**3GPP TSG-SA3 Meeting #119AdHoc-e Draft\_S3-250151-r1**

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Update sol#9 on authenticate and authorize DA client to access a digital asset**

**Document for: Approval**

**Agenda item: 5.18**

**Spec: 3GPP TR 33.721**

**Version: 0.5.0**

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

**Comments**

<Proposals, reason for change, abstract, comments if necessary (optional)>

The contribution proposed to update solution#9 of the TR on authenticate and authorize DA client to access a digital asset, to address the ENs, and add evaluation for the solution.

As association between UE subscriber and user is not specified in TS 23.438, replace subscriber with user, VAL user, Owner user or Allowed user to align with the TS 23.438.

In case the resource owner is associated with a UE and can be identified by CCF, the CCF may check with the ROF in the UE for user authorization.

**Proposed Changes**

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

<Proposed change in revision marks>

## 6.9 Solution #9: authenticate and authorize VAL server/client to access digital asset

### 6.9.1 Introduction

This solution addresses Key Issue #3 on Security aspects of digital asset container in 5G.

Avatar and digital asset support, including digital asset avatar management and discovery, is discussed in Key issue #3 in TR 23.700-21[2]. The corresponding requirements were defined in clause 5.4 of the TR 23.700-21[2] which include, for example, subject to operator policy, regulatory requirements and user consent, the metaverse enablement service shall provide digital asset management mechanisms as follows:

- to create, update, retrieve, delete and discover digital assets securely.

- to manage associations between digital assets and user identifiers.

- to allow an authorized third party to manage digital asset(s) associated with a user.

Correspondingly, KI#3 on Security aspects of digital asset container in 5G was described in TR 33.721 which requires 5G system to authenticate and authorize a digital asset service consumer to access the digital asset(s) in a digital asset container.

Architecture, procedures and information flows for digital asset service to support mobile metaverse services are specified in TS 23.438 [8]. Especially, figure 6.2-2 of TS 23.438 [8] illustrates the DA architecture to support Metaverse services using CAPIF architecture.

Users can be associated with one or more digital assets like Avatars, software licenses, files, etc. Applications like mobile metaverse services can utilize the digital assets related to users, and the users can benefit from having the use of their digital assets between the various metaverse applications/platforms in an interoperable way.

This solution aims to authenticate and authorize a VAL client (a.k.a DA client) or VAL server to access digital asset(s) based on CAPIF.

### 6.9.2 Solution details



Figure 6.9.2-1 Procedure to authorize VAL\_C/VAL\_S to access digital asset

Precondition:

- Digital asset client (DA client/APIInvoker), CAPIF core function (CCF), digital asset DA server (DA server/AEF) are preconfigured with certificates and trust anchor for TLS based mutual authentication.

- CAPIF core function (CCF) is preconfigured with authorization policies for API Invokers, which may define authorization policies that what AEF services can be accessed by the API Invokers.

- Digital asset is created and stored in DA server which may include authorization information provisioned by the owner of the digital asset, refer to clause 7.2 of TS 23.438 [8] for the detail information in DA profile.

Procedure:

1. VAL server/client (or API invoker) is onboarded successfully and CAPIF-1E authentication is performed with CCF. The authorization polices for the API invoker may be updated based on the API invoker profile.

2. VAL server/client sends Access Token Request to CCF to update/retrieve/delete digital asset, the request includes client id, and optional digital asset identifier .

3. CCF checks if the VAL server/client is allowed to access digital asset services based on preconfigured authorization policies for the API invoker or updated policies in step 1.

4. If so, based on the deployment option, CCF may check if authorization information associated to the digital asset identifier existed locally. If not, CCF locates corresponding DA server based on API type, location, UE information, digital asset identifier, etc., and performs CAPIF-3 authentication with the DA server.

5. Optionally, CCF sends request to the DA server to get authorization information of the digital asset.

6. DA server returned authorization information of the digital asset based on the DA profile created in precondition step.

7. CCF stores the authorization information of the digital asset, and checks if the VAL server/client, is allowed to update/retrieve/delete the digital asset based on allowed application list .

8. Based on the policy, CCF may ask authorization from the resource owner based on RNAA framework in case the resource owner is associated with a UE which can be identified by CCF.

Editor’s Note: How CCF identifies the UE based on resource owner user id is FFS.

9. If the VAL server/client is allowed to update/retrieve/delete digital asset, CCF sends access token to the VAL server/client which includes authorized operations and parameters.

10. After received access token for accessing of digital asset, the VAL server/client performs CAPIF-2E authentication with DA server.

11. VAL server/client sends DA update/retrieve/delete request to DA server which includes access token besides other parameters.

12-13. DA server verifies the access token and proceeds the request accordingly and returns the result to the VAL server/client.

Note: Instead of retrieving authorization information of the DA from DA server in step 4 and 8, the CCF may only authorize the VAL server/client based on preconfigured/updated local authorization policies and include related permissions in the scope of the access token, and DA server may further authorized the access based on authorization information of the required DA.

### 6.9.3 Evaluation

The solution addresses requirements of Key issue #3 to support authorizing DA client to manage digital asset container in 5G.

DA server, DA client, CCF need to enhance to support authorization of DA access. Especially DA server enhances to enable CCF to retrieve authorisation policies of a digital asset.

RNAA is reused for getting authorization from the resource owner in case the resource owner is associated with a UE which can be identified by CCF

Editor’s Note: How CCF identifies the UE based on resource owner user id is FFS.

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