**3GPP TSG-SA3 Meeting #119 draft\_S3-245289-r1**

**Orlando, US, 11 – 15 November 2024**

**Source: Samsung**

**Title: [TR 33.721] Update to solution#6**

**Document for: Approval**

**Agenda Item: 5.18**

# 1 Decision/action requested

***It is proposed to approve this pCR to update solution#6 in TR 33.721.***

# 2 References

[1] 3GPP TR 33.721 ' Study on security aspects of 5G Mobile Metaverse services'

# 3 Rationale

It is proposed to approve this pCR to update solution#6 in TR 33.721. This pCRs add details on procedure for access token request/response deleting the corresponding EN related to it.

For the below EN, if the VAL client has received authorization from the SEAL server to download the avatar it is difficult to prevent the mentioned threat, but it is understood that with the authorization there is a trust with the VAL client. Further no such use case of direct transfer of downloaded avatar is discussed so far. It is only possible if the VAL client goes malicious.

Further, if there is a network side involvement the network will be able to detect that an unauthorized/un-allowed user is pretending to use the avatar. With this understanding it is suggested to delete the below EN.

Editor’s Note: The threat that the VAL client shares the downloaded avatar to another VAL client not in the user list is FFS.

Further, evaluation for the solution is added.

# 4 Detailed proposal

\*\*\* Start Change \*\*\*

## 6.6 Solution #6: Digital asset request validation

### 6.6.1 Introduction

This solution addresses key issue#3. In this solution it is assumed that the SEAL security procedure is re-used for user authentication and authorization as specified in 5.2 of TS 33.434 [4]. Further, it is proposed that the access\_token claims include the allowed user related information to authorize the avatar or digital asset download request from the VAL Client/SEAL Client/VAL Server.

In this solution, it is proposed that the SEAL Server (Digital Asset Container Management) digitally signs the requested avatar object using the private key, obtained as part of key provisioning procedure defined in TS 33.434 [4].

### 6.6.2.1 Access token request/response



**Figure 6.6.2.1-1: Updated VAL user authentication from TS 33.434 [4]**

Figure 6.6.2.1-1 describes the VAL Authentication Framework using the OpenID Connect protocol when using HTTPS as specified in TS 33.343 [4]. Additionally, at step 5a the SIM-S gets the Avatar/digital asset consumer list from the SEAL server (DACM).

NOTE: Creation of user list or the asset or avatar profile in SEAL Server (DACM) is not in scope of this solution.

The VAL profile as specified in table A.2.2.3-1 in TS 33.343 [4] is further extended with the additional claims based on the VAL service i.e., metaverse service as follows:

Table 6.2.2.1-1: Access token VAL claims

|  |  |
| --- | --- |
| Parameter | Description |
| SKeyProv | OPTIONAL for SEAL. The SKeyProv parameter shall be present when the VAL Server SKM-C is authorized to provide key material to the KMS. |
| Digital\_profile | OPTIONAL. A JSON string containing a space-separated list of allowed User(s). |

### 6.6.2.2 Solution details



**Figure 6.6.2.2-1: Digital asset request validation**

1. The VAL Client/SEAL Client/VAL Server sends an avatar or digital asset download request to the SEAL Server (DACM) function with the Avatar ID, GPSI/External ID of the UE. The request also includes the access token.

2. The SEAL Server (DACM) function checks the authorization of the VAL Client/SEAL Client/VAL Server based on the Avatar ID, GPSI/External ID of the UE present in the request message against the allowed user list in the access token to perform the operation. If successful, the SEAL Server (DACM) function performs the media adaptation as per the request on the avatar object/media.

3. The SEAL server function sends a response to the VAL Client/SEAL Client/VAL Server indicating success or failure of the operation. If successful, the avatar object/media/base avatar is included in the response, the SEAL Server (DACM) returns digitally signed avatar object/media/base avatar using the keys obtained from SEAL KM Server. The VAL Client/SEAL Client/ VAL Server which sent the download request if in possession of the required public key would be able to verify the digital signature in the avatar object/media/base avatar for its use.

Editor’s Note: Necessity of access token at step 1 for authorization is FFS.

### 6.6.3 Evaluation

This solution addresses the security requirements of key issue#3. In this solution it is assumed that the SEAL security procedure is re-used for user authentication and authorization as specified in 5.2 of TS 33.434 [4]. Further, the access\_token claims include the allowed user related information to authorize the avatar or digital asset download request from the VAL Client/SEAL Client/VAL Server.

In this solution, it is proposed that the SEAL Server (Digital Asset Container Management) digitally signs the requested avatar object using the private key, obtained as part of key provisioning procedure defined in TS 33.434 [4].

Editor’s Note: Further evaluation is FFS.

\*\*\* End of Change \*\*\*