**3GPP TSG-SA3 Meeting #124 draft\_S3-253666\_r4**

Wuhan, China, 13 – 17 October 2025 is revision of S3-253333, merger of S3-253312 and S3-253349 and S3-253518

**Title: [draft]reply LS on Security risk of usage permission management of Digital Asset**

**Response to: LS S6-253789 on Security risk of usage permission management of Digital Asset from** **SA6**

**Release: Rel-20**

**Work Item: Metaverse\_Ph2-APP**

**Source: SA3**

**To:** **SA6**

**Cc:**

**Contact person: Xiaoting Huang**

**huangxiaoting@chinamobile.com**

**Send any reply LS to: 3GPP Liaisons Coordinator,** **mailto:3GPPLiaison@etsi.org**

**Attachments:** **n/a**

# 1 Overall description

SA3 thanks SA6 for the LS on security risk of usage permission management of Digital Asset. SA3 would like to answer the 2 questions as below:

**Question 1:** SA6 would like to ask whether and how it is possible for the digital asset owner to delegate the authority to grant the permission to another entity (e.g. DA server or authorized user)?

**Answer 1:** SA3 believes the answer depends on which entity the digital asset owner wants to delegate the authority to. If the digital asset owner wants to delegate the authority to the operators’ DA server or authorization server, the DA/authorization server is able to check its local DA profile/authorization policy which could be implemented or configured to store the granted permission to the digital asset client by the digital asset owner. SA3 has not studied how to delegate to another digital asset user.

**Question 2:** What is SA3’s opinion on such security risks/threats?

**Answer 2:** SA3 believes it is a trust issue and SLA between the digital asset owner and the delegated entity, which can be implementation dependent.

# 2 Actions

**To SA6:**

**ACTION:** SA3 kindly asks SA6 to take the above answers into account and sync with SA3 for any security solutions.

# 3 Dates of next TSG SA WG 3 meetings

SA3#125 17 – 21 November 2025 Dallas, US

SA3#126 9 – 13 February 2026 India (TBD)