**3GPP TSG-SA3 Meeting #119AdHoc-e Draft\_S3-250150-r1**

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Update sol#8 on authenticate and authorize DA client to create 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#8 of the TR on authenticate and authorize DA client to create 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.

**Proposed Changes**

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

<Proposed change in revision marks>

## 6.8 Solution #8: authenticate and authorize DA client to create a digital asset

### 6.8.1 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 were 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 digital asset client, on behalf of a VAL user, to create a digital asset based on CAPIF.

### 6.8.2 Solution details





Figure 6.8.2-1 Procedure to authorize digital asset client for DA creation

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.

- The user behind the UE has been identified and authenticated by the DA server .

Editor’s Note: How DA server authenticates the user is FFS.

Procedure:

1. DA client, on behalf of a user, is onboarded successfully and CAPIF-1E authentication is performed with CCF.

2. DA client sends Access Token Request to CCF for create digital asset service, the request includes client id, , optional digital asset type (e.g. avatar).

3. CCF checks if the DA client is allowed to create related digital asset based on client/API invoker profile and corresponding authorization policies.

4. If the DA client is allowed to create digital asset, CCF sends access token to the DA client which includes authorized operations for the DA client.

5. After received access token for creation of digital asset, the DA client performs CAPIF-2E authentication with DA server.

6. DA client sends DA creation request to DA server which includes access token besides other parameters such as client id, user id, digital asset type (e.g. avatar) and digital asset profile parameters.

7. DA server verifies the access token.

8. If successfully verified the access token, DA server creates digital assets according to DA profile, which includes DA type (e.g. avatar), authorization information (e.g. owner user which is set to the user id in the request, allowed applications, allowed users, Metaverse service providers, location, expire time, etc.).

9. DA server returns digital asset identifier to the DA client.

### 6.8.3 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 creation.

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