|  |  |
| --- | --- |
| 3GPP TR 33.790 V0.3.0 (2024-05) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on the security support for the next generation real time communication services phase 2  (Release 19) | |
|  | |
|  | 3GPP-logo_web |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

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

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 8

3.2 Symbols 8

3.3 Abbreviations 8

4 Assumptions 8

4.1 General 8

4.2 Architectural Assumptions and Principles 8

5 Key issues 9

5.1 Key issue #1: Third party specific user identities 9

5.1.1 Key issue details 9

5.1.2 Threats 9

5.1.3 Potential security requirements 9

5.2 Key issue #2: Security of IMS based Avatar Communication 9

5.2.1 Key issue details 9

5.2.2 Threats 9

5.2.3 Potential security requirements 10

5.3 Key Issue #3: Security and privacy aspects of IMS DC capability exposure 10

5.3.1 Key issue details 10

5.3.2 Security threats 10

5.3.3 Potential security requirements 10

6 Solutions 11

6.0 Mapping between key issues and solutions 11

6.1 Solution #1: Signing/verification of third party ID information 11

6.1.1 Introduction 11

6.1.2 Solution details 11

6.1.3 Evaluation 13

6.2 Solution #2: Security of 3rd party specific identities 13

6.2.1 Introduction 13

6.2.2 Solution details 13

6.2.2.1 Solution Description 13

6.2.2.2 How the Originating IMS network invokes the signing on behalf of 3rd party (SIP trunk) 15

6.2.2.3 How the Originating IMS network invokes the signing on behalf of 3rd party (Single SIP registration) 16

6.2.3 Evaluation 18

6.3 Solution #3: Support of Third Party specific User Identities in IMS using STIR/SHAKEN 18

6.3.1 Introduction 18

6.3.2 Solution detail 20

6.3.3 Evaluation 22

6.4 Solution #4: SHAKEN based third-party specific user identities 22

6.4.1 Introduction 22

6.4.2 Solution details 22

6.4.2.1 General procedures 22

6.4.2.2 Alternative authorisation procedure 23

6.4.3 Evaluation 23

6.5 Solution #5: Securing the IMS based avatar communication 24

6.5.1 Introduction 24

6.5.2 Solution details 24

6.5.3 Evaluation 25

6.6 Solution #6: Solution for secure IMS based avatar communication 25

6.6.1 Introduction 25

6.6.2 Solution details 26

6.6.2.1 Network centric IMS avatar call flow 26

6.6.2.2 UE-A centric IMS avatar call flow 27

6.6.2.3 UE-B centric IMS avatar call flow 28

6.6.2.4 UE-A attestation 28

6.6.3 Evaluation 29

6.7 Solution #7: Protect IMS DC based Avatar Communication 29

6.7.1 Introduction 29

6.7.2 Solution details 29

6.7.2.1 Procedure to protect IMS DC based Avatar Communication 29

6.7.3 Evaluation 32

6.8 Solution #8: Security for IMS based Avatar Communication 32

6.8.1 Introduction 32

6.8.2 Solution details 32

6.8.3 Evaluation 35

6.9 Solution #9: Secure IMS DC capability exposure 36

6.9.1 Introduction 36

6.9.2 Solution details 36

6.9.2.1 Procedure of DC AS authorization for DC event subscription 36

6.9.2.2 Procedure of DC AS authorization for data channel session control 37

6.9.3 Evaluation 38

7 Conclusions 38

Annex A (informative): Change history 40

# Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

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

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

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

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

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

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

**should** indicates a recommendation to do something

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

**may** indicates permission to do something

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

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

**can** indicates that something is possible

**cannot** indicates that something is impossible

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

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

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

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

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

In addition:

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

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

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

# Introduction

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

# 1 Scope

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

- IMS third party identity security handling

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

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

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

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

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

[2] 3GPP TR 23.700-77: ""Study on system architecture for next generation real time communication services; Phase 2".

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

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

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

[6] IETF draft-ietf-stir-passport-rcd-26: "PASSporT Extension for Rich Call Data"

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

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

[8] IETF draft-ietf-sipcore-callinfo-rcd-09: "SIP Call-Info Parameters for Rich Call Data".

