|  |  |
| --- | --- |
| 3GPP TR 33.790 V1.2.0 (2025-02) | |
| 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.  © 2025, 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 7

1 Scope 9

2 References 9

3 Definitions of terms, symbols and abbreviations 10

3.1 Terms 10

3.2 Symbols 10

3.3 Abbreviations 10

4 Assumptions 11

4.1 General 11

4.2 Architectural Assumptions and Principles 11

5 Key issues 11

5.1 Key issue #1: Third party specific user identities 11

5.1.1 Key issue details 11

5.1.2 Threats 11

5.1.3 Potential security requirements 12

5.2 Key issue #2: Security of IMS based Avatar Communication 12

5.2.1 Key issue details 12

5.2.2 Threats 12

5.2.3 Potential security requirements 12

5.3 Key Issue #3: Security and privacy aspects of IMS DC capability exposure 13

5.3.1 Key issue details 13

5.3.2 Security threats 13

5.3.3 Potential security requirements 13

6 Solutions 14

6.0 Mapping between key issues and solutions 14

6.1 Solution #1: Signing/verification of third party ID information 14

6.1.1 Introduction 14

6.1.2 Solution details 14

6.1.3 Evaluation 16

6.2 Solution #2: Security of 3rd party specific identities 16

6.2.1 Introduction 16

6.2.2 Solution details 16

6.2.2.1 Solution Description 16

6.2.2.2 How the Originating IMS network invokes the signing on behalf of 3rd party (SIP trunk) 18

6.2.2.3 How the Originating IMS network invokes the signing on behalf of 3rd party (Single SIP registration) 19

6.2.3 Evaluation 21

6.3 Solution #3: Support of Third Party specific User Identities in IMS using STIR/SHAKEN 21

6.3.1 Introduction 21

6.3.2 Solution detail 23

6.3.3 Evaluation 25

6.4 Solution #4: SHAKEN based third-party specific user identities 25

6.4.1 Introduction 25

6.4.2 Solution details 25

6.4.2.1 General procedures 25

6.4.2.2 Alternative authorisation procedure 27

6.4.3 Evaluation 27

6.5 Solution #5: Securing the IMS based avatar communication 27

6.5.1 Introduction 27

6.5.2 Solution details 27

6.5.2.1 Network centric procedure 27

6.5.2.2 Sending UE centric procedure 29

6.5.2.3 Receiving UE centric procedure 30

6.5.3 Evaluation 31

6.6 Solution #6: Solution for secure IMS based avatar communication 31

6.6.1 Introduction 31

6.6.2 Solution details 32

6.6.2.1 Network centric IMS avatar call flow 32

6.6.2.2 Sending UE centric IMS avatar call flow 32

6.6.2.3 Receiving UE centric IMS avatar call flow 33

6.6.2.4 UE1 attestation 35

6.6.3 Evaluation 35

6.7 Solution #7: Protect IMS DC based Avatar Communication 35

6.7.1 Introduction 35

6.7.2 Solution details 36

6.7.2.1 Procedure to protect IMS DC based Avatar Communication (Network based Rendering) 36

6.7.2.2 Procedure to protect IMS DC based Avatar Communication (UE-A based Rendering) 39

6.7.2.3 Procedure to protect IMS DC based Avatar Communication (UE-B based Rendering) 40

6.7.3 Evaluation 40

6.8 Solution #8: Security for IMS based Avatar Communication 41

6.8.1 Introduction 41

6.8.2 Solution details 41

6.8.3 Evaluation 45

6.9 Solution #9: Secure IMS DC capability exposure 45

6.9.1 Introduction 45

6.9.2 Solution details 45

6.9.2.1 Procedure of DC AS authorization for DC event subscription 45

6.9.2.2 Procedure of DC AS authorization for data channel session control 46

6.9.3 Evaluation 47

6.10 Solution #10: User aware IMS DC capability exposure 48

6.10.1 Introduction 48

6.10.2 Solution details 48

6.10.3 Evaluation 48

6.11 Solution #11: IMS (DC) capability exposure security based on existing specification 48

6.11.1 Introduction 48

6.11.2 Solution details 48

6.11.2.1 General 48

6.11.2.2 IMS event exposure security 48

6.11.2.3 IMS DC session control exposure security 50

6.11.3 Evaluation 51

6.12 Solution #12: Solution for secure IMS based avatar communication using STIR/SHAKEN 52

6.12.1 Introduction 52

6.12.2 Solution details 52

6.12.2.1 Network centric IMS avatar call flow 52

6.12.2.2 Sending UE centric IMS avatar call flow 53

6.12.2.3 Receiving UE centric IMS avatar call flow 54

6.12.3 Evaluation 55

6.13 Solution #13: IMS avatar communication security based on existing specification 56

6.13.1 Introduction 56

6.13.2 Solution details 56

6.13.2.1 General 56

6.13.2.1.1 Security for the Sending UE centric procedure 56

6.13.2.1.2 Security for the Receiving UE centric procedure 57

6.13.2.1.3 Security for the Network centric procedure 59

6.13.3 Evaluation 59

7 Conclusions 60

7.1 Conclusions for Key issue #1: Third party specific user identities 60

7.2 Conclusions for Key Issue #2: Security of IMS based Avatar Communication 60

7.3 Conclusions for Key Issue #3: Security and privacy aspects of IMS DC capability exposure 61

Annex A (informative): Change history 62

# 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.

# 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.

# 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"

[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".

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

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

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

[12] IETF RFC 7515: "JSON Web Signature (JWS)"

[13] 3GPP TS 33.122: " Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs "

[14] 3GPP TS 23.501: "Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2"

[15] 3GPP TS 33.203: "3G security; Access security for IP-based services"

[16] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[17] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security"

# 3 Definitions of terms, symbols and 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].

**Avatar ID:** The identifier of an Avatar object.

## 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].

ADC Application Data Channel

A2P Application to Peer

BAR Base Avatar Repository

BDC Bootstrap Data Channel

CA Certification Authority

CCA Client Credential Assertion

CCF CAPIF Core Function

(P/S-)CSCF (Proxy/Serving-)Call Session Control Function

DC Data Channel

DC AS Data Channel Application Server

IBCF Interconnect Border Control Function

IMPU IMS Public Identity

IMS AS IMS Application Server

MF Media Function

MMTel AS Multimedia Telephony Application Server

NNI Network to Network Interface

P2A Peer to Application

P2P2A Peer to Peer to Application

P2P Peer to Peer

PASSPorT Personal Assertion Token

PBX Private Branch Exchange

RCD Rich Call Data

RTP Real-Time Transport Protocol

SIP Session Initiation Protocol

(O/T-)STI-AS (Originating/Terminating-) Secure Telephone Identity Authentication Service

(O/T-)STI-VS (Originating/Terminating-)Secure Telephone Identity Verification Service

STIR/SHAKEN Secure Telephone Identity Revisited/ Signature-based Handling of Asserted information using toKENs

UA User Agent

UNI UE to Network Interface

XR AS Augmented/Virtual Reality Application Server

# 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 is potentially manipulated by intermediary network entities. Consequently, the callee potentially receives 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.

## 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 potentially includes 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.

NOTE: Whether exposure events reveal subscriber habits and whether these habits are privacy issue is not addressed in the present document.

### 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.

# 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 | KI#3 |
| 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 |  |  |
| Solution #4: SHAKEN based third-party specific user identities | X |  |  |
| Solution #5: Securing the IMS based avatar communication |  | X |  |
| Solution #6: Solution for secure IMS based avatar communication |  | X |  |
| Solution #7: Protect IMS DC based Avatar Communication |  | X |  |
| Solution #8: Security for IMS based Avatar Communication |  | X |  |
| Solution #9: Secure IMS DC capability exposure |  |  | X |
| Solution #10: User aware IMS DC capability exposure |  |  | X |
| Solution #11: IMS (DC) capability exposure security based on existing specification |  |  | X |
| Solution #12: Solution for secure IMS based avatar communication using STIR/SHAKEN |  | X |  |
| Solution #13: IMS avatar communication security based on existing specification |  | 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.

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

No evaluation is addressed in the present document.

## 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 optionally are 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.

According to ATIS-1000094[5] RCD can be included in the PASSporT of a SIP Identity header.

#### 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. Alternatively, HSS optionally stores RCD server address. Storing just URL(s) or RCD server address 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 also optionally stores 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. Based on operator policies, the source IMS AS optionally uses 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 Rich Call Data information or URL is used by the Signing AS for signing the RCD PASSporT and by the Verification AS to verify the signed RCD PASSporT.

Based on operator policies, the terminate IMS AS will invoke verification of the RCD information or RCD URL included in the incoming SIP INVITE request with a verification AS, and forward the RCD information or RCD URL to the terminating UE.

The terminating UE optionally retrieves third party user identity information from the third party server based on the received RCD URL or RCD information.

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

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) server address, or RCD URL, or RCD information of the third party identity from HSS. HSS optionally returns RCD server address, 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. The CA root certificate used to sign the certificate(s) of https of the RCD URL/URIs is optionally included in the response.

NOTE: If HSS returns concrete RCD to the IMS AS in this step, it is a recommendation that HSS fetches the RCD from the third party database in advance based on RCD URL/third party identity associated to the IMPU/IMPI.

4b. Optionally, the IMS AS/CSCF retrieves RCD information of the third party identity from third party database based on RCD server address and 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 information 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 through CSCF which including signed RCD URL or RCD information of the third party identity, and optional the CA root certificate received in step 4.

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

9. If verification is successful, the terminating IMS subsystem sends SIP INVITE to terminating UE which including the RCD URL or RCD information if verification is successful in step 8, the CA root certificate used to sign the certificate(s) of https of the RCD URL/URIs is optionally included in the message. Otherwise, terminating IMS subsystem optionally sends SIP INVITE to terminating UE without including RCD.

10. Optionally, the UE-B fetches RCD information from third party databased based on the RCD URLs/URIs received in step 9 after verifying the https of the URLs/URIs with the root certificate received in step 9.

