**SA WG3 Meeting S3#116 Draft\_S3-242436r1**

**Jeju, Korea 20 - 24 May 2024** revision of S3-242346

**Source: Nokia, Nokia Shanghai Bell, CableLabs**

**Title: new solution for Security of IMS based Avatar Communication**

**Document for: Approval**

**Agenda Item: 5.2**

**Work Item / Release: FS\_NG\_RTC\_Ph2/Rel19**

# 1 Decision/action requested

***Approve the solution added to TR 33.790***

# 2 References

[1] 3GPP TR 23.700-77 Study on system architecture for next generation real time communication services Phase 2

[2] 3GPP TR 33.790 Study on the security support for the Next Generation Real Time Communication services phase 2

# 3 Rationale

The contribution proposes a new solution for secure IMS DC capability exposure.

# 4 Detailed proposal

All content in the change part is new.

\* \* \* \* First change\* \* \* \*

# 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*.

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

\* \* \* \* Next change \* \* \* \*

## 6.x Solution #x: Protect IMS DC based Avatar Communication

### 6.X.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.X.2 Solution detail

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.

Editorial Notes: SHAKEN framework can be used sign and verify the avatar-id. Other options are FFS.

Editor's Note: Alignment with SA2 is FFS

#### 6.x.2.1 Procedure to protect IMS DC based Avatar Communication



Figure 6.x -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.

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/UDM or locally based on subscription data retrieve from HSS/UDM 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 checks if the UE-A is allowed to use the Avatar-id for the application by verifying the signed Avatar-id. If successful, it forwards the Avatar-id to UE-B.

Editor's note: how to provision subscription data with Avatar-id is out of scope of this workflow.

NOTE 1: 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 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.

5(Optional). IMS AS initiates a media re-negotiation request with UE-A by exchanging the Avatar-id via the application DC, to connect 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 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.

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/UDM. The access token includes application id, DAC instance id, Avatar-id and operations on the avatar metadata associated to the Avatar-id.

NOTE 2: 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.

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

8.

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 3: the certificate used to sign the avatar can be preconfigured in XR AS.

Editor's note: 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 4: the certificate used to sign the avatar can be preconfigured in the MF.

Editor's note: 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 5: If exception happened in security steps, the IMS session may not be established or may be established without avatar media.

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

Editor's Notes: 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.X.3 Evaluation

TBD

\* \* \* \* End of changes \* \* \* \*