-e | S3-241637 |  |  |  | Version after incorporating changes in: S3-241520, S3-241528, S3-241529, S3-241531, S3-241605 | 0.2.0 |