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

### 6.3.3 Evaluation

The solution addresses requirements of Key issue #1 which leverages STIR/SHAKEN framework, RCD and PASSporT defined in IETF to verify and authorize the third-party specific user identities, and support integrity protection of the third-party specific user identities on the originating side and terminating side. The solution also supports the terminating UE to securely retrieve RCD information from the third party database.

IMS-AS, HSS and UE need to be enhanced to support RCD, PASSporT and protection of the RCD on the originating side and terminating side.

## 6.4 Solution #4: SHAKEN based third-party specific user identities

### 6.4.1 Introduction

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

### 6.4.2 Solution details

#### 6.4.2.1 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 6.4.2-1: Call flow for using third party identity

The enhancement to SHAKEN reference call flow specified in clause 4.3 of ATIS-1000074 [5] is 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, it is a recommendation that option A is 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).

3. The third party Authorization Server authorizes the request and provides 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 6.4.2.2.

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 [9] and draft-ietf-stir-passport-rcd-26 [6].

4-5. The Signing Server signs the SIP INVITE and adds Identity header field(s) per IETF RFC 8224 [10] 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.

#### 6.4.2.2 Alternative authorisation procedure

This clause provides an alternative authorisation method for option B at step 3 in clause 6.4.2.1.

Rather than using the token to authorise the UE, the authorization server optionally initiates 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.

### 6.4.3 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).

## 6.5 Solution #5: Securing the IMS based avatar communication

### 6.5.1 Introduction

This solution addresses KI#2 Security of IMS based Avatar Communication.

In TR 23.700-77 [2], conclusion is reached to support the network-based avatar communication by media capability invocation. Specifically, the avatar representations are stored in the Base Avatar Repository (BAR), and the UE sends the Avatar ID to the Data Channel Application Server (DC AS). The MF or DC AS downloads the avatar representation from the Base Avatar Repository (BAR) based on the Avatar ID.

* The Data Channel Application Server is responsible for service control related to avatar communication, including avatar representation management, access control, avatar communication session media control, and so on.
* The Base Avatar Repository is used to store and retrieve the avatar representations. BAR can be inside the PLMN, e.g. a new network function, or outside the PLMN, e.g. a webserver of the 3rd party provider [7].

This solution proposes security procedures to verify Avatar ID, and authorize the UE/IMS entity (i.e., MF or DC AS) that accesses the avatar representations, preventing the unauthorized UE/IMS entities from accessing the avatar representations and thus impersonating the IMS caller/callee.

The avatar communication can be unidirectional or bidirectional. In this solution, only unidirectional avatar communication is described. When bidirectional avatar communication is used, UE2 also performs the operation same as UE1 described in the procedure.

### 6.5.2 Solution details

To prevent the UE from providing the Avatar ID belonging to other UEs, the solution proposes to verify whether the Avatar ID provided by the UE is in the UE's Avatar ID list.

To prevent the MF from downloading the wrong avatar representation based on other UE's Avatar ID, the solution requires the MF to download the avatar representation based on the token received from the UE.

Both network centric mode and UE centric mode are supported.

#### 6.5.2.1 Network centric procedure



Figure 6.5.2.1-1: Network Centric Authorization procedure for Avatar communication

Step 0a. Bootstrap data channel (BDC) is established. Through BDC, UE1 receives the Avatar ID list.

NOTE 1: Bootstrap data channel is a data channel established within an IMS session between the UE and the network, to transfer a graphical user interface that can include a list of data channel applications, as described in TS 23.228 [7].

Step 0b. Application data channel (ADC) is established.

NOTE 2: Application data channel is a data channel within an IMS session used to transfer data of data channel applications between UEs or between the UE and the network, as described in TS 23.228 [7].

NOTE 3: The avatar ID list can also be pre-configured in the UE locally.

Step 1. UE1 chooses Avatar ID from the Avatar ID list and generates the token. The token claim includes Avatar ID, issuer (UE1 ID, i.e., IMPU of the UE1), subject (MF type), audience (BAR type) and expiration time. The UE1 generates the token based on UE1’s private key that corresponds to the UE1's certificate. The generation of the signature in the token can be referred to clause 5 of IETF RFC 7515 [12].

Step 2. UE1 sends the Avatar ID and token to DC AS during Avatar animation negotiation procedure.

Step 3. DC AS determines whether the received Avatar ID is in the UE1's Avatar ID list. If the received Avatar ID is equal to one of the Avatar ID in the UE1's Avatar ID list, Steps 4 and 5 are executed. Otherwise, DC AS will send an error message to the UE1. If DC AS does not have the UE1's Avatar ID list, it retrieves the UE1's Avatar ID list from the BAR. DC AS also optionally checks whether the token is valid .

Steps 4, 5. DC AS sends the Avatar ID and token to the MF/MRF via the IMS AS.

Step 6. MF requests to download the avatar representation from the BAR, including parameters of token and Avatar ID.

Step 7. BAR verifies the token provided by the MF. Specifically, BAR verifies the signature in the token based on the public key in the UE1's certificate. BAR checks whether the audience matches its own type, the subject is the MF type, the token is not expired. BAR also checks whether Avatar ID in the request equals to that in the token. How the BAR can obtain the UE1's certificate can be left to implementation. For example, the UE1's certificate can be issued by the operator's CA, and the BAR can obtain the UE1's certificate from the operator's CA.

Step 8. BAR sends the avatar representation downloading response message to the MF. If the verification in Step 7 is passed, the message includes the avatar representation, otherwise the message includes the error code, indicating that the token verification or the verification of the certificate fails.

Step 9. The subsequent procedure continues.

NOTE 4: Alignment with TR 23700-77 conclusion is not addressed in the present document.

#### 6.5.2.2 Sending UE centric procedure



Figure 6.5.2.2-1: Sending UE Centric Authorization procedure for Avatar communication

Steps 0-1. Same as Steps 0-1 in Clause 6.5.2.1. The only difference is that subject is UE1 ID.

Step 2. UE1 sends the Avatar Representation downloading request to MF through ADC, including parameters of token and Avatar ID.

Step 3. MF sends the Avatar Representation downloading request to DC AS, including parameters of token and Avatar ID.

Step 4. DC AS determines whether the received Avatar ID is in the UE1's Avatar ID list. If the received Avatar ID is equal to one of the Avatar ID in the UE1's Avatar ID list, Step 5 is executed. Otherwise, DC AS will send an error message to the UE1 via MF. If DC AS does not have the UE1's Avatar ID list, it retrieves the UE1's Avatar ID list from the BAR. DC AS also optionally checks whether the token is valid.

Step 5. DC AS sends the Avatar Representation downloading request to BAR, including parameters of token and Avatar ID.

Step 6. BAR verifies the token provided by the DC AS. Specifically, BAR verifies the signature in the token based on the public key in the UE1's certificate. BAR checks whether the audience matches its own type, the subject is the UE1 ID and matches that in the certificate, the token is not expired. BAR also checks whether Avatar ID in the request equals to that in the token. How the BAR can obtain the UE1's certificate can be left to implementation. For example, the UE1's certificate can be issued by the operator's CA, and the BAR can obtain the UE1's certificate from the operator's CA.

Step 7. BAR sends the avatar representation downloading response message to the UE1 via DC AS and MF. If the verification in Step 6 is passed, the message includes the avatar representation, otherwise the message includes the error code, indicating that the token verification or the verification of the certificate fails.

Step 8. The subsequent procedure continues.

NOTE 4: Authorization of UE centric mode is left to implementation when both BAR and DC AS are outside the IMS network.

#### 6.5.2.3 Receiving UE centric procedure



Figure 6.5.2.3-1: Receiving UE Centric Authorization procedure for Avatar communication

Steps 0-1. Same as Steps 0-1 in Clause 6.5.2.1. The only difference is that subject is UE2 ID, i.e., IMPU of the UE2.

Step 2. UE1 sends the Avatar ID and token to UE2 during Avatar animation negotiation procedure.

Steps 3, 4. UE2 sends the Avatar representation downloading request to the DC AS via MF, including parameters of token, Avatar ID, and optionally CCA. The structure the CCA can be referred to clause 13.3.8.2 of TS 33.501 [11]. CCA is a token signed by the UE2, and enables the BAR to authenticate UE2. CCA is expected to be more short-lived than UE1 generated access tokens. CCA contains subject (UE2 ID), audience (BAR type), timestamp, and expiration time. The UE2 shall sign the generated CCA based on its private key that corresponds to the UE2's certificate.

Step 5. DC AS determines whether the received Avatar ID is in the UE1's Avatar ID list. If the received Avatar ID is equal to one of the Avatar ID in the UE1's Avatar ID list, Step 6 is executed. Otherwise, DC AS will send an error message to the UE1via MF and UE2. If DC AS does not have the UE1's Avatar ID list, it retrieves the UE1's Avatar ID list from the BAR. DC AS also optionally checks whether the token is valid.

Step 6. DC AS sends the Avatar representation downloading request to the BAR, including parameters of token and Avatar ID.

Step 7. BAR verifies the token provided by the DC AS. Specifically, BAR verifies the signature in the token based on the public key in the UE1's certificate. BAR checks whether the audience matches its own type, the subject is the DC AS type, the token is not expired. BAR also checks whether Avatar ID in the request equals to that in the token. If additional authentication of UE2 is required, BAR checks whether the subject in the CCA matches that in the token. The verification of the CCA can be referred to clause 13.3.8.2 of TS 33.501 [11]. Specifically, the BAR should check that the audience in the CCA matches its own type. The BAR verifies that the subject matches UE2 ID in the certificate used for signing the CCA. How the BAR can obtain the UE1 and UE2's certificate can be left to implementation. For example, the UE1 and UE2's certificate can be issued by the operator's CA, and the BAR can obtain the UE1 and UE2's certificate from the operator's CA.

Steps 8-10. BAR sends the avatar representation downloading response message to the UE2 via DC AS and MF. If the verification in Step 7 is passed, the message includes the avatar representation, otherwise the message includes the error code, indicating that the token verification or the verification of the certificate fails.

Step 11. The subsequent procedure continues.

