**3GPP TSG-SA3 Meeting #119AdHoc-e draft\_S3-250034-r6**

**Online, Electronic meeting, 13 -16 January 2025** merger of S3-250034,S3-250052,S3-250152

**Source: ZTE, Huawei(?), Nokia, Nokia Shanghai Bell**

**Title: Pseudo-CR on Conclusion for KI #3**

**Document for: Approval**

**Agenda item: 5.18**

**Spec: 3GPP TR 33.721**

**Version: 0.5.0**

**Work Item: Study on security aspects of 5G Mobile Metaverse services**

**Comments**

This pCR proposes to conclude on KI#3 in TR 33.721.

**Proposed Changes**

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

## 7.2 Key issue #3: Security aspects of digital asset container in 5G

The TS 23.438 [8] specifies in sufficient detail the requirements, architecture, procedures and APIs for digital asset management, the digital asset service is part of the SEAL services specified in 3GPP TS 23.434  [7].

The normative work of the KI#3 aligns with the architecture of digital asset management defined in the TS 23.438 [8] and the below security solution principles should be followed:

* Security for the SEAL interfaces, especially SEAL-S, SEAL-UU, specified in TS 33.434 [4] is applied for protection of digital asset management interfaces such as DA-S, DA-UU as specified in TS 23.438 [8].
* When CAPIF is used as specified in TS 23.434 [7], the security mechanism for CAPIF specified in TS 33.122 [5] shall be followed for authenticating a digital asset requestor (API Invoker) to access the digital asset(s).
* When CAPIF is used as specified in TS 23.434 [7], the security mechanism for CAPIF specified in TS 33.122 [5] shall be extended for authorizing a digital asset requestor (API Invoker) to create the digital asset(s).

Editor’s note: When DA server has sufficient local information to authorize the digital asset requestor to access digital assets stored in the DA server, whether CAPIF needs to be used for authorization is FFS.

Editor’s note: Before authorizing the digital asset requestor to access digital assets stored in the DA server based on allowed users of the digital asset, DA server shall first authenticate the (VAL) user behind the digital asset requestor. How DA server authenticates the (VAL) user is FFS.

Editor’s note: Further conclusions are FFS.

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