**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250088-r1**

**Online, Electronic meeting, 13 -16 January 2025**

**Source: Samsung**

**Title: Updates to solution#6**

**Document for: Approval**

**Agenda item: 5.18**

**Spec: 3GPP TR 33.721**

**Version: 0.5.0**

**Work Item: FS\_Metaverse\_Sec**

**Comments**

It is proposed that the access token can optionally include the list of allowed user. Irrespective of that an access token is presented to the DAC for service authorization.

**Proposed Changes**

\* \* \* First 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].

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) to verify the mapping between allowed user and the metaverse services based on the digital asset profile.

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

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |

#### 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 to authorize the requestor.

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 locally stored 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.

### 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 authentication and authorization as specified in 5.2 of TS 33.434 [4].

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 Changes \* \* \* \*