### 6.5.3 Evaluation

The solution addresses the requirement of KI#2 related to the access of stored Avatar representations and Avatar-IDs. The procedure proposes to use the Avatar ID list to check the validity of the Avatar ID provided by the UE1, and a token with an Avatar ID for the authorization of obtaining the Avatar representation. This solution considers both network centric mode and the UE centric mode.

The solution requires DC AS to check whether the received Avatar ID is in the UE1's Avatar ID list.

The solution requires UE to generate a token with an Avatar ID.

The solution requires MF to request the Avatar representation with a token and Avatar ID in the network centric mode. The solution requires UE1/UE2 to request the Avatar representation with the token and Avatar ID in the UE centric mode.

The solution requires the BAR to determine whether the MF/UE1/UE2 is authorized to retrieve the Avatar representation by checking whether the Avatar ID in the Avatar representation downloading request is equal to the Avatar ID in the token.

The solution requires the UE1/UE2 to be provisioned with a certificate. The certificates are used to generate the tokens.

The solution requires the UE2 in the receiving UE centric procedure to optionally generate a CCA.

## 6.6 Solution #6: Solution for secure IMS based avatar communication

### 6.6.1 Introduction

This solution addresses key issue #2: Security of IMS based Avatar Communication.

According to TR 23.700-77 [2], rendering of avatar media can be performed by network, UE-1, or UE-2, which are called network centric IMS avatar call, sending UE centric IMS avatar call, and receiving UE centric avatar call, respectively.

In this solution, only authorized entity from UE-1 can access and retrieve the UE-1's avatar representation which is stored in a data storage called Base Avatar Repository (BAR). This solution proposes to use UE-1's attestation for the security procedure of IMS based avatar communication.

In this solution, it is assumed that BAR has CA certificate to verify UE-1's (UE-2’s) certificate, with UE-1's (UE-2’s) avatar representation and avatar ID. The UE certificate for media plane security can be reused to generate the signature in the attestation. In this solution, only unidirectional avatar communication is described. When bidirectional avatar communication is used (i.e., when UE-1's avatar and UE-2's avatar are sent to each other), UE-2 also performs the operation same as UE-1 described in this solution.

NOTE: Which entity acts as certificate authority is out of scope of this solution.

### 6.6.2 Solution details

#### 6.6.2.1 Network centric IMS avatar call flow



Figure 6.6.2.1-1 Network centric IMS avatar call flow

1. The UE1 initiates an IMS session and establishes audio and video session connections with theUE2. The bootstrap channel is established for both the UE1 andUE2. UE1obtains UE1's avatar id(s)through bootstrap data channel.

2. The UE1 decides to request network to perform avatar animation based on its status such as power, signal, computing power, internal storage, etc.

3. The UE1 performs the avatar animation negotiation with the DC AS. The UE1 generates UE1's attestation. The UE1's attestation consists of Avatar ID, rendering option (i.e., network centric), expiration time, signature generated by using UE1's private key, as described in clause 6.6.2.4 of this document. The UE1 sends UE1's attestation and UE1's certificate to the DC AS via DCSF. Before sending the attestation, DCSF optionally checks whether the UE1 is allowed to use the avatar ID after reading the avatar ID in the UE1’s attestation.

4. P2A2P Application data channel is established between UE1/UE2 and DC AS, and media re-negotiation between UE1, UE2, and MF is optionally performed. In this step, DC AS sends UE1's attestation and UE1's certificate to MF as described in step 7 in clause AC.11.3.3 of TS 23.228 [7].

5. MF requests avatar representation using UE1's attestation and UE1's certificate.

6. After BAR verifies the UE1's certificate, BAR verifies the signature in UE1's attestation using the UE1's public key. If the verification is successful the BAR responds with the UE1's avatar representation.

NOTE 1: When BAR and DC AS are outside of IMS network, step 5-6 is up to implementation.

NOTE 2: Protection between BAR and DC AS is out of scope of this solution.

7. The UE1 sends avatar metadata for the rendering (e.g., facial feature points).

8. The MF/MRF performs the media transcoding and animates the UE1's avatar representation.

10. The animated avatar media is sent as regular video media to UE2.

11. The animated avatar media is sent back to the UE1 as feedback.

#### 6.6.2.2 Sending UE centric IMS avatar call flow



Figure 6.6.2.2-1 Sending UE centric IMS avatar call flow

1. The UE1 initiates an IMS session and establishes audio and video session connections with the UE2. The bootstrap channel is established for both the UE1 and UE2. UE1 obtains UE1's avatar id(s) through bootstrap data channel.

2. Application data channel is established between UE1 and DC AS, and media re-negotiation is optionally performed.

3. The UE1 generates UE1's attestation. The UE1's attestation consists of Avatar ID, rendering option (i.e., sending UE centric), expiration time, signature generated by using UE1's private key, as described in clause 6.6.2.4 of this document. The UE1 sends UE1's attestation and UE1's certificate to the DC AS to download UE1's avatar representation.

4. DC AS optionally checks whether the UE1 is allowed to use the avatar ID after reading the avatar ID in the UE1's attestation.

DC AS requests avatar representation using UE1's attestation and UE1's certificate.

5. After BAR verifies the UE1's certificate, BAR verifies the signature in UE1's attestation using the UE1's public key. If the verification is successful the BAR responds with the protected UE1's avatar representation.

6. The DC AS sends the avatar representation to UE1.

NOTE: If UE1 is already storing its own avatar representation locally, step 3-6 is skipped.

7. The UE1 performs the avatar animation.

8. The UE1 transmits the animated video stream over RTP to UE2.

#### 6.6.2.3 Receiving UE centric IMS avatar call flow



Figure 6.6.2.3-1 Receiving UE centric IMS avatar call flow

1. The UE1 initiates an IMS session and establishes audio and video session connections with the UE2. The bootstrap channel is established for both the UE1 and UE2. UE-A obtains UE1's avatar id(s) through bootstrap data channel.

2. P2A2P Application data channel is established between UE1/UE2 and DC AS, and media re-negotiation is optionally performed.

3. UE1 decides to request UE2 to perform avatar animation based on its status such as power, signal, computing power, internal storage, etc.

4. UE1 performs avatar animation negotiation with the DC AS and UE2. The UE1 obtains UE2's ephemeral public key. The UE1 generates UE1's attestation. The UE1's attestation consists of Avatar ID, rendering option (i.e., receiving UE centric), ephermeral public key of UE2, expiration time, signature generated by using UE1's private key, as described in clause 6.6.2.4 of this document. The UE1 sends UE1's attestation and UE1's certificate to the UE2.

NOTE 1: Whether the information (e.g., ephemeral public key of UE2, UE1's attestation, UE1's certificate, etc.) can be exchanged in step 4 is not addressed in the present document.

5. UE2 downloads UE1's avatar representation from DC AS using the UE1's attestation and UE1's certificate

6. DC AS optionally checks whether the UE1 is allowed to use the avatar ID after reading the avatar ID in the UE1's attestation. DC AS requests avatar representation using UE1's attestation and UE1's certificate.

NOTE 2: Whether DC AS needs to check whether UE2 is allowed to download UE1's avatar representation is not addressed in the present document.

7. After BAR verifies the UE1's certificate, BAR verifies the signature in UE1's attestation using the UE1's public key. If the verification is successful, the BAR generates ephemeral public/private key pair and protects the UE1's avatar representation using the session key generated by ephemeral public key of UE2 included in the UE1's attestation and ephemeral private key of BAR. The BAR responds with the protected UE1's avatar representation and ephemeral public key of the BAR.

8. The MF sends the protected avatar representation and ephemeral public key of the BAR to UE2.

9. The UE1 sends the avatar metadata to UE2.

10. The UE2 generates session key using the ephemeral public key of the BAR and the ephemeral private key of UE2. UUE2 verifies the protected avatar representation using the session key and performs the UE1's avatar representation animation using the UE1's avatar representation and the avatar metadata received from UE1 in step 9.

NOTE 3: Whether it is necessary to protect the privacy of an avatar representation is not addressed in the present document.

NOTE 4: The alignment with TS 23.228 [7] is not addressed in the present document.

#### 6.6.2.4 UE1 attestation

UE1's attestation is generated by UE1 and it consists as follows:

Table 6.6.2.4-1 UE1 attestation

|  |  |
| --- | --- |
| Parameter | Description |
| Avatar ID | REQUIRED. ID used to retrieve UE-A's avatar representation. |
| Rendering option | REQUIRED. One of the followings: network centric, sending UE centric, or receiving UE centric |
| Ephemeral public key of UE2 | OPTIONAL. This is included when the rendering option is receiving UE centric. BAR uses ephemeral public key of UE2 and ephemeral private key of BAR to protect the UE1's avatar representation. The protected avatar representation is sent to UE2 and it is end-to-end protected between BAR and UE2. |
| Expiration time | REQUIRED. The expiration time of the UE1 attestation. |
| Signature | REQUIRED. Signature generated by UE1 using UE1's public key and the parameters in the attestation. |

### 6.6.3 Evaluation

This solution addresses the requirements of KI#2: Security of IMS based Avatar communication.

In this solution, BAR returns the avatar representation only when the avatar representation owner (i.e., UE1) requests its avatar. For that purpose, UE1 generates the attestation which BAR uses to verify whether the owner is requesting its avatar representation. In addition, the avatar representation which is privacy related information is end-to-end protected.

This solution requires UE to generate an attestation with an avatar ID.

This solution requires DCSF to check whether the received avatar ID is in the UE1’s avatar ID list.

This solution requires MF/DC AS to request the UE1's avatar representation with UE1’s attestation.

This solution requires BAR to determine whether the request for an avatar representation originates from the host of the avatar representation (i.e., UE1) by verifying the UE1's attestation.

## 6.7 Solution #7: Protect IMS DC based Avatar Communication

### 6.7.1 Introduction

The solution addressed KI#2 Security of IMS based Avatar Communication.

