**3GPP TSG SA WG 1 Meeting #104 S1-xx**

**Chicago, USA, 13 - 17 November 2023** *(revision of S1-xx)*

**Source: China Telecom, Huawei, Samsung**

**pCR Title: 22.156 pCR 5.2.3 Digital asset management**

**Draft Spec: TS 22.156**

**Agenda item: 7.3.2**

**Document for: Approval**

**Contact: Yinglin Chen <chenyl37@chinatelecom.cn>**

*Abstract: This pCR adds three consolidated requirements from TR 22.856 to TS 22.156.*

**1. Introduction**

This pCR adds three requirements in the TS.

**2. Reason for Change**

CPR 5.6, 5.7 and 5.8 were consolidated in SA1 103 and have not been added in the TS.

**3. Conclusions**

None.

**4. Proposal**

It is proposed to agree the following changes to 3GPP TS 22.156 version 1.0.0

FIRST CHANGE

### 5.2.3 Digital asset management

#### 5.2.3.1 Description

Mobile metaverse services can depend upon information that is associated with the user, e.g. User Identifiers and personal data that are commonly required and represented in a machine-readable format. The requirements as described in 3GPP TS 22.101 [4] clause 26a apply for identification of users. These can be used to provide proof for regulatory constrained service, e.g. proof of residential address for services that are restricted to local residents.

Further, the services can benefit from common information, such as avatar parameters and configuration information, so that a user's digital representation is consistent across different applications. Users can benefit from the support of associating their digital assets with different User Identities, to flexibly control their stored information.

Finally, some more specific information used by different services can also be shared in different mobile metaverse services and be considered 'digital assets' in that the user needs or could benefit from having this information available when access mobile metaverse services. According to regulation, this information can be considered as personal data.

An example of such service is the EU digital wallet initiative [6]. Both the digital wallet and the digital asset management functionality described in the present document emphasize the need for security, privacy and control over access to authorized parties.

#### 5.2.3.2 Requirements

Subject to operator policy, regulatory requirements and user consent, the 5G system shall be able to provide functionality to store digital assets associated with a user, and to remove such digital assets associated with a user.

Subject to operator policy, regulatory requirements and user consent, the 5G system shall provide a means to allow a user to securely access and update their digital assets.

Subject to operator policy and user consent, the 5G system shall be able to allow an authorized third party to retrieve the digital asset(s) associated with a user, e.g. when the user accesses a specific application.

NOTE: When a user accesses an immersive mobile metaverse service, the authorized third party (service provider) could obtain relevant digital assets of a user associated with that service.

The 5G system shall be able to associate a stored digital asset with one or more User Identities.

Subject to operator policy, regulatory requirements and user consent, the 5G system shall support a mechanism for users to define conditions (e.g. based on user location information) to restrict the access to, and management of, stored digital assets associated with User Identity.

The 5G system shall support mechanisms to request specific formats of stored digital assets associated with a user by an authorized mobile metaverse service.

END OF CHANGES