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

[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".

# 3 Definitions of terms, symbols and abbreviations

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

## 3.1 Terms

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

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

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

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

<ABBREVIATION> <Expansion>

# 4 Assumptions

## 4.1 General

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

## 4.2 Architectural Assumptions and Principles

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

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

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



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

# 5 Key issues

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

### 5.1.1 Key issue details

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

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

### 5.1.2 Threats

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

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

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

### 5.1.3 Potential security requirements

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

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

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

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

### 5.2.1 Key issue details

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

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

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

### 5.2.2 Threats

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

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

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

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

Avatar objects could be used for impersonating a IMS caller.

### 5.2.3 Potential security requirements

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

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

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

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

### 5.3.1 Key issue details

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

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

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

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

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

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

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

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

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

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

### 5.3.2 Security threats

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

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

### 5.3.3 Potential security requirements

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

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

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

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

# 6 Solutions

## 6.0 Mapping between key issues and solutions

Table 6.0-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | 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 |

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

### 6.1.1 Introduction

This solution addresses key issue #1.

### 6.1.2 Solution details

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

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

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

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



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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

### 6.1.3 Evaluation

TBD

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

### 6.2.1 Introduction

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

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

This solution proposes to use the existing Ms reference point and procedures as described in TS 24.229 [4] and STIR/SHAKEN framework [5] while adopting draft-ietf-stir-passport-rcd-26 [6].

### 6.2.2 Solution details

#### 6.2.2.1 Solution Description

The Ms reference point as described in TS 24.229 [4] is used to request signing of a SIP Identity header field and verification of a signed assertion in a SIP Identity header field as shown in Figure 4.2-1. This enables calling number verification using signature verification and attestation information based on the STIR/SHAKEN framework.

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

The main user identity information involved in this solution includes:

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

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

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

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

Examples of Rich Call Data are:

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

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

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

- information related to the location of the caller;

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

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

The types of 3rd party user identities as used in IMS need to be aligned with the definitions in IETF draft-ietf-stir-passport-rcd-26 [6] and include the calling person's name and job title, information related to the organization the caller is associated with and information related to the caller's location. The overall reference architecture is depicted in Figure 4.2-1. The 3rd party (Enterprise) network can be connected to the serving IMS network via UNI (UE to Network Interface) or NNI (Network to Network) interfaces. The serving IMS network handles outbound SIP calls from the Third Party.

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

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

Prerequisites:

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

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

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

NOTE 2: When the 3P ID Server is located outside the IMS operator domain, the access to the 3P ID Server can be secured in the same way as the SIP trunk link between the IMS network and the PBX; i.e., using mutual TLS as defined in Clause S.2.2 of TS 23.228 [7].

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

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. Storing just URL(s) in the HSS avoids potential misusing a Third Party specific user identities that no longer belongs to an UE to initiate IMS calls (e.g., the user uses the identities allocated by a particular company even after leaving it), and possibly frequent updates to the data based on request from the Third Party network and avoids defining Third Party specific data formats in HSS. Nevertheless, the HSS may also store additional data in the subscription of a Third Party subscriber like caller name, organization information, job title, and location information. The URL(s) and possibly other data are fetched from the HSS by the CSCF or IMS AS depending which entity invokes the signing. Optionally, the IMS AS may use the RCD URL received from the HSS to fetch Rich Call Data from a server that can be in the operator domain or external in the Third Party network and provide these data or the RCD URL in SIP signalling (SIP INVITE) towards the terminating party. The fetched Rich Call Data information is used by the Signing AS for signing the RCD PASSporT and by the Verification AS to verify the signed RCD PASSporT.

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

Editor's Note: In case RCD is stored in HSS and URLs are included in the RCD, e.g. URIs of photo and/or logo are data elements of the RCD, whether the data is fetched by source IMS or target IMS based on the URIs is FFS.

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

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

Figure 6.3.2-1: Third Party Identity signing and verification workflow

1. The originating UE sends a SIP INVITE that contains the IMPU of the calling UE and optional Third Party specific user identity (or third party identity).

2. The CSCF forwards the SIP request to the IMS AS.

3. The IMS AS checks with HSS if the calling user (IMPI or IMPU based) is authorized to use the third party identity based on subscription. The association between IMPU/IMPI and third party ID/RCD URL is pre-configured in HSS as subscription data.

4a. The IMS AS/CSCF retrieves Rich Call Data (RCD) information of the third party identity from HSS. HSS may return RCD URL pointing to the RCD on Web servers or concrete RCD, like caller name, job title, organization, and location information, etc., based on deployment option.

NOTE: If HSS returns concrete RCD to the IMS AS in this step, HSS should fetch the RCD from the third party database in advance based on RCD URL/third party identity associated to the IMPU/IMPI.

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

4b. Optionally, the IMS AS/CSCF may retrieve RCD of the third party identity from third party database based on the third party identity or RCD URL.

5. The IMS AS/CSCF calls STI-AS to sign the SIP header, e.g. call-info, which including RCD URL or RCD of the third party identity.

6. The STI-AS returns the signed SIP header back to the IMS AS/CSCF.

7. The IMS-AS/CSCF forward the SIP INVITE to the terminating IMS subsystem which including signed RCD URL or RCD of the third party identity.

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

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

10. The terminating IMS subsystem sends SIP INVITE to terminating UE which including the RCD if verification is successful in step 8. Otherwise, terminating IMS subsystem may send SIP INVITE to terminating UE without including RCD.

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

### 6.3.3 Evaluation

TBD

## 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.

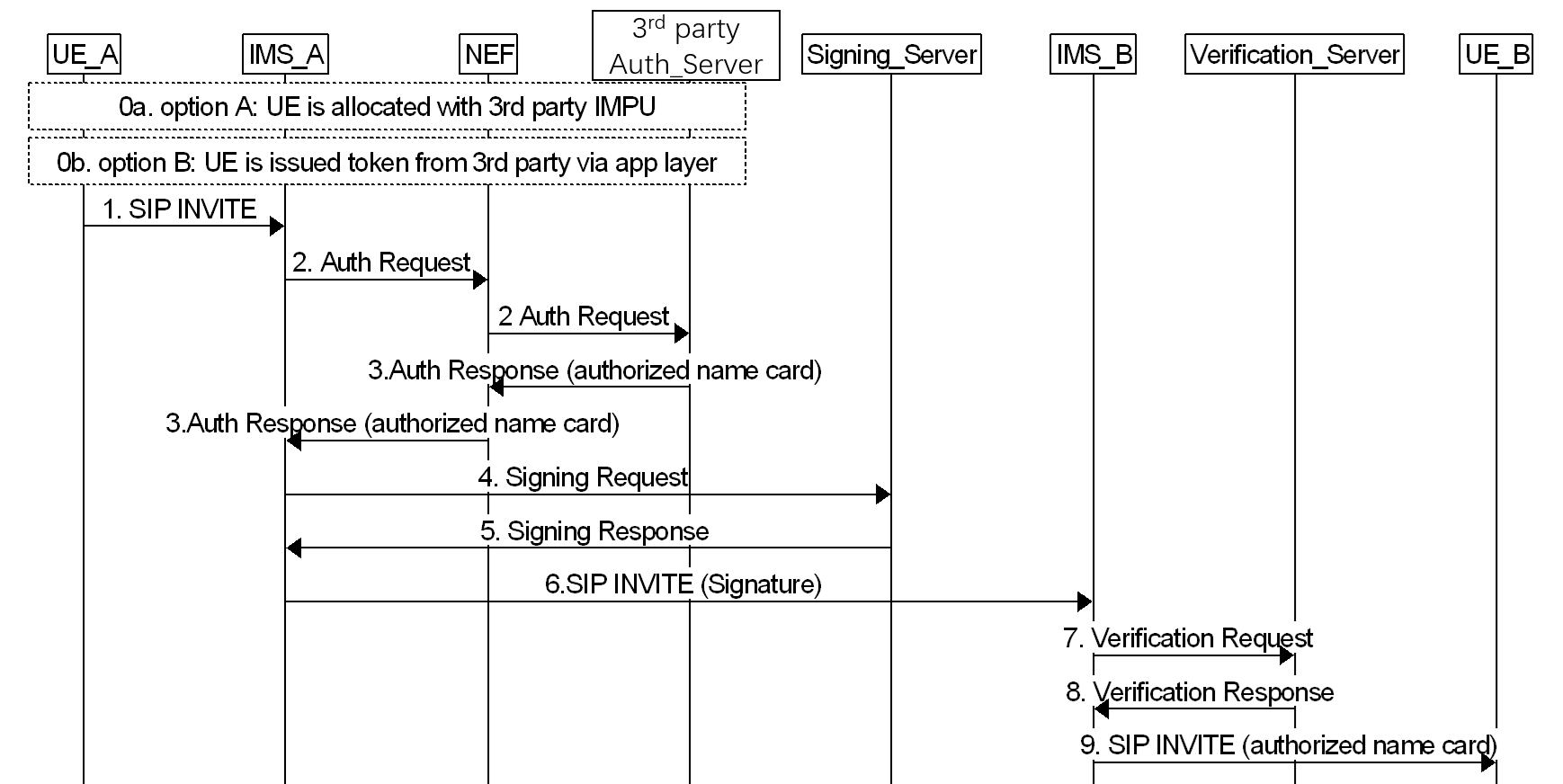


Figure 6.4.2-1: Call flow for using third party identity

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, option A should be used since the legacy UE can only use IMPU.

1. The originating UE or the PBX creates a SIP INVITE with:

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

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

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

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

Editor's Note: Alignment with the SA2 TR 23.2700-77 and exposure mechanisms is FFS.

3. The third party Authorization Server authorizes the request and creates an enterprise name card for the user, which is going to be delivered in the SIP header. For option B, the authorization can be done using the token received in the INVITE as mentioned above or as described in clause 6.4.2.2.

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].

Editor's Note: Dynamic name card details are FFS.

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 sever may initiate an authentication procedure with UE based on local policy upon receiving the request from IMS. After successful authentication, the authorization sever can create an enterprise name card for the user. The authentication between UE and the authorization server is out of scope of this study.

### 6.4.3 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], several solutions are proposed to support the network-based avatar communication by media capability invocation. Specifically, the base avatar models are stored in the Base Avatar Repository (BAR), and the XR AS obtains the Avatar ID, which contains the Avatar URL, from the BAR. The UE sends the Avatar ID to the XR Application Server (XR AS). The MF/MRF downloads the base avatar model based on the Avatar URL received from the XR AS.

* The XR Application Server is responsible for service control related to avatar communication, including base avatar model management, access control, avatar communication session media control, and so on.
* The Base Avatar Repository is used to store and retrieve the avatar models. 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/MRF) that accesses the base avatar models, preventing the unauthorized UE/IMS entities from accessing the base avatar models and thus impersonating the IMS caller/callee.

### 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/MRF from downloading the wrong base avatar model based on other UE's Avatar URL, the solution requires the MF/MRF to download the base avatar model based on the token received from the UE.



Figure 6.5.2-1: Authorization procedure for Avatar communication

Step 0a. During the BDC (Bootstrap data channel) and ADC (Application data channel) procedure, UE1 chooses the Avatar ID, and then generates the token including the Avatar ID and JWS (JSON Web Signature). After that, UE1 sends the token to the MF/MRF in this step or before Step 3.

Editor's Note: Whether the UE should send the token to MF/MRF before Step 1 is FFS.

Editor's Note: The details of token handling is FFS.

- Bootstrap data channel: 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 [7].

- Application data channel: A data channel within an IMS session used to transfer data of data channel applications between UEs or between the UE and the network [7].

Step 0b. UE1 sends the Avatar ID to XR AS.

Step 1. XR AS determines whether the received Avatar ID is in the UE's Avatar ID list.

Editor's Note: How the XR AS determines that the received Avatar ID is in the UE's avatar ID list is FFS.

Step 2. If the received Avatar ID is not equal to any Avatar ID in the UE's Avatar ID list, XR AS will send an error message to the UE1.

Steps 3, 4. If the Avatar ID is equal to one of the Avatar ID in the UE's Avatar ID list, XR AS sends the Avatar ID to the MF/MRF via the DCSF.

Step 5. MF/MRF requests to download the avatar model from the BAR, including parameters of token and Avatar ID.

Step 6. BAR verifies the token by checking the JWS in the token, based on the UE's certificate, which can be pre-configured or transmitted to the BAR. BAR also checks whether Avatar ID in the request equals to that in the token.Step7. BAR sends the avatar model downloading response message to the MF/MRF. If the verification in Step 6 is passed, the message includes the base avatar model, otherwise the message includes the error code, indicating that the token verification is not passed.

Step8. The subsequent procedure continues.

Editor's Note: Whether the token should contain the session related information is FFS.

Editor's Note: Alignment with SA2 TR 23700-77 conclusion is FFS.

Editor's Note: Whether there is direct interface between MF/MRF and BAR is FFS.

Editor's Note: When BAR is outside of IMS network, whether it is up to implementation is FFS.

Editor's Note: Whether the token needs to be verified by XR AS is FFS.

### 6.5.3 Evaluation

TBD

## 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 meida can be performed by network, UE-A, or UE-B, which are called network centric IMS avatar call, UE-A centric IMS avatar call, and UE-B centric avatar call, respectively.

In this solution, only authorized entity from UE-A can access and retrieve the UE-A's avatar object which is stored in a data storage called Ditigal Asset Container (DAC). This solution proposes to use UE-A's attestation for the security procedure of IMS based avatar communication.

In this solution, it is assumed that DAC has UE-A's public key to verify the signature in UE-A's attestation, with UE-A's avatar object and 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, UE-B also performs the operation same as UE-A described in the procedure.

### 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 UE-A initiates an IMS session and establishes audio and video session connections with the UE-B. The bootstrap channel is established for both the UE-A and UE-B. UE-A obtains UE-A's avatar id(s) in this step.

2. The UE-A performs the XR media rendering negotiation with the XR Application Server. The UE-A generates and sends UE-A's attestation to the XR Application Server. The UE-A's attestation consists of Avatar ID, identity of the XR AS, rendering option (i.e., network centric), expiration time, signature generated by using UE-A's private key, as described in clause 6.6.2.4 of this document.

3. The UE-A decides to use network centric rendering of an avatar object.

4. Application data channel is established between UE-A and IMS network, and media re-negotiation may be performed.

5. XR Application Server requests avatar object using UE-A's attestation.

6. After DAC retrieves UE-A’s public key based on avatar ID in UE-A’s attestation, DAC verifies the signature in UE-A's attestation using the UE-A's public key. If the verification is successful and the identity of XR AS in the UE-A's attestation is same as that of the XR Application Server which requested in step 5, the DAC responds with the UE-A's avatar object.

Editor's Note: Whether the avatar object should be protected is FFS.

7. The XR Application Server sends the avatar object to MF/MRF and requests rendering of the avatar.

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

9. The MF/MRF performs the rendering using the UE-A's avatar object and the data received from UE-A in step 8.

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

11. The rendered avatar media is sent back to the UE-A as feedback.

#### 6.6.2.2 UE-A centric IMS avatar call flow



Figure 6.6.2.2-1 UE-A centric IMS avatar call flow

1. The UE-A initiates an IMS session and establishes audio and video session connections with the UE-B. The bootstrap channel is established for both the UE-A and UE-B. UE-A obtains UE-A's avatar id(s) in this step.

2. The UE-A performs the XR media rendering negotiation with the XR Application Server. The UE-A generates and sends UE-A's attestation to the XR Application Server. The UE-A's attestation consists of Avatar ID, identity of the XR AS, rendering option (i.e., UE-A centric), ephemeral public key of UE-A, expiration time, signature generated by using UE-A's private key, as described in clause 6.6.2.4 of this document.

3. The UE-A decides to use UE-A centric rendering of an avatar object.

4. Application data channel is established between UE-A and IMS network, and media re-negotiation may be performed.

5. XR Application Server requests avatar object using UE-A's attestation.

6. After DAC retrieves UE-A’s public key based on avatar ID in UE-A’s attestation, DAC verifies the signature in UE-A's attestation using the UE-A's public key. If the verification is successful and the identity of XR AS in the UE-A's attestation is same as that of the XR Application Server which requested in step 5, the DAC generates ephemeral public/private key pair and protects the UE-A's avatar object using the session key generated by ephemeral public key of UE-A included in the UE-A's attestation and ephemeral private key of DAC. The DAC responds with the protected UE-A's avatar object and ephemeral public key of the DAC.

7. The XR Application Server sends the protected avatar object and ephemeral public key of the DAC to UE-A, and requests rendering of the avatar.

8. The UE-A generates session key using the ephemeral public key of the DAC and the ephemeral private key of UE-A. UE-A verifies the protected avatar object using the session key and performs the rendering.

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

#### 6.6.2.3 UE-B centric IMS avatar call flow



Figure 6.6.2.3-1 UE-B centric IMS avatar call flow

1. The UE-A initiates an IMS session and establishes audio and video session connections with the UE-B. The bootstrap channel is established for both the UE-A and UE-B. UE-A obtains UE-A's avatar id(s) in this step.

2. The UE-A performs the XR media rendering negotiation with the XR Application Server and UE-B. In this step, UE-A obtains UE-B's ephemeral public key. The UE-A generates and sends UE-A's attestation to the XR Application Server. The UE-A's attestation consists of Avatar ID, identity of XR AS, rendering option (i.e., UE-B centric), ephemeral public key of UE-B, expiration time, signature generated by using UE-A's private key, as described in clause 6.6.2.4 of this document.

2. The UE-A decides to use UE-B centric rendering of an avatar object.

4. Application data channel is established between UE-A and IMS network, and media re-negotiation may be performed.

5. XR Application Server requests avatar object using UE-A's attestation.

6. After DAC retrieves UE-A’s public key based on avatar ID in UE-A’s attestation, DAC verifies the signature in UE-A's attestation using the UE-A's public key. If the verification is successful and the identity of XR AS in the UE-A's atteststion is same as that of the XR Application Server, the DAC generates ephemeral public/private key pair and protects the UE-A's avatar object using the session key generated by ephemeral public key of UE-B included in the UE-A's attestation and ephemeral private key of DAC. The DAC responds with the protected UE-A's avatar object and ephemeral public key of the DAC.

7. The XR Application Server sends the protected avatar object and ephemeral public key of the DAC to UE-B, and requests rendering of the avatar.

8. The UE-A sends the data for rendering to UE-B.

9. The UE-B generates session key using the ephemeral public key of the DAC and the ephemeral private key of UE-B. UE-B verifies the protected avatar object using the session key and performs the rendering using the UE-A's avatar object and the data for rendering received from UE-A in step 8.

Editor's Note: When DAC and XR AS are outside of IMS network, whether it is upto implentation is FFS.

Editor's Note: The alignment with SA2 conclusions from TR 23.700-77 [2] is FFS.

Editor's Note: The details of how the DAC/XR AS verifies the claimed avatar ID based on UE generated attestation are FFS.

Editor's Note: The need for confidentiality protection of the avatar information transportation is FFS.

#### 6.6.2.4 UE-A attestation

UE-A's attestation is generated by UE-A and it consists as follows:

Table 6.6.2.4-1 UE-A attestation

|  |  |
| --- | --- |
| Parameter | Description |
| Avatar ID | REQUIRED. ID used to retrieve UE-A's avatar object. |
| Identity of XR AS | REQUIRED. The identifier of the XR Application Server that requests UE-A's avatar object to DAC. |
| Rendering option | REQUIRED. One of the followings: network centric, UE-A centric, or UE-B centric |
| Ephemeral public key of UE-A | OPTIONAL. This is included when the rendering option is UE-A centric. DAC uses ephemeral public key of UE-A and ephemeral private key of DAC to protect the UE-A's avatar object. The protected avatar object is sent to UE-A and it is end-to-end protected between DAC and UE-A. |
| Ephemeral public key of UE-B | OPTIONAL. This is included when the rendering option is UE-B centric. DAC uses ephemeral public key of UE-B and ephemeral private key of DAC to protect the UE-A's avatar object. The protected avatar object is sent to UE-B and it is end-to-end protected between DAC and UE-B. |
| Expiration time | REQUIRED. The expiration time of the UE-A attestation. |
| Signature | REQUIRED. Signature generated by UE-A using UE-A's public key and the parameters in the attestation. |

### 6.6.3 Evaluation

TBD

## 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 object (or representation/metadata) for avatar media rendering. An avatar object is stored in a data storage entity (called as Digital Asset Container (DAC). The avatar object 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 object from the DAC based on CAPIF, NEF or SBI security defined in TS 33.122 and 33.501.

### 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, and perform authentication and authorization based on CAPIF/NEF/SBI security when an avatar object consumer accesses the avatar object from the DAC. SIP security defined in 33.303 and DC integrity and confidentiality protection defined in 33.228 can be used to protect avatar id and avatar object transmitted through IMS network.

Editor's Note: SHAKEN framework can be used sign and verify the avatar-id. Other options are FFS.

Editor's Note: Alignment with SA2 is FFS

#### 6.7.2.1 Procedure to protect IMS DC based Avatar Communication



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. UE-A also downloads the avatar application and Avatar-id(s) through a BDC.

Editor's Note: How the UE-A is configured or is aware of the Avatar-id is for FFS.

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, 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 centric 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. A UE token is included in the DC establishment messages. The UE token is generated by UE to sign UE IMS id (IMPU) and XR application server (XR AS) id with UE certificate. The fingerprint of the UE certificate can be 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 DAC.

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 centric avatar rendering.

7. Before retrieving the avatar metadata from DAC, 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 DAC. 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 fingerprint 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 and policy configured locally or got from HSS. The access token includes application id, DAC instance id, Avatar-id and operations on the avatar metadata associated to the Avatar-id.

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

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

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

Editor's Note: the usage of UE token and how it is used by the NEF/CAPIF CF/NRF are FFS.

8. The XR Application Server retrieves the avatar metadata using the Avatar-id from DAC.

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

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 metadata 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 then may tamper the avatar metadata.

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 metadata, 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 may not be established or may be established without avatar media.

Editor's Note: The procedure of Avatar Communication depends on SA2's conclusion.

Editor's Note: The procedure addressed security aspects of DC based IMS Avatar Communication on network centric rendering. Security aspects of DC based IMS Avatar Communication on UE centric rendering and non-DC based IMS Avatar Communication are FFS.

### 6.7.3 Evaluation

TBD

## 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.

Editor's Note: Whether this procedure is applicable to DC based avatar communication is FFS.

Editor's Note: Alignment with TR 23.700-77 terminology is FFS.

### 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.

Editor's Note: How is UE authorized to use avatars is FFS

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 1: 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 2: 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 3: 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.

Editor's Note: It is FFS how the avatar repository determines whether an avatar model/data can be returned to the IMS system.

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 4: 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.

Editor's Note: It is FFS when does the originating IMS system retrieve 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 may 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.

Editor's Note: It is FFS 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.

Editor's Note: Further evaluation is FFS.

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

### 6.9.1 Introduction

The solution addressed KI#X 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. Without proper security control, the IMS DC services may be illegally used by malicious application function/server (AF/AS), e.g. the malicious AF may eavesdrop or manipulate IMS DCs, the malicious AF may launch DoS attack with updating/terminating an ongoing DC, and cause interruption on the IMS communication of an end user, privacy of IMS user may also be 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. 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/UDM or NEF, and the authorization decision will be made by NEF/DCSF based on DC AS properties, DC related services and other conditions.

Editor's Note: Alignment with SA2 is FFS

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

Precondition:

- Authorization policies are provisioned in NEF/HSS/UDM.



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/UDM.

3. NEF makes authorization decision and grants permission for the request based on the policies and user consent.

4. NEF sends DC event subscription request to DCSF.

5. NEF receives response from DCSF.

6. NEF sends response to the DC AF/AS

7. NEF receives event notification from DCSF.

8. NEF sends the notification to the DC AF/AS. The notification may be 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/UDM.

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

NOTE 1: NEF may check 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 sends DC session control request to DCSF. DCSF triggers IMS AS to re-invite the IMS call to include DC offer with UEs, and reserve DC resource with MF if needed.

6. NEF receives response from DCSF.

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

Editor's Note: The procedure of IMS DC capability exposure depends on SA2's conclusion.

### 6.9.3 Evaluation

TBD

# 7 Conclusions

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

Annex A (informative):  
Change history

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