IMS avatar communication aims to provide avatar media rendered calls between the UE-A and the UE-B over IMS network. There're solutions in TR 23.700-77 proposed to use application data channel (DC) to download avatar representation (or object/metadata) for avatar media rendering. An avatar representation is stored in a data storage entity, called as Base Avatar Repository(BAR). The avatar representation is identified by an avatar id and can be fetched from the DAC using the avatar id.

This solution proposes security procedures to protect avatar id and object at rest, in transmission and in use. The solution proposes to authenticate and authorize a UE to use an avatar with signing and verifying the avatar id based on SHAKEN procedure and proposes to authenticate and authorize the XR application or MF/MRF to get avatar representation from the DAC based on CAPIF, NEF or SBI security defined in TS 33.122 [13] and TS 33.501[11]. For UE based rendering, the solution proposes to verify the authenticity of the avatar representation before using it for rendering.

### 6.7.2 Solution details

To prevent an avatar being accessed and used by unauthorized IMS caller, the solution proposes to sign and verify the avatar-id during IMS call. The solution proposes authentication and authorization based on CAPIF/NEF/SBI security when an avatar representation consumer accesses the avatar representation from the DAC. SIP security defined in TS 33.203[15] and DC integrity and confidentiality protection defined in TS 33.328[17] can be used to protect avatar id and avatar representation transmitted through IMS network.

NOTE: The alignment with TS 23.228 [7] is not addressed in the present document.

#### 6.7.2.1 Procedure to protect IMS DC based Avatar Communication (Network based Rendering)



Figure 6.7.2.1-1 Security procedure of IMS DC based Avatar Communication - network centric rendering

1. The UE-A initiates an IMS session and establishes audio and video session connections with the UE-B. The bootstrap data channel(s) (BDCs) are established at the same time for both the UE-A and UE-B. The Avatar ID list is downloaded to the UE through bootstrap data channel via DCSF. The DCSF can for example retrieve the Avatar ID list from DC AS or HSS repository data as a part of subscription data in HSS.

2. The UE-A decides to request network media rendering based on its status such as power, signal, computing power, internal storage, etc. The UE-A selects the Avatar-id of the avatar from the Avatar-id list downloaded from the first step, which is intended to use for the call.

3. As shown in the step 1 to step 26 of workflow in the AC.7.2.2 of TS 23.228 [7], the UE-A performs the application data channel (ADC) negotiation with the XR Application Server for XR media rendering. The negotiation includes usage of the Avatar-id and the indication of network based rendering preference received from the UE-A. During this workflow, the IMS AS validates with HSS or locally based on subscription data retrieve from HSS before. If the UE is authorized to use the Avatar-id for the application based on subscription data, IMS AS signs the Avatar-id together with at least calling id, application id, then includes the signed Avatar-id in negotiation message to UE-B through the terminate IMS. The terminating IMS network verifies the signed Avatar-id. If successful, it forwards the Avatar-id to UE-B.

NOTE 1: How to provision subscription data with Avatar-id is out of scope of this workflow.

NOTE 2: Ms reference point can be used to sign Avatar-id together with application id. The signed Avatar-id is generated by authorized signing server based on at least calling UE IMS id (e.g. IMPU of the calling UE), Avatar-id, and application Id for the avatar call.

4. If the negotiation result is successful in step 3, the UE-A initiates new P2A application data channels, which are used for XR data transmission between the UE-A and the network. During the P2A application data channel establishment procedure, the DCSF will instruct the MF via IMS AS how to establish the data channel and corresponding media processing specification. An optional UE token is included in the DC establishment messages. The UE token is generated by UE which includes UE IMS id (IMPU or IMPI) and XR application server (XR AS) id, expire time, and signature signed with UE certificate. The UE certificate used for media plane protection can be reused and exchanged via SIP message in step 3, which can be used to validate the UE token by IMS network. The UE token is sent to XR AS during ADC establishment or via ADC after the ADC establishment.

NOTE 3: The UE token will be used by XR AS for authorization of accessing BAR on behalf of the UE-A. XR AS includes the UE token in the request to NEF/CCF/NRF to get access token. NEF/CCF/NRF verifies the signature of the UE token with the UE certificate , and validates if the token expired by checking expire time of the UE token . If the verification is successful, the XR AS is treated as delegation of UE-A and NEF/CCF/NRF optionally authorizes BAR access to the XR AS on behalf of the UE-A. If UE token is not available, local policy is used by NEF/CCF/NRF to authorize the XR AS to access the BAR.

5(Optional). IMS AS initiates a media re-negotiation request with UE-A by exchanging the Avatar-id via the application DC, to connect/anchor UE-A's audio/video media stream to MF/MRF. UE-A provides to the XR Application Server via the application DC the Avatar-id of the avatar intended to use for the call.

6. IMS AS initiates a media re-negotiation request with UE-B, to connect/anchor UE-B's audio/video media stream to MF/MRF. The Avatar-id is exchanged with UE-B to indicate about the avatar session during the signalling. UE-B has the option to reject the avatar alone or terminate the session based on Avatar-id.

NOTE 4: Media re-negotiation in step 5 and 6 is for anchoring audio/video in MF to support network based avatar rendering.

7. Before retrieving the avatar representation from BAR, the XR AS authenticates with NEF/CAPIF CF/NRF based on mTLS and sends token request to NEF/CAPIF CF/NRF to access avatar from the BAR. The token request includes at least signed Avatar-id, UE token, application id. NEF/CAPIF CF/NRF verifies the signed Avatar-id with IMS AS and validates the UE token based on UE certificate exchanged in SIP message. If successfully verified Avatar-id and UE token, the NEF/CAPIF CF/NRF grants access token to the XR AS based on UE IMS Id, Avatar-Id, application id in the request and in the UE token, and policies configured locally or got from HSS. The access token includes application id, BAR instance id, Avatar-id and operations on the avatar representation associated to the Avatar-id.

NOTE 5: Authentication and authorization mechanism defined in TS 33.122 [13] or TS 33.501 [11] can be reused to authenticate and authorize XR AS.

The XR Application Server retrieves the avatar representation from BAR using the Avatar-id and access token got from NEF, CAPIF CF or NRF.

NOTE 6: The procedure assumed the BAR is inside IMS or 5GC network. It's implementation dependent if BAR is out of IMS or 5GC network.

8. The XR Application Server retrieves the avatar representation using the Avatar-id from BAR.

9. The BAR validates the access token and responds to the XR Application Server with the signed avatar representation.

9.1. The XR AS verifies the signature of the avatar and expiration time of the avatar.

NOTE 7: The certificate used to sign the avatar can be preconfigured in XR AS.

NOTE 8: It's implementation dependent if XR AS is outside of IMS or 5GC network.

10. The XR Application Server starts controlling the XR media rendering.

11. The XR Application Server sends the avatar representation to MF/MRF and requests rendering of the avatar by MF/MRF.

11.1 The MF verifies the signature of the avatar and expiration time of the avatar.

NOTE 9: The certificate used to sign the avatar can be preconfigured in the MF.

NOTE 10: MF verifies the signature of the avatar only when XR AS is outside of IMS or 5GC network in which case the XR AS is untrusted by MF and can potentially tamper the avatar representation.

12. The UE-A sends information about UE-A to MF/MRF.

13. The MF/MRF receives the information of UE-A from the UE-A and replaces the face/body with the selected avatar representation, e.g. via face detection and/or recognition mechanisms.

14. The rendered avatar media is sent as regular video media to UE-B.

15. The rendered avatar media is sent back to the UE-A as feedback (same content as the one sent to the UE-B in step 13), e.g. to display a thumbnail view of the avatar to the UE-A in the IMS session.

NOTE 11: If exception happened in security steps, the IMS session is potentially not be established or is potentially established without avatar media.

#### 6.7.2.2 Procedure to protect IMS DC based Avatar Communication (UE-A based Rendering)



Figure 6.7.2.1-2 Security procedure of IMS DC based Avatar Communication - UE-A based rendering

1-8. Same to steps 1-9 of Figure 6.7.2.1-1 except certificate to sign the avatar representation is sent to UE-A in step 3, UE-A based rendering indication is exchanged in step 3, and optional step 5 of Figure 6.7.2.1-1 for media re-negotiation between IMS AS and UE-A is not needed for the UE-A based rendering procedure.

9. To ensure the avatar is not tampered especially in case the XR Application Server is not owned by the operator, the XR AS sends the signed avatar representation to the UE-A through application data channel to trigger UE-A based rendering.

10. If the avatar representation is signed, the UE-A verifies signature of the signed avatar representation with the certificate received in step 3 from IMS AS. The UE-A locally mixes the avatar representation together with the audio/video media received from local sensors (e.g. camera) to animate the avatar (the rendered avatar audio/video media).

11. The UE-A sends the rendered avatar audio/video media as regular video media to the UE-B.

#### 6.7.2.3 Procedure to protect IMS DC based Avatar Communication (UE-B based Rendering)



Figure 6.7.2.1-3 Security procedure of IMS DC based Avatar Communication - UE-B based rendering

1-8. Same to steps 1-9 of Figure 6.7.2.1-1 except certificate to sign the avatar representation is sent to UE-B in step 3, UE-B based rendering indication is exchanged in step 3, and optional step 5 of Figure 6.7.2.1-1 for media re-negotiation between IMS AS and UE-A is not needed for the UE-B based rendering procedure.

9. To ensure the avatar is not tampered especially in case the XR Application Server is not owned by the operator, the XR AS sends the signed avatar representation to the UE-B through application data channel based on UE-B based rendering indication.

10. If the avatar representation is signed, UE-B verifies signature of the signed avatar representation using the certificate received at step 3, and sends response to XR Application Server

11. After receiving the successful response from UE-B, the XR Application Server forwards the response to UE-A via IMS AS indicating about the readiness of UE-B based rendering.

12. The UE-A sends XR information about UE-A, which is sufficient for rendering, to UE-B.

13. The UE-B locally mixes the avatar representation together with the received information of UE-A to animate the avatar (the rendered avatar audio/video media).

