**3GPP TSG-SA3 Meeting #116 *S3-24xxxx***

**Jeju, South Korea, 20th - 24th May 2024**

————————————————————————————————————————————————

**Source:** **Huawei, HiSilicon**

**Title:** **New key issue on security aspect of digital asset container in 5GC**

**Document for:** **Approval**

**Agenda Item:** **5.18**

# 1 Decision/action requested

***Approve the new KI for inclusion in TR 33.721 [1]***

# 2 References

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

# 3 Rationale

This contribution proposes a new key issue about the digital asset container security. The issues was proposed in the WT #2 in S3-240974.

Several requirements on digital asset management have been agreed in SA1 and consolidated in TS 22.156:

[R-5.2.3-001] 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.

[R-5.2.3-003] 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.

[R-5.2.3-006] 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.

[R-7.2.4-001] Subject to operator policy, regulatory requirements and user consent, the 5G system shall provide secure means to authorize the use of digital assets associated with a user (e.g., digital assets belonging to a third party customer).

[R-7.2.4-002] The 5G system shall provide mechanisms to certify the authenticity of digital assets associated with a user.

# 4 Detailed proposal

\*\*\* BEGIN OF 1st CHANGE\*\*\*

## 5.X Key issue #X: Security aspects of digital asset container in 5GC

### 5.X.1 Key issue details

According to SA1 TS 22.156 [3], several requirements corresponding the digital asset container of the metaverse are identified:

*[R-5.2.3-003] 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.*

*[R-5.2.3-006] 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.*

*[R-7.2.4-001] Subject to operator policy, regulatory requirements and user consent, the 5G system shall provide secure means to authorize the use of digital assets associated with a user (e.g., digital assets belonging to a third party customer).*

*[R-7.2.4-002]The 5G system shall provide mechanisms to certify the authenticity of digital assets associated with a user.*

The requirements will lead new functionalities of the digital asset container. Correspondingly, the security aspect of the digital asset as well as the digital asset container itself deserve a thorough KI in order to further clarify the potential risks of the digital asset container in 5GC.

This KI aims to comprehensively study the security requirements of the digital asset container in 5GC.

### 5.X.2 Security threats

An attacker may access a digital asset if the authentication and authorisation of the usage of digital assets are not performed.

### 5.X.3 Potential security requirements

The 5G system shall provide the means to ensure authenticity of the digital asset(s) in a digital asset container.

The 5G system shall support to authenticate and authorize a 3rd party to access the digital asset(s) in a digital asset container.

Editor’s Note: The requirements need to further align with the feedback from SA1 and SA6.

\*\*\* END OF 1st CHANGE \*\*\*