|  |
| --- |
| 3GPP TR 33.890 V0.2.0 (2022-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security support for Next Generation Real Time Communication services(Release 18) |
|   |
|  | 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 address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://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.© 2022, 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 members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® 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 6

3.3 Abbreviations 7

4 Assumptions 7

5 Key issues 7

5.1 Key issue #1: Third party specific user identities 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 7

5.X Key issue #X: <Title> 8

5.X.1 Key issue details 8

5.X.2 Threats 8

5.X.3 Potential security requirements 8

6 Proposed solutions 8

6.1 Mapping of solutions to key issues 8

6.A Solution #A: <Title> 8

6.A.1 Introduction 8

6.A.2 Solution details 8

6.A.3 Evaluation 8

7 Conclusions 8

Annex <A>: <Informative annex title for a Technical Report> 9

Annex X: Change history 9

# 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

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The present document studies security aspects for any potential enhancements based on the ongoing study in TR 23.700-87 [2]. For each of the key issues in the scope of the SA WG2 study, the security aspects that are to be covered in this study are as follows:

- Analysing the potential security aspects on how to verify and authorize the 3rd party specific identity information during a call both on originating and terminating sides.

- Analysing potential security impacts from supporting service-based architecture in IMS media control interfaces.

- Analysing potential security aspects to support Data Channel usage in IMS network.

# 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)".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

# 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].

Definition format (Normal)

**<defined term>:** <definition>.

**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 format (EW)

<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 format (EW)

<ABBREVIATION> <Expansion>

# 4 Assumptions

This clause contains assumptions for the study. If there are no assumptions at the end of the study, the clause will be removed before sending for approval.

# 5 Key issues

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

### 5.1.1 Key issue details

According to TR 23.700-87 [2], there are scenarios that the third party subscribers (e.g. employees) 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

Third party specific user identities shall be authorized and verified by the originating IMS network before or during a call.

The originating IMS network 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.

## 5.2 Key issue #2: Security aspects of Data Channel usage in IMS network

### 5.2.1 Key issue details

Existing IMS procedures need to be changed to support Data Channel usage in IMS as is being studied in TR 23.700-87 [2]. It needs to be studied whether usage of Data Channel in IMS brings new security threats and requirements, and if so, it needs to be studied whether existing solutions could be re-used or if new solutions would need to be developed. For example, clause N.3 of TS 33.328 [3] describes media security of the WebRTC data channel, but only e2ae (End-to-access edge) security is specified at the moment. Current security mechanisms in WebRTC data channel needs to be reviewed and possibly reused for data channel in IMS.

### 5.2.2 Security threats

TBD.

### 5.2.3 Potential security requirements

TBD.

## 5.3 Key issue #3: security aspects of SBA in IMS media control plane

### 5.3.1 Key issue details

Service based architecture is introduced in IMS media control plane. Security for service based architecture need to be considered. Current security mechanisms in 5GC SBA needs to be reviewed and possibly resued for service based architecture in IMS. Co-existence of 5G service based and legacy IMS media control interfaces also needs to be considered.

### 5.3.2 Security threats

The attacker can easily obtain or tamper context transferred between IMS nerwork functions when there is no confidentiality and integrity protection between these IMS nodes.

If no authentication has been performed before signalling exchange between IMS NFs, these nodes will potentially suffer spoofing attack from both sides and Man-in-the-Middle attack.

If no authorization has been performed in service based architecture, a requester NF can potentially obtain information and request NF service which are not allowed for it.

### 5.3.3 Potential security requirements

Service based interfaces in IMS media control plane should support mutual authentication, confidentiality and integrity protection.

NF service access shall be authorized in service based architecture.

## 5.X Key issue #X: <Title>

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Proposed solutions

## 6.0 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
| Solution #1: How the Originating IMS network signs the 3rd party IDs and terminating IMS network verifies the 3rd party IDs | X |  |  |
| Solution #2: SHAKEN based third-party specific user identities | X |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 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.X.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 were securely provided from the 3rd Party to the originating IMS network and were associated to the corresponding IMS identities. How this is done is out of scope of the present solution.

2. Originating IMS network is assumed to have a secure channel to a Database which includes rich call data info. How this secure channel is set-up is out of scope of the present solution. The data base can also be co-located with HSS.

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 containing 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. Based on the 3P ID the originating IMS subsystem gets Rich Call Data of 3rd party susbscriber from the Database and also checks UE’s subscription information whether the 3P ID matches with an IMS identity allocated for the calling PBX.

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.X.2.1-2: 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 sends SIP INVITE with 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 INVITE 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 with 3P ID.

2. Based on the 3P ID the originating IMS subsystem gets Rich Call Data of 3rd party subscriber from the Database and also checks the UE’s subscription information whether the 3P ID matches with an IMS identity allocated for the calling SIP UA.