### 6.7.3 Evaluation

The solution addresses requirements of KI#2 which ensures that stored Avatar representations and Avatar-IDs are accessed only by authenticated and authorized entities, supports the integrity protection of the Avatar-ID and Avatar representation on the originating side and terminating side, as well as ensures Avatar representation will not be used for impersonating a IMS caller.

The solution covers security aspects of network based, UE-A and UE-B based avatar media rendering for data channel based avatar communication.

IMS-AS, MF, HSS, XR AS, NRF/CCF and UE need to be enhanced to protect Avatar representation and Avatar-ID at rest and in transmission, as well as ensure the Avatar can only be used by the authorized IMS user.

NOTE: The alignment with TS 23.228 [7] is not addressed in the present document.

## 6.8 Solution #8: Security for IMS based Avatar Communication

### 6.8.1 Introduction

This solution addresses the Key Issue #2 "Security of IMS based Avatar Communication".

As stated in key issue #2 details, subscribers could use Avatars during their calls to other subscribers. Avatars are expected to be identified by Avatar IDs and Avatar IDs are used for referring to the Avatar objects during IMS calls. From a security point of view, a solution for handling IMS calls using 3P IDs is quite similar to handling of Avatar enriched IMS calls. Therefore this solution description is similar to solution #2 " Security of 3rd party specific identities ".

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] for signing and verification of both the caller and the callee avatar related data and metadata.

NOTE 1: Whether this procedure is applicable to DC based avatar communication is not addressed in the present document.

NOTE 2: The alignment with TR 23.700-77 [2] terminology is not addressed in the present document.

### 6.8.2 Solution details

Figure 6.8.2-1 shows the sequence diagram of the solution.



Figure 6.8.2-1: Avatar IMS communication

1. The Caller UE sends a SIP INVITE that contains the Caller IMPU and optionally the Avatar identifier (Caller Avatar ID) .

2. The originating IMS system checks whether the IMS subscription of the calling UE is authorized to use avatars and the Avatar ID.. If the UE is not authorized to use avatars , then the originating IMS system ignores the Avatar ID data within the SIP INVITE (if present) and does not execute the rest of avatar related steps during the call set-up. The call continues without presenting any avatar to the callee.

NOTE 1: How is UE authorized to use avatars, is not addressed in the present document.

If the UE is authorized to use avatar IMS communication, the originating IMS system retrieves the avatar object data (avatar representations such as avatar images or avatar animation models, avatar metadata e.g. avatar name, avatar user name etc) or avatar object references of the caller from an Avatar Object Server (AOS) based on the received IMS identity and potentially provided Avatar ID. The originating IMS system could also provide the callee IMS identity (Callee IMPU) for authorization purposes in Step 21. If the Callee IMPU is also provided to the OAS upon the originating system accessing the avatar objects then the OAS maintains a tuple (see Step 21) for the purposes of authorization when the caller/callee attempts to access the callee/caller avatar in a later stage. If no Avatar object data exist for this subscriber (IMS identity), the rest of avatar related steps are not executed during the call set-up. The call continues without presenting any avatar to callee.

NOTE 2: The AOS is in general a database of avatar objects for each IMS subscriber. An IMS subscriber is identified by the IMS identity and for each identity there could be multiple avatar objects each of which identified with a unique identifier Avatar ID. Each avatar object can include an avatar image, or avatar animation model, avatar name/nickname, etc. The OAS can also have a default avatar object for a specific IMS identity for a Avatar ID with no value.

NOTE 3: If no Avatar ID is received in the SIP INVITE from the UE, suppression of a AOS lookup can be optionally applied based on a local policy. If there is a mismatch between the received Avatar ID in the SIP INVITE and data retrieved from the AOS based on the IMS identity, it is governed by a local policy of the originating IMS system how the population of the Avatar object data or avatar object references into the SIP (Identity) header will be done. It can be noted that the SIP identity header is an example header that can carry avatar objects, avatar object references (e.g. URIs) or the Caller Avatar ID. In the context of avatar communication a new SIP header could be introduced or the these pieces of information (avatar objects, avatar object references, Avatar ID etc) could be grouped along when calculating the signature and could be included as additional data in a SIP INVITE.

3. The originating IMS system adds a P-Asserted-Identity header field asserting the telephone number and avatar object data of the SIP UA and invokes the originating STI-AS (O-STI-AS)to sign the SIP Identity header.

NOTE 4: The avatar object data to be signed can be any combination of the avatar object information included in the AOS database for a specific IMS subscriber and a specific Avatar ID. For example the avatar object data to be used for signing can be the Avatar ID, a reference (URI) to an avatar image, an avatar nickname, the IMS user full name etc.

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

5. The O-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 system invokes the terminating STI-VS (T-STI-VS) to verify the signed SIP identity header.

8. The T-STI-VS validates the certificate, extracts the public key and verifies the signature in the Identity header field, which validates the Caller ID and avatar data signed in the INVITE message on the originating O-STI-AS.

9. Depending on the result of the STI validation, the T-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 avatar data (avatar object or avatar references), the call can continue but without using any avatar to the terminating SIP UA.

10. The SIP INVITE with the verstat parameter is sent to terminating SIP UA. The terminating IMS system could optionally send the avatar data to the terminating SIP UA. The purpose of this information is for the terminating SIP UA to be able to render the originating avatar object at the terminating side.

11. The terminating SIP UA sends 18X and 200 to the terminating IMS system. If the terminating SIP UA can support avatar IMS communication, the SIP UA can optionally include the Callee Avatar ID in the 18X or 200 type of message.

12. The terminating IMS system checks whether the IMS subscription of the callee UE is authorized to use avatars and the Avatar ID in the IMS communication between the caller and the callee. If the UE is not authorized to use avatars, then the terminating IMS system ignores the Avatar ID data within the 18X/200 message (if present) and does not execute the rest of avatar related steps during the call set-up. The call continues without presenting any avatar to the caller. The terminating IMS system could also provide the callee IMS identity (Callee IMPU) for authorization purposes in Step 21.

NOTE 5: How the avatar repository determines whether an avatar model/data can be returned to the IMS system, is not addressed in the present document.

If the callee UE is authorized to use avatar IMS communication, the terminating IMS system retrieves the avatar data objects of the callee from the (AOS) based on the received IMS identity. If the caller IMS identity is also provided to the OAS upon the terminating system accessing the avatar objects then the OAS maintains a tuple (see Step 21) for the purposes of authorization when the caller/callee attempts to access the callee/caller avatar in a later stage. Please observe that the OAS of the caller and the AOS of the callee could be different. If no Avatar object data exist for this subscriber (IMS identity), the rest of avatar related steps are not executed during the call set-up. The call continues without presenting any avatar to caller.

NOTE 6: If no Avatar ID is received in the SIP 18X/200 from the UE, suppression of a AOS lookup can be optionally applied based on a local policy. If there is a mismatch between the received Avatar ID in the SIP 18X/200 and data retrieved from the AOS based on the IMS identity, it is governed by a local policy of the originating IMS system how the population of the avatar object data into the SIP (Identity) header will be done. In this step the It can be noted that the SIP identity header is an example header and similar considerations as in Step 2 are assumed.

13. The terminating IMS system potentially adds a P-Asserted-Identity header field asserting the telephone number and avatar object data of the SIP UA of the callee and invokes the terminating STI-AS (T-STI-AS)to sign the SIP Identity header.

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

15. The T-STI-AS returns the signed SIP identity header back to terminating IMS system.

16. The terminating IMS system sends the 18X/200 message including the signed avatar object databack to the originating IMS system. Over the NNI through the standard inter-domain routing configuration.

17. The originating IMS system invokes the originating STI-VS (O-STI-VS) to verify the signed SIP identity header.

18. The O-STI-VS validates the certificate, extracts the public key and verifies the signature in the Identity header field, which validates the Caller ID and avatar object or avatar object references signed in the 18X/200 message on the originating T-STI-AS.

19. Depending on the result of the STI validation, the O-STI-VS determines that the call is to be completed with an appropriate indicator and the result is passed back to the originating IMS system which continues to set up the call to the originating SIP UA. If the Caller ID is validated OK but not the avatar related data (avatar object or avatar references), the call can continue but without using any avatar to the terminating SIP UA.

20. The SIP 18X/200 message with the verstat parameter is sent to originating SIP UA. The originating IMS system could optionally send avatar object data to the originating SIP UA. The purpose of this information is for the originating SIP UA to be able to render the terminating avatar object at the originating side.

NOTE 7: It is not addressed in the present document when the originating IMS system retrieves the callee avatar data.

21. An avatar call is being initiated between the originating and terminating UEs. As part of this step the originating and terminating UEs optionally access avatar objects of the other party in order to render the avatars at each UE, i.e., the callee UE could access the avatar objects of the caller based on avatar object data in the signed SIP identity header received from step 10 and similarly the caller could access the avatar objects of the callee based on avatar object data in the signed SIP identity header received from Step 20. If the OAS includes a tuple of (Caller IMS Identity, Callee IMS identity, Caller Avatar ID, Callee Avatar ID) for authorization purposes, the OAS allows access to caller or callee avatar objects based on UEs providing their IMS identities and Avatar IDs. A local policy on OAS can determine if the UEs can access the avatar objects once or multiple times.

NOTE 8: It is not addressed in the present document how the solution works in case the rendering is caller-UE or callee-UE centric (and not both) or network-centric.

### 6.8.3 Evaluation

This solution addresses the requirements of Key Issue #2 "Security of IMS based Avatar Communication"

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 SIP identity header including avatar object data or references.

The solution relies on a Avatar Object Server which contains the association of the Avatar ID and the corresponding Avatar objects (e.g. avatar images, animation models etc) with the corresponding IMS identities.

## 6.9 Solution #9: Secure IMS DC capability exposure

### 6.9.1 Introduction

The solution addressed KI#3 security and privacy aspects of IMS DC capability exposure.

Solutions to support IMS event and capability exposure in the context of data channel (DC) communication/session are developed in TR 23.700-77 [7]. Without proper security control, the IMS DC services are potentially illegally used by malicious application function/server (AF/AS), e.g. the malicious AF potentially eavesdrops or manipulates IMS DCs, the malicious AF potentially launches DoS attack with updating/terminating an ongoing DC, and causes interruption on the IMS communication of an end user, privacy of IMS user is also potentially compromised.

