|  |
| --- |
| 3GPP TR 33.890 V0.6.0 (2023-2) |
| 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)".

[9] IETF RFC 8831: “WebRTC Data Channels”

[10] 3GPP TS 23.334: “IP Multimedia Subsystem (IMS) Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures descriptions”

[11] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[12] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2”

[13] IETF RFC 8827: “WebRTC Security Architecture”

[14] 3GPP TS 32.274: "Telecommunication management; Charging management; Short Message Service (SMS) charging"

[15] GSMA NG.129: "IMS Data Channel White Paper"

…

[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].

DC Data Channel

DCMF Media Function of Data Channel Server

DCMTSI Data Channel Multimedia Telephony Service for IMS

DCSF Control Function of Data Channel Server

P2A Person to Application

P2P Person to Person

# 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.

One of the security issues of Data Channel is as follows. 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. It means that an SCTP over DTLS connection is established between the DCMTSI client and the IMS-AGW (see section 5.20.2 of 3GPP TS 23.334 [10]). The text is void of any references to e2e security mode for the IMS data channels. However, GSMA has pointed in their LS to a use case where Data Channel Server (DCS) can be deployed in an external data server outside the operator’s administrative domain. Such server may have or may not have WebRTC data channel protocol support. According to IETF RFC 8831 [9] (clause 6.2), SCTP over DTLS connection needs to be established between two endpoints supporting WebRTC data channel protocol (i.e., the DCMTSI client and the external data server). Current security mechanisms in WebRTC data channel needs to be reviewed and possibly reused for data channel in IMS.

### 5.2.2 Security threats

The lack of security over the IMS data channel can open up for attackers to eavesdrop or tamper with the data transferred over the data channel.

The lack of authentication between UE and peers (i.e., another UE and data channel server) before media exchange can open up for spoofing attack from both sides and Man-in-the-Middle attacks as well.

If only the Mb interface i.e., DCMTSI client to IMS-AGW part of the data channel path is protected, IMS-AGW to external data server path will stay unprotected and exposed to attacks like eavesdropping, modification and replay.

### 5.2.3 Potential security requirements

Communication over IMS data channel shall be confidentiality, integrity and replay protected.

The peers over IMS data channel shall be mutually authenticated.

The path between IMS-AGW and external data server shall be confidentiality, integrity and replay protected.

## 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.

# 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 |  |  |
| Solution #3: Service based interface protection in media control plane |  |  | X |
| Solution #4: End-to-access-edge security for IMS data channels |  | X |  |
| Solution #5: How to avoid e2ae limitation and achieve e2e security for IMS Data Channel |  | 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 6.1.2.1-1 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 and the corresponding rich call data information related to each 3rd Party specific user identity that are subject for signing in the originating IMS network are associated to the corresponding IMS identities in a Database. The address of the applicable Database for the user can be stored in HSS. 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. Otherwise, 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 enterprise administrator (in the PBX case) or the UE (in the single UE case) 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 [12].

NOTE 3: If the user has multiple 3rd party IDs, the RCD data that matches the provided 3rd  party ID 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.

#### 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 susbscriber 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.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 returns the signed SIP identity header back to IMS subsystem.

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].

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

This solution addresses the requirements of KI#1 and is applicable to both UNI (SIP UA) and NNI (IP PBX) case. The solution reuses 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 Database which contains the association of the 3rd Party specific user identities 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.

## 6.2 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 and the content of the token are out of the scope of this study report.

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.

In the PBX case, it is assumed that the PBX will authenticate the UE and create the SIP INVITE on behalf of UE which is out of scope of this solution.

For legacy UEs and PBX, option A should be used since the legacy UE can only use IMPU.

1. The originating UE or the PBX 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 or the PBX 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 or the PBX 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.

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 and optionally with a failed code, i.e., verstat tel URI parameter as described in TS 24.229 [4].

 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 may initiate an authentication procedure with UE based on local policy upon 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.

### 6.2.3 Evaluation

This solution meets the requirements of KI#1. 3rd party on its own performs the user verification and name cards delivery, therefore, the solution can be applied in case that the users of the 3rd party change dynamically (e.g., employees leaving or joining an enterprise).

## 6.3 Solution #3: Service based interface protection in media control plane

### 6.3.1 Introduction

This solution propose to reuse the security mechanisms defined for 5GC to protect the service based interface in IMS media control plane.

### 6.3.2 Solution details

#### 6.3.2.1 Protection at the network or transport layer

All service based network functions in IMS media control plane shall support protection in network or transport layer as specified in clause 13.1.0 of TS 33.501 [11].

#### 6.3.2.2 Authentication and authorization

All service based network functions in IMS media control plane and NRF shall support either static authorization as specified in clause 13.3.0, clause 13.3.1 and clause 13.3.2.1 of TS 33.501 [11] or OAuth 2.0 based authorization as specified in clause 13.4.1.1 TS 33.501 [11].

