**3GPP TSG-SA3 Meeting #119AdHoc-e S3-250148r1**

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Update sol#5 on Privacy protection during metaverse service discovery**

**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# 5 of the TR on Privacy protection during metaverse service discovery, to address the ENs, and add evaluation for the solution.

According to Annex V of TS 33.501, any NF that is deemed an enforcement point for user consent shall support to retrieve the user consent parameters from the UDM, and based on clause 5.1.3 of TS 33.558, the EES, as edge application enabler server, can be an enforcement point for user consent, so it’s rational that the SEAL server, as service enabler server or API exposure server, acting as an enforcement point and support to retrieve the user consent parameters from the UDM, especially if the SEAL server is trusted by the 5G core network. So the EN “whether the user consent information in the UDM can be specific for metaverse services is FFS” will be removed, and the condition that the SEAL server is trusted by the 5G core network will be added. If the SEAL server is trusted by the 5G core network, NEF is not required when the SEAL server accesses UDM.

**Proposed Changes**