This solution proposes security procedures to authenticate and authorize DC AS before grant permission to the DC AS on IMS DC event or IMS DC session control.

### 6.9.2 Solution details

Basically, the DC AS/AF is authenticated based on the description in clause 13 or clause 12 of TS 33.501 [11]. The AF authorization is based on clause 13 or clause 12 or local configuration at the NEF. In addition, the solution describes detail procedure to authorize an DC AS/AF to subscribe to DC event or control DC session in IMS network. The solution assumes the DC specific authorization policies are preconfigured in HSS or NEF, and the authorization decision will be made by NEF/HSS based on DC AS properties, DC related services and other conditions.

#### 6.9.2.1 Procedure of DC AS authorization for DC event subscription

Precondition:

- Authorization policies are provisioned in NEF/HSS.



Figure 6.9.2.1-1 DC AS authorization for DC event subscription

Procedures:

1. NEF receives DC event subscription request from DC AF/AS.

2. After authenticating the AF/AS (TLS based mutual authentication), NEF retrieves authorization policies locally or from HSS.

3. NEF makes authorization decision and grants permission for the request based on the policies. For subscriber specific event subscription request, the authorization decision is optionally made by HSS when it received event subscription request from the NEF.

4. NEF sends DC non-subscriber specific event subscription request to IMS AS, or sends subscriber specific event subscription requests to HSS, then HSS forwards the request to the IMS AS.

5. NEF receives response from IMS AS/HSS.

6. NEF sends response to the DC AF/AS

7. NEF receives event notification from IMS AS.

8. NEF sends the notification to the DC AF/AS. The notification is optionally anonymized based on privacy policies or regulations.

#### 6.9.2.2 Procedure of DC AS authorization for data channel session control

DC session control includes bootstrap and application DC establishment, update and termination, as well as DC application download.



Figure 6.9.2.2-1 DC AS authorization for data channel session control

Procedures:

1. NEF receives bootstrap data channel (BDC)/application DC (ADC) establishment/termination/update or application download request from DC AF/AS.

2. After authenticating the DC AF/AS (TLS based mutual authentication), NEF retrieves authorization policies locally or from HSS.

3. If the session control is targeted an ADC, according to authorization policies, NEF optionally further checks if the DC AF/AS is matched to the DC application associated to the target ADC.

NOTE 1: NEF optionally checks locally or check with DCSF, or this check can be done by DCSF.

4. If the DC AF/AS is allowed to perform the required session control on the DC based on the authorization policies, NEF grants permission for the request.

5. NEF searches IMS AS from HSS and sends DC session control request to the IMS AS. IMS AS re-invites the IMS call to include DC offer with UEs, and reserve DC resource with MF if needed.

6. NEF receives response from IMS AS.

7. NEF sends response to the DC AF/AS.

### 6.9.3 Evaluation

The solution addresses requirements of Key issue #3 to support authentication and authorization of data channel application server during the IMS capability exposure procedures.

NEF, or CAPIF Core Function in case CAPIF is deployed, needs to enhance to support data channel specific authorization.

The solution is aligned with SA2 conclusion on KI#1 of TR  23.700-77 [2], and whether IMS AS or DCSF is contacted for DC session control will be aligned with SA2 on solution of KI#2 of TR 23.700-77 [2].

The solution assumes that the NEF performs local authorization or authorization based on authorization policies retrieved from the HSS.

## 6.10 Solution #10: User aware IMS DC capability exposure

### 6.10.1 Introduction

The solution addresses KI#3 on the security aspects of IMS DC capability exposure.

### 6.10.2 Solution details

The solution addresses the problem that the malicious AF such as DC AS, eavesdrop or manipulate the IMS DC without the permission of the resource owner. When the NEF supports CAPIF for external exposure as specified in clause 6.2.5.1 in TS 23.501 [14], it is proposed to reuse clause 6.5.3, TS 33.122 [13], with which the AF can controlthe IMS DC with the permission from the resource owner. Specifically, the API invoker is the AF.

When the AF controls the DC session, the interaction with the UE is required.

### 6.10.3 Evaluation

The solution addresses the requirements of KI#3 on the authorization of AF (such as DC AS) based on resource owner permission, during the IMS capability exposure procedures.

The solution requires the NEF to support CAPIF.

The solution requires the interaction with the UE.

No further impact is identified.

## 6.11 Solution #11: IMS (DC) capability exposure security based on existing specification

### 6.11.1 Introduction

This solution addresses the requirements of Key Issue #3: "Security and privacy aspects of IMS DC capability exposure".

Under this solution it is assumed that an Application Function (AF) subscribes to IMS events that are DC related as well as IMS events that are non-DC related.

Moreover, the AF can control DC lifecycle operations such as initiation, update and termination of DC.

### 6.11.2 Solution details

#### 6.11.2.1 General

The solution for the DC capability exposure security includes two parts, one covers the security of the IMS (DC or non-DC) event exposure and the other covers the security of the IMS DC control procedures.

#### 6.11.2.2 IMS event exposure security

The sequence diagrams of the IMS event exposure are shown in Figures 6.11.2.2-1 and 6.11.2.2-2 which are based on the conclusions in TR 23.700-77 [2].



Figure 6.11.2.2-1: IMS event exposure security for subscriber specific IMS events

The steps for the subscriber-specific IMS event exposure are the following.

1. The UE performs initial IMS Registration and IMS-AS instances also register with the HSS. .Moreover the AF is assumed to have a valid TLS certificate. For the NEF - AF security TS 33.501 [11], clause 12 is assumed to be followed.

2. The AF subscribes to NEF initiating the Subscribe Request for a subscriber specific IMS event/event category. The AF can include one or more IMS subscriber identifiers (IMPUs) in the subscription request.

NOTE 1: It is assumed that the AF logic includes the list of IMS subscriber identifiers for whom the AF logic is programmed to react to related IMS events.

3. The NEF checks whether the AF is authorized to subscribe to events as per TS 33.501 [11], clause 12.

4. The NEF discovers and subscribes for each IMS subscriber in the incoming subscription request a separate subscription request towards IMS-AS for the requested event/event category

5. The NEF returns to the AF a Subscribe Response.

6. At some point, the requested event for the UE is detected by the IMS AS.

7. The IMS AS exchanges a Notify Request/Response with the NEF.

8. The NEF and AF exchange a Notify Request/Response.

It can observed that the security aspects of this procedure are mainly how the NEF authenticates and authorizes the AF requests for the specific IMS subscribers and specific events.



Figure 6.11.2.2-2: IMS event exposure security for non-subscriber specific IMS events

The steps for the non-subscriber-specific IMS event exposure are the following.

1. The UE performs initial IMS Registration and IMS-AS instances also register with the HSS. .Moreover the AF is assumed to have a valid TLS certificate. For the NEF - AF security TS 33.501 [11], clause 12 is assumed to be followed.

2. The AF subscribes to NEF initiating the Subscribe Request for a non-subscriber specific IMS event/event category.

3. The NEF checks whether the AF is authorized to subscribe to events as per TS 33.501 [11], clause 12.

4. NEF discovers and subscribes to the IMS AS instances that support the requested IMS event/event category via the NRF

5. The NEF returns to AF a Subscribe Response.

6. At some point, the requested event for the UE is detected by the IMS AS.

7. The IMS AS and NEF exchange a Notify Request/Response.

8. The NEF and AF exchange a Notify Request/Response.

It can observed that the security aspects of this procedure are mainly how the NEF authenticates and authorizes the AF requests for the specific events.

#### 6.11.2.3 IMS DC session control exposure security

The procedure for the IMS DC session control exposure is shown in Figure 6.11.2.3-1 which is based on the conclusions in TR 23.700-77 [2].



Figure 6.11.2.3-1: IMS DC session control exposure

The steps for the IMS DC session control exposure are the following.

1. The UE performs initial IMS Registration and IMS-AS (or DCSF) instances also register with the HSS. .Moreover the AF is assumed to have a valid TLS certificate. For the NEF - AF security TS 33.501 [11], clause 12 is assumed to be followed.

2. The AF initiates a request for IMS DC session control providing the IMS subscriber identity (IMPU) and the command specification (establishment, update, termination of bootstrap and application data channels).

NOTE 1: It is assumed that the AF logic includes the list of IMS subscriber identifiers for whom the AF logic is programmed to affect the IMS DC sessions.

3. The NEF checks whether the AF is authorized to invoke a DC session control request as per TS 33.501 [11], clause 12.

4. The NEF exchanges a DC session control Request/Response with an IMS-AS (or DCSF)..

5. The NEF responds to the AF with a DC session control response.

### 6.11.3 Evaluation

This solution fulfils the requirements of Key Issue #3: "Security and privacy aspects of IMS DC capability exposure " by reusing the existing specification in TS 33.501 [11], clause 12.

The external DC AS can be considered as an AF within the 3GPP operator domain.

The existing authentication and authorization requirements and procedures for the NEF - AF interactions specified in TS 33.501 [11], clause 12 are sufficient in addressing the KI#3 requirements.

## 6.12 Solution #12: Solution for secure IMS based avatar communication using STIR/SHAKEN

### 6.12.1 Introduction

This solution addresses key issue #2: Security of IMS based Avatar Communication.

According to conclusion in TR 23.700-77 [2], rendering of avatar media can be performed by network, UE1, or UE2. This solution proposes security procedures for the three avatar calls to protect avatar ID and avatar representation.

This solution proposes to use STIR/SHAKEN framework for signing and verification of the avatar ID.

The avatar communication can be unidirectional or bidirectional. In this solution, only unidirectional avatar communication is described. When bidirectional avatar communication is used, UE2 also performs the operation same as UE1 described in the procedure.

### 6.12.2 Solution details

#### 6.12.2.1 Network centric IMS avatar call flow



Figure 6.12.2.1-1 Network centric IMS avatar call flow

1. UE1 initiates an IMS session and establishes audio and video session connections with UE2. The bootstrap channel is established for both UE1 and UE1. UE1 optionally obtains its own avatar ID list from HSS/UDM.

2. UE1 performs the XR media rendering negotiation. UE1 chooses an avatar ID to be used from the list and sends it to DCSF. DCSF checks whether the UE1 is allowed to use the avatar ID. DCSF optionally retrieves UE1's avatar ID list from HSS/UDM.

3. DCSF requests Avatar representation by sending the UE1's avatar ID.

4. BAR responds with the avatar representation.

5. DCSF requests a signature to STI AS by sending the UE1's avatar ID.

6. STI AS signs UE1's avatar ID and sends it to DCSF.

7. DCSF sends the UE1’s avatar representation to MF for the rendering. UE1's avatar ID with the signature is sent to the terminating IMS network. The terminating IMS network invokes the STI VS to verify the signature.

8. The UE1 sends data for the rendering (e.g., facial feature points).

9. The MF performs the rendering using the UE1's avatar representation and the data received from UE1 in step 8.

10. The rendered avatar media is sent as regular video media to UE2.

11. The rendered avatar media is sent back to the UE1 as feedback.

#### 6.12.2.2 Sending UE centric IMS avatar call flow



Figure 6.10.2.2-1 UE1 centric IMS avatar call flow

1. UE1 initiates an IMS session and establishes audio and video session connections with UE2. The bootstrap channel is established for both UE1 and UE2. UE1 optionally obtains its own avatar ID list from HSS/UDM.

2. UE1 performs the XR media rendering negotiation. UE1 chooses an avatar ID to be used from the list and sends it to DCSF. DCSF checks whether the UE1 is allowed to use the avatar. DCSF optionally retrieves UE1's avatar ID list from HSS/UDM.

3. DCSF requests Avatar representation by sending the UE1's avatar ID.

4. BAR responds with the avatar representation.

5. DCSF requests a signature to STI AS by sending the UE1's avatar ID.

6. After STI AS signs UE1's avatar ID, STI AS sends the signature to DCSF.

7. DCSF sends UE1's avatar representation to UE1 for the rendering. UE1's avatar ID with the signature is sent to the terminating IMS network. The terminating IMS network invokes the STI VS to verify the signature.

NOTE: The need to send the avatar ID and the signature verification is not addressed in the present document.

8. The UE1 performs the rendering.

9. The rendered avatar media is sent as regular video media to UE2.

#### 6.12.2.3 Receiving UE centric IMS avatar call flow



Figure 6.12.2.3-1 UE2 centric IMS avatar call flow

1. UE1 initiates an IMS session and establishes audio and video session connections with UE2. The bootstrap channel is established for both UE1 and UE2. UE1 optionally obtains its own avatar ID list from HSS/UDM.

2. UE1 performs the XR media rendering negotiation. UE1 chooses an avatar ID to be used from the list and sends it to DCSF. DCSF checks whether the UE1 is allowed to use the avatar ID. DCSF optionally retrieves UE1's avatar ID list from HSS/UDM.

3. DCSF requests Avatar representation by sending the UE1's avatar ID.

4. BAR responds with the avatar representation.

5. DCSF requests a signature to STI AS by sending the UE1's avatar ID and avatar representation.

6. STI AS signs them and sends the signature to DCSF.

7. DCSF sends UE1’s avatar representation to UE2 for the rendering. UE1's avatar ID and avatar representation with the signature are sent to the terminating IMS network. The terminating IMS network invokes the STI VS to verify the signature.

8. The UE1 sends data for the rendering (e.g., facial feature points).

9. The UE2 performs the rendering using the UE1's avatar representation and the data received from UE1 in step 8.

NOTE 1: Whether DCSF can retrieve the avatar representation from BAR is not addressed in the present document.

NOTE 2: Which entity (CSCF or DSCF) transfers the avatar representation is not addressed in the present document.

NOTE 3: The alignment with conclusions from TR 23.700-77 [2] is not addressed in the present document.

NOTE 4: Whether to use SIP to transfer avatar ID and avatar representation is not addressed in the present document.

### 6.12.3 Evaluation

This solution addresses the requirements of KI#2: Security of IMS based Avatar Communication.

In this solution, STIR/SHAKEN framework is used to sign and verify the avatar ID. In UE2 centric avatar call flow where avatar representation itself is sent to UE2 via terminating IMS network, signed avatar representation is also transferred to the IMS network of UE2.

NOTE 1: The Impact on the network functions is not addressed in the present document.

NOTE 2: Whether to use non-DC to transfer avatar ID and avatar representation is not addressed in the present document.

## 6.13 Solution #13: IMS avatar communication security based on existing specification

### 6.13.1 Introduction

This solution addresses the Key Issue #2 "Security of IMS based Avatar Communication". It proposes the changes on the procedures in TS 23.228 [7], clause AC.11.3.

The Base Avatar Repository (BAR) is considered to be a database with records which associate a UE public identity e.g. IMPU with a list of Avatar IDs. Each Avatar ID is associated with an avatar representation and avatar metadata. It is assumed that the BAR is provisioned with this information for each UE which supports IMS avatar communication.

As such the BAR includes allowed lists of UE identities and Avatar ID, therefore these lists can be used for authorization purposes in subsequent procedures.

The solution is based on the observation that that the access of the Avatar ID and the avatar representation and avatar metadata is mediated by IMS nodes which have authenticated any UE involved in the procedures and therefore can also authorize the related UEs when accessing the Avatar ID and Avatar representation and metadata.

In addition, although not stated in the requirements of KI#2, the solution proposes the addition of the requirements for entities who don't own Avatar IDs and avatar representations/metadata, that they delete these pieces of information as soon as the avatar communication session is terminated.

### 6.13.2 Solution details

#### 6.13.2.1 General

The security of the of the different cases of rendering are captured in the clauses below.

Editor's Note: Whether additional evidence needs to be presented to BAR by DC AS/MF to prove it has been authorized is FFS.

Editor's Note: How implicit authorization works if BAR or DC AS is deployed outside of the operator domain, is FFS.

##### 6.13.2.1.1 Security for the Sending UE centric procedure

Figure 6.13.2.1.1-1 depicts the procedure from TS 23.228 [7], AC.11.3.2.1, "Sending UE centric procedure". The Application Data Channel (ADC) setup between the UE1 and DC AS is a P2A (Peer to Application) data channel as specified in TS 33.328 [17]. Therefore the UE and DC AS are mutually authenticated and the transport of information between these entities is secure.



Figure 6.13.2.1.1-1: Procedures of Sending UE centric IMS Avatar communication (TS 23.228 [7], AC.11.3.2.1-1)

By Step 3 (UE1 to DC AS) the DC AS has already authenticated the UE1 and it also possesses the UE1 Identity e.g. IMPU1 and UE Avatar ID1. Therefore, it can act as a delegate for the UE1 towards the BAR. The interface between the DC AS and the BAR is assumed to be secure in order to prevent any leakage of the UE1 IMPU1, Avatar ID1 and avatar representation corresponding to the Avatar ID1. Step 4 is subject to authorization as per requirements of KI#2, that only authorized entities which present the right Avatar IDs and the right UE identities can have access to the avatar representations. This solution assumes that the BAR checks (Step 4a) whether the provided (IMPU1, Avatar ID1) tuple by the DC AS is in its database of allowed IMPUs and Avatar IDs and returns the avatar representation to the DC AS if there is a match. The assumption is that the DC AS acts as delegate for the UE which is requesting its own avatar representation corresponding to Avatar ID1. The changes to the procedure in TS 23.228 [7], AC.11.3.2.1 are the following:

Step 3a. The DC AS retrieves the Avatar ID list for the specific UE1 identity from the BAR. Based on this list the DC AS checks if the UE1 provided Avatar ID1 is in the Avatar list of UE1. Then Step 4 could be an avatar representation access request to the BAR. Depending on the implementation the BAR can be a simple data base which allows access to the avatar representation by the DC AS assuming that the DC AS has already authorized the request from UE1.

Step 4a. The BAR optionally checks whether the provided (IMPU1, Avatar ID1) tuple by the DC AS is in its database of allowed IMPUs and Avatar IDs and returns the avatar representation to the DC AS if there is a match.

##### 6.13.2.1.2 Security for the Receiving UE centric procedure

Figure 6.13.2.1.2-1 depicts the procedure from TS 23.228 [7], AC.11.3.2.2 "Receiving UE centric procedure". The Application Data Channel (ADC) setup between the UE1, UE2 and DC AS is a P2A2P (Peer to Application to Peer) data channel. Therefore, the UE1 and DC AS are mutually authenticated and the transport of information between these entities is secure. The same holds for UE2 and DC AS. As a result, the transport of the Avatar ID1 to the UE2 is secure hop-by-hop via the DC AS.



Figure 6.13.2.1.2-1: Procedures of Receiving UE centric IMS Avatar communication (TS 23.228 [7], AC.11.3.2.2-1)

After Step 2 the DC AS has already authenticated the UE1 and UE2 and it also possesses the UE1 IMPU1 and UE Avatar ID1. In Step 4 the DC AS provides the Avatar ID1 to the UE2. The changes to the procedure in TS 23.228 [7], AC.11.3.2.2 are the following:

Step 4a. As part of the media negotiation step 4, the DC AS retrieves the Avatar ID list from the BAR for UE1 and checks if the UE1 is allowed to access an avatar representation using Avatar ID1.

Step 4b. The solution proposes that the DC AS stores the tuple {(UE1 IMPU1, Avatar ID1), UE2 IMPU2, "Receiving UE centric"} received from UE1 from earlier steps, e.g., Step 4, with the following semantics. The UE1 possesses the Avatar ID1 and it has also expressed a request to set up a receiving UE centric IMS avatar communication with the UE2. This tuple also expresses the implicit permission given by UE1 to UE2 to request and use the avatar representation corresponding to Avatar ID1. This information can be used for authorization purposes later on when the UE2 attempts to access the Avatar of UE1 by providing Avatar ID1' in Steps 5 and 6.

Step 5a. The DC AS checks the provided Avatar ID1' by the UE2 and the stored tuple {(UE1 IMPU1, Avatar ID1), UE2 IMPU2} to determine if the UE2 is allowed to request Avatar ID1 by checking if Avatar ID1 is equal to the provided Avatar ID1'. If the UE2 provided the right Avatar ID1 then the DC AS requests the avatar representation corresponding to the Avatar ID1 by presenting to the BAR the tuple (IMPU1, Avatar ID1) implying that the DC AS requests the avatar representation on behalf of the UE1. Then the DC AS provides the avatar representation to UE2 (in Steps 7, 8) on behalf of UE1.

Step 6a. The BAR optionally checks if the UE1 (IMPU1) is allowed to access the avatar representation corresponding to Avatar ID1 and returns the avatar representation if there is a match.

Step 11a, 11b: When the IMS avatar communication session is terminated the UE2 removes the Avatar ID1 and avatar representation corresponding to the Avatar ID1 and the DC AS removes the tuple {(UE1 IMPU1, Avatar ID1), UE2 IMPU2}. This prevents future re-use of the avatar representation corresponding to Avatar ID1 by the UE2 and any future attempt by the UE2 to retrieve the avatar representation of UE1.

##### 6.13.2.1.3 Security for the Network centric procedure

Figure 6.13.2.1.3-1 depicts the procedure from TS 23.228 [7], AC.11.3.3 "Network centric procedure". The Application Data Channel (ADC) setup between the UE1, UE2 and DC AS is a P2A2P (Peer to Application to Peer) data channel. Therefore, the UE1 and DC AS are mutually authenticated and the transport of information between these entities is secure. The same holds for UE2 and DC AS.



Figure 6.13.2.1.3-1: Procedures of network centric IMS Avatar communication (TS 23.228 [7], AC.11.3.3-1)

This case is similar to the sending UE centric case with respect to authorization with the difference that the MF is accessing the avatar representation from the BAR by providing the tuple (IMPU1, Avatar ID1) in Step 7. Step 7, which was a bidirectional step in TS 23.228 [7], AC.11.3.3, is replaced by Steps 7a (request), 7c (response) and 7b, the actual authorization check proposed by this solution. The changes to the procedure in TS 23.228 [7], AC.11.3.3 are the following:

Step 7b. The BAR checks if the IMPU1 is allowed to access the avatar representation corresponding to Avatar ID1 and returns the avatar representation if there is a match. The UE1 has provided the Avatar ID1 to the MF in one of the steps before Step 7.

Step 13. When the avatar communication session terminates the MF removes the Avatar ID1 and avatar representation(s) used for the rendering.

### 6.13.3 Evaluation

This solution addresses the requirements of KI#2: "Security of IMS based Avatar Communication".

The authentication between the UE and network entities is addressed by the existing bootstrap and application data channel procedures.

The authorization aspects of KI#2 are addressed by the DC AS being a trusted delegate of the UE1 to request from the BAR (on behalf of UE1) the avatar representation corresponding to the Avatar ID1.

The DC AS can retrieve the Avatar list from the BAR for a specific UE and check if the provided Avatar ID is in this list for the specific UE.

The BAR optionally checks according to its provisioned list of IMPUs and Avatar IDs whether the specific UE1 IMPU1 is allowed to access the avatar representation corresponding to Avatar ID1. This authorization check by the BAR is not optional for the case of the network centric rendering in order to make reduce the impact to the system, i.e. either the DC AS or the BAR perform avatar representation access authorization.

The authorization is implicit in the sense that the DC AS and MF are trusted to present to the BAR the UE identifiers and Avatar IDs provided by UE1 and the BAR optionally (sending UE and receiving UE centric rendering) or mandatorily (in the case of network centric rendering) checks if there is a match.

For the case of the receiving UE centric rendering, the fact that the UE1 requests to setup an avatar application session with UE2 with a specific Avatar ID1 implies that the UE1 provides implicit permission to the DC AS to act on behalf of UE1 to request the avatar representation from the BAR and provide it securely to UE2. Moreover, UE1 provides implicit permission to the UE2 to use the avatar representation corresponding to Avatar ID1 by providing the Avatar ID1 to UE2.

Similarly, the fact that the UE1 selects network centric rendering implies that the UE1 provides implicit permission to the MF to retrieve the avatar representation corresponding to Avatar ID1 and render it.

The solution proposes that the Avatar IDs and the avatar representations of the UE1 are removed from the UE2 or the network (MF) for the case of receiving UE centric rendering and the network centric rendering correspondingly.

The authorization solution has minimum impact on DC AS, MF and BAR which need to maintain only allowed lists of UE identifiers and Avatar IDs.

# 7 Conclusions

## 7.1 Conclusions for Key issue #1: Third party specific user identities

For KI#1 the normative work principles from the conclusions in TR 23.700-77 [2], clause 8.4 (Conclusions for KI#4) are followed. Moreover there is an agreed CR for TS 23.228 [7] which specifies in sufficient detail the support for authorization, signing, and verification of third party user identity information in IMS.

As a result the normative work for KI#1 in this document is proposed to be a new clause in TS 33.501 [11] or TS 33.203 [15] which will provide a summary of the new feature, list of security requirements and a reference to the related clauses in TS 23.228 [7].

## 7.2 Conclusions for Key Issue #2: Security of IMS based Avatar Communication

The following principles are concluded for normative work:

1. Any security normative work for this key issue will take the TS 23.228[7], Annex AC.11 in account.

2. Avatar ID sent by the UE1 should be verified by the IMS network about whether it belongs to the UE1.

Editor's Note: Whether there is a need for a token based solution and the potential token details are FFS.

3. e2DCe protection mechanism specified in TS 33.328 [17] is reused for authentication, integrity and confidentiality protection between UE and MF for Avatar ID List downloading and avatar representation downloading via BDC/ADC. As a result there is no need for new normative work for authentication, integrity and confidentiality protection when bootstrap and application data channels are used between two communicating entities

4. Reuse existing security specification in TS 33.328 [17], Annex P.1, for security of aspects of SBA in IMS media control interface, to protect SBA communication between MF/DCSF and DC AS/BAR, or between DC AS and BAR, if the DC AS and BAR are deployed inside of operator’s domain.

Editor's Note: Whether there is an SBA interface between the DC-AS and BAR is in the remit of SA2.

5. Reuse existing security specification in TS 33.501 [11], clause 12 for Protection of the NEF – AF interface, to protect communication between DCSF and DC AS if the DC AS is deployed outside of operator’s domain.

Editor's Note: It is in the remit of SA2 to specify the interfaces between DCSF and DC-AS for the IMS avatar communication and whether NEF is used for control plane messages between the DC-AS and DCSF.

Editor's Note: Protection of communication between MF and DC AS/BAR if the DC AS/BAR is deployed outside of operator’s domain is FFS.

Editor's Note: Protection of communication between DC AS and BAR if one of them is deployed outside of operator’s domain and another is deployed inside of operator’s domain is FFS.

Editor's Note: It is in the remit of SA2 to decide the different combination of cases for the deployment of the DC-AS and BAR with respect to inside/outside the 3GPP operator domain.

NOTE: if both DC AS and BAR are deployed outside of operator’s domain, the security mechanism is out of scope.

Editor's Note: Whether the integrity and privacy of the avatar representation during the transmission should be protected is FFS.

Editor's Note: Further conclusion is FFS.

## 7.3 Conclusions for Key Issue #3: Security and privacy aspects of IMS DC capability exposure

It is concluded to reuse authentication and authorization procedure specified in clause 12 of TS 33.501 [11].

TS 23.228 [7] and the TS 23.502 [16], specify in sufficient detail the IMS Subscribe/Notify Framework Architecture as well as the DC session control handling.

The normative work for KI#3 is proposed to be a new clause in TS 33.328 [17]. This clause will provide a summary of the new feature, a reference to the related clauses in TS 23.228 [7] and TS 23.502 [16] a list of security requirements, a statement that existing security specification in TS 33.501 [11], clause 12 for the NEF-AF interface can be re-used.

Moreover, for the IMS event exposure procedures it can be stated in the normative work that the Nnef\_EventExposure\_Subscribe, Unsubscribe and Notify operations defined for 5GC in clause 4.15.3.2.3 of TS 23.502 [16] are applicable for the Subscriber specific IMS event subscriptions.

Editor's Note: The authorization for non-subscriber specific IMS event subscriptions is FFS.

Editor's Note: The authorization for the IMS DC session control is FFS.

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 |
| 2024-05-30 | SA3#116 | S3-242431 |  |  |  | Version after incorporating changes in: S3-242298, S3-242432, S3-242434, S3-242435, S3-242436, S3-242437, S3-242438, | 0.3.0 |
| 2024-08-29 | SA3#117 | S3-243656 |  |  |  | Version after incorporating changes in: S3-243296, S3-233022, S3-243616, S3-243617, S3-243618, S3-243619, S3-243620, S3-243621, S3-243622, S3-243623, S3-243624, S3-243625, S3-243626 | 0.4.0 |
| 2024-10-24 | SA3#118 | S3-243817 |  |  |  | Version after incorporating changes in: S3-244195, S3-244399, S3-244400, S3-24401, S3-244402, S3-244403. | 0.5.0 |
| 2024-11-21 | SA3#119 | S3-245186 |  |  |  | Version after incorporating changes in: S3-244809, S3-245120, S3-245188, S3-245190, S3-245191, S3-245355. | 0.6.0 |
| 2024-12 | SA#106 | SP-241792 |  |  |  | Presented for information | 1.0.0 |
| 2025-01-23 | SA3#119Adhoc-e | S3-250205 |  |  |  | Version after incorporating changes in: S3-250207, S3-250184, S3-250185, S3-250192, S3-250210. | 1.1.0 |
| 2025-02-27 | SA3#120 | S3-250969 |  |  |  | Version after incorporating changes in: S3-251076, S3-250793, S3-250874, S3-251075, S3-251142. | 1.2.0 |