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.X.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 sends SIP INVITE with 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 INVITE 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

## 6.2 Solution #2: SHAKEN based third-party specific user identities

### 6.2.1 Introduction

This solution addresses key issue #1.

### 6.2.2 Solution details

#### 6.2.2.1 General procedures

Following preconditions are fulfilled before a third party specific user identity can be used:

- For the originating UE, subscription data for the usage of third party specific user identity is configured in the HSS.

- For the terminating UE, subscription data for the verification of third party specific user identity is configured in the HSS.

- Third party Authorization server is authorized by the serving IMS network to provide third party specific user identity for specific group of UEs.

- The originating UE is authorized by third party Authorization Server to use designated third party specific user identity by one of the two following methods:

 - Option A: The third party leverages the subscriber management capability exposed by HSS via NEF to allocate a designated Public User Identity and associated Service Profile for the UE.

 - Option B: The third party assigned a token to the UE for the authorization of third party specific ID via application layer. How the third party Authorization Server distributes the token to the UEs is out of the scope of this study report.

Editor's Note: the content of the token is ffs.

Figure 6.2.2-1: Call flow for using third party identity

The enhancement to SHAKEN reference call flow specified in clause 4.3 of ATIS-1000074 [5] are as following:

0a. (For option A) The third party Authorization Server is authorized by NEF to request allocation of designated IMPU and associated Service Profile for the UE to HSS. The allocated IMPU is received and configured in the UE in IMS registration procedure.

0b. (For option B) Third party Authorization server is authorized by the serving IMS network to provide third party specific user identity. The UE interacts with the third party via application layer to receive a token for the authorization of third party specific ID.

1. The originating UE creates a SIP INVITE with:

 - the Public User Identity allocated by third party (for option A); or

 - an Authorization Header which contains the third party specific user identity, realm of the third party Authorization Server and the token assigned by the third party Authorization Server (for option B).

NOTE 1: How the UE interacts with the third party Authorization Server via application layer to get the third party specific user identity or token is out of scope of this study.

2. originating IMS network (e.g. S-CSCF) checks the UE subscription data to confirm that the UE is allowed to use a third party specific user ID. The S-CSCF resolves the address of the third party Authorization Server based on the Public User Identity (option A) or realm information in the authorization request (option B). The authorization request is forwarded to the NEF. The NEF discovers and selects the third party Authorization Server for the authorization of using third party specific user identity.

Editor's Note: Whether timestamp is needed and if so whether it is included in the token and how to verify is ffs

3. The third party Authorization Server authorizes the request and creates an enterprise name card for the user, which is going to be delivered in the SIP header. For option B, the authorization can be done using the token received in the INVITE as mentioned above or as described in clause 6.2.2.2.

If the authorization request is rejected, the IMS call can continue without presentation of third party specific user identity.

Editor's Note: Whether the IMS call can continue if the authorization request is rejected is FFS

 NOTE 2: The key information of enterprise name card and integrity protection mechanism are specified in draft-ietf-sipcore-callinfo-rcd-03 [7] and draft-ietf-stir-passport-rcd-18 [6].

4-5. The Signing Server signs the SIP INVITE and adds Identity header field(s) per IETF RFC 8224 [8] using the third party specific user ID in the P-Asserted-Identity header field and enterprise name card information. The signing can reuse Ms reference point as described in TS 24.229 [4].

6 SIP INVITE with signature is sent to the terminating IMS networks.

7-8. Upon receiving the SIP INVITE with third party specific user identity, the terminating IMS checks whether the terminating UE has subscribed for verification of third party identity. If allowed, the terminating IMS triggers the verification procedure with the Verification Server.

9. The third party specific user identity and enterprise name card is received and rendered in the terminating UE.

#### 6.2.2.2 Alternative authorisation procedure

This clause provides an alternative authorisation method for option B at step 3 in clause 6.2.2.1.

Rather than using the token to authorise the UE, the authorization sever can also initiate authentication with UE on receiving the request from IMS. After successful authentication, the authorization sever can create an enterprise name card for the user. The authentication between UE and the authorization server is out of scope of this study.

Editor's Note: It’s ffs whether authentication between UE and authorization server is needed and whether SIP can support the authentication exchanges.

Editor's Note: If no authentication is performed between UE and authorization server, how to prevent malicious UE from using token belonging to others is ffs.

### 6.2.3 Evaluation

This is FFS.

## 6.A Solution #A: <Title>

### 6.A.1 Introduction

### 6.A.2 Solution details

### 6.A.3 Evaluation

# 7 Conclusions

Annex <A>:
<Informative annex title for a Technical Report>

Annex X:
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107Adhoc-e | S3-221482 |  |  |  | Skeleton | 0.0.0 |
| 2022-07 | SA3#107Adhoc-e | S3-221686 |  |  |  | S3-221483, S3-221682 | 0.1.0 |
| 2022-08 | SA3#108-e | S3-222340 |  |  |  | S3-221953, S3-222338, S3-222401, S3-222320 | 0.2.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |