**3GPP TSG-SA WG4 Meeting #132S4-250873\_r01**

**Fukuoka, Japan, 19 - 23 May 2025**

**Source: Samsung Electronics Co., Ltd.**

**Title: [AvCall-MED] On base avatar registration via IMS network**

**Agenda item: 10.7**

**Document for: Agreement**

**1. Introduction**

This contribution provides a call flow on base avatar registration using defined interfaces in the IMS network.

**2. Discussion**

There has been much discussion related to the management of users’ base avatars in particular with a possible direct interface between the UE and BAR. Such an interface however has not been defined by SA2 (which deemed it out of scope of their work), and would be only an informative guideline. Still, the use of BAR involves the use of related SA2 defined parameters such as avatar ID. As such, the registration of a base avatar into the BAR via IMS network and interfaces is needed for the secure assignment of such parameters to the user’s base avatar.

Assuming an avatar native or web application with functionality to register a user’s base avatar to BAR, a base avatar can be uploaded and registered to BAR either via the bootstrap data channel or application data channel. Assigning an avatar ID to the base avatar data during registration allows the BAR to guarantee the uniqueness of the registered base avatar ID. Encrypting the base avatar before upload using the UE's private key and then allowing the BAR to generate a HASH code from the decrypted base avatar data (using a public key) ensures both the integrity of the data and its security throughout the registration process.

**3. Proposal**

It is proposed to agree the following additions to the latest version of the CR for 3GPP TR 26.264.

\* \* \* First Change \* \* \* \*

## A.1.7 Base Avatar Registration via IMS Network



Figure 25: IMS base avatar registration flow

1. UE creates the base avatar.

Base avatar registration request (the use of an avatar ID assigned by the BAR is required for the secure upload of the base avatar by the UE):

2. UE requests the registration of its base avatar to MF/DC AS via bootstrap or application data channel.

 NOTE: The UE may share its public key with either DC AS or BAR before this step.

3. DC AS forwards the registration request to BAR.

4. BAR assigns a unique Avatar ID for the UE and URL for the base avatar according to the UE identifier known via the DC AS..

5. BAR sends a registration response containing the Avatar ID and URL to the UE via MF/DC AS.

6. The UE inserts the assigned Avatar ID into the Base Avatar data created from step 1.

 NOTE: the avatar storage is assumed to be a trusted component.

Editor’s Note: Requests for other base avatar management functionalities to be defined.

Base avatar upload:

[7. Upload request from avatar app to avatar storage.

8. Avatar storage creates a hash code for the unencrypted base avatar data and encrypts the base avatar data with UE1’s private key.

9. Avatar storage delivers the encrypted base avatar data to BAR via MF using the URL received in step 5.

10. BAR registers the base avatar data under the UE’s identifier, decrypts the base avatar data with the UE’s public key and creates a verification hash code.

 NOTE: The generated hash code serves as a confirmation that the BAR successfully received and decrypted the base avatar data.

11. BAR delivers the verification hash code to the UE.

12. Avatar storage verifies the received hash code.

13. Avatar storage sends a response to the avatar app on the completion of the upload and registration of the base avatar to BAR.]

Editor’s Note: Bracketed text contains security aspects related to SA3, and requires their opinion/feedback.

\* \* \* End of Changes \* \* \* \*