NOTE: It is assumed that slice related aspects or indirect communication using SCP are not applicable in IMS.

### 6.3.3 Evaluation

The solution meets the security requirements of KI#3.

## 6.4 Solution #4: End-to-access-edge security for IMS data channels

### 6.4.1 Introduction

This solution addresses key issue #2.

### 6.4.2 Solution details

There are two types of data channels according to TR 23.700-87 [2], i.e., bootstrap data channel which is used to transfer data channel application list and data channel applications between the UE and the network and application data channel which is used to transfer data of data channel applications between the UEs or between the UE and the network.

For application data channel, it can be further classified into 4 types: P2A without the involvement of DCSF, P2A with DCSF, P2P without DCMF/enhanced MRF, and P2P with DCMF/enhanced MRF.

In bootstrap data channel case (bootstrap data channel between UE and DCMF/enhanced MRF as showed in the figure 6.4.2.1-1), two P2A cases of application data channel (application data channel between UE and DC application server as showed in the figure 6.4.2.1-1) and P2P with DCMF/enhanced MRF case of application data channel (application data channel between UE and UE in remote IMS as showed in the figure 6.4.2.1-1), the DCMF/enhanced MRF is proposed to terminate DTLS protecting with UE.

In the P2P without DCMF/enhanced MRF case, the eIMS-AGW is responsible for terminate DTLS protecting with UE.

The protection between DCMF/enhanced MRF and DCSF can be TLS or DTLS which depends on the underlying protocols, i.e., UDP or TCP.



Figure 6.4.2.1-1: IMS supporting DC usage with DCMF (see TS 23.700-87 [2], clause 6.20.1.2)

NOTE: The protocols between DCMF/DCSF and DC application server are out of scope of this study.

The DTLS between UE and the IMS is established based on the certificate fingerprints exchanged over SDP. To ensure the integrity of the certificate fingerprint the signalling path is assumed to be protected. In case the DTLS is between UE and DCMF/enhanced MRF, the eP-CSCF should include the certificate fingerprint of the DCMF/enhanced MRF in the SDP answer to UE. In case the DTLS is between UE and eIMS-AGW, the eP-CSCF should include the certificate fingerprint of the eIMS-AGW in the SDP answer to UE. In both cases, the UE should include its certificate fingerprint in the SDP offer to eP-CSCF.

### 6.4.3 Evaluation

The solution meets the security requirements of KI#2 when the external DC Application Server only supports the HTTP protocol and e2e security between UE and application server is not addressed in this solution.

## 6.5 Solution #5: How to avoid e2ae limitation and achieve e2e security for IMS Data Channel

### 6.5.1 Introduction

This solution addresses the key issue #2 (Security aspects of Data Channel usage in IMS network). As stated in the key issue details, 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 now. It means that an SCTP over DTLS connection is established between the DCMTSI client and the IMS-AGW (see section 5.20.2 of 3GPP TS 23.334 [10]). The text is void of any references to e2e security mode for the IMS data channels. However, there exist use cases in TS 23.700-87 [2] (Solutions #3, #6, #9, #16, and #20) where Data Channel Server (DCS) or related data channel application functionality can be deployed in an external data server outside the operator’s administrative domain. According to IETF RFC 8831 [9] (clause 6.2), SCTP over DTLS connection needs to be established between two endpoints supporting WebRTC data channel protocol (e.g., the DCMTSI client and the external data channel server or data channel application server).

This solution proposes to allow the DTLS connection from the data channel endpoints to pass transparently through the IMS network by allowing e2e security mode for IMS (and thus WebRTC) data channel media if the external Data Server supports both HTTP and IETF RFC 8831 WebRTC data channel protocols. In the model when the external Data Server supports only HTTP protocol and responds to DCMTSI service requests for the data channel content, end-to-access edge (e2ae) encryption is used, therefore all data channel traffic is anchored in IMS network and is transported unencrypted from IMS-AGW towards the external entities.

### 6.5.2 Solution details

#### 6.5.2.1 Solution Description

The MDC2 reference point as described in TS 23.700-87 [2] Solution#20(and similar reference points in other solutions in that document) is used for transport of data channel media between DC Media Function (either DCMF or enhanced MRF) and DC Application Server, see Figure 6.5.2.1-1 as one example of such solution. If the external DC application server supports both HTTP and IETF RFC 8831 WebRTC data channel protocols, the server responds to UE(DCMTSI client)service requests for the data channel content and the content driving the interaction with the server is delivered over the data channel. In order to establish the WebRTC data channel between the UE and the DC Application Server a signaling channel is required e.g. to exchange fingerprints binding the certificates. The end-to-end (e2e) encryption for the data channel should be used as specified in IETF RFC 8831 [9] and IETF RFC 8827 [13].



Figure 6.5.2.1-1: Use of IMS-external data channel media (see TS 23.700-87 [2], clause 6.20.1)

There are two types of Data Channels: Bootstrap Data Channel and Application Data Channel. According to GSMA NG.129 [15], the application Data Channel supports the P2P, P2A and A2P use cases. The data channel related P2P/P2A/A2P definitions follow from 3GPP TS 32.274 [14] and are applied accordingly to this document with the following meaning:

1. Person-to-Person (P2P): The session is originated by a UE and terminated on another UE.

2. Person-to-Application (P2A): The session is originated by a UE and terminated on a third-party application.

3. Application-to-Person (A2P): The session is originated by a third-party application and terminates on a UE.For the P2P use case, DC media resources are not required. So, the application data channel can either involve DCMF (enhanced MRF) or not.

For the P2A/A2P use cases, DC media resources are required. So, the application data channel should involve DCMF (enhanced MRF).

The IMS Data Channel user plane (not depicted in Figure 6.5.2.1-1) from UE (DCMTSI client in terminal) to the IMS-AGW is secured with DTLS regardless of e2ae or e2e security being used. The DC Application server can be deployed outside the operator’s administrative domain and provides service logic and/or media content for the data channel application.

If the DC Application server supports only the HTTP protocol, the data channel is established between the DCMTSI and the IMS. An SCTP connection over DTLS over UDP is established between the DCMTSI client (UE) and the IMS-AGW which is applied to P2P use case without DC media resources. An SCTP connection over DTLS over UDP is established between the DCMTSI client (UE) and DCMF (enhanced MRF) which is applied to the A2P/P2A use cases, the P2P use case with DC media resources and the bootstrap data channel. The data channel transport layer is terminated at IMS-AGW or DCMF (enhanced MRF) and e2ae security is achieved.

If the DC Application server supports both HTTP and IETF RFC 8831 [9] WebRTC data channel protocols, the application data channel is established between the DCMTSI client (UE) and the External DC Application Server. An SCTP connection over DTLS over UDP is established directly between the DCMTSI client (UE) and the external DC Application server, which is applied to the A2P and P2A use cases. In order to establish the WebRTC data channel, a signaling channel is required e.g., to exchange fingerprints binding the certificates.

IMS-AGW does not terminate DTLS and thus only anchors IP and UDP protocol layers towards DCMF/enhanced MRF, and DCMF/enhanced MRF is also transparent to DTLS traffic between Mb and MDC2 reference points, e2e security is achieved between the UE and the DC Application Server, without security risks even if the DC Application Server is placed outside of the operator’s domain.

### 6.5.3 Evaluation

The solution addresses the KI#2 Security aspects of Data Channel usage in IMS network for the two cases: when the external DC Application Server supports only HTTP protocol and when the external DC Application Server supports both HTTP protocol and WebRTC Data Channel protocols. The following changes are suggested:

* TS 33.328 [3] needs to be enhanced to allow e2e security for IMS (and WebRTC) Data Channel media and should (recommend or) mandate using e2e security whenever IMS Data Channel media is used towards an entity deployed outside the operator’s administrative domain.
* TS 23.334 [10] needs to be enhanced to describe use of e2e security for IMS (and WebRTC) Data Channel media.
* TS 24.229 [4] needs to be enhanced to describe use of e2e security for IMS (and WebRTC) Data Channel media.

# 7 Conclusions

## 7.1 Conclusion on Key Issue #3

For key issue#3, it is recommended to use solution #3 to protect the service based interfaces in IMS media control plane and the service access authorization

## 7.2 Conclusion on Key Issue #2

The following conclusions are agreed for KI#2:

A) The DCMF/enhanced MRF will terminate DTLS for the following cases:

1) Bootstrap data channel;

2) P2A/A2P application data channel if the external Data Server supports only HTTP;

3) P2P application data channel with the involvement of DCMF/enhanced MRF;

C) If the external Data Server supports both HTTP and IETF RFC 8831 WebRTC data channel protocols, the end-to-end (e2e) encryption for the data channel should be supported as specified in IETF RFC 8831 [9] and IETF RFC 8827 [13] for the P2A/A2P Application data channel use cases.

Editor’s Note: Conclusion on further P2P cases are FFS.

NOTE: LI considerations are FFS.

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 |
| 2022-08 | SA3#108 Adhoc-e | S3-222958 |  |  |  | S3-222932, S3-222955, S3-222956, S3-222957 | 0.3.0 |
| 2022-11 | SA3#109 | S3-224179 |  |  |  | S3-224157, S3-224158, S3-224142, S3-224143, S3-224124 | 0.4.0 |
| 2023-01 | SA3#109 Adhoc-e | S3-230570 |  |  |  | S3-230092, S3-230094, S3-230569, S3-230413, S3-230568 | 0.5.0 |
| 2023-02 | SA3#110 | S3-231558 |  |  |  | S3-231293, S3-231536 | 0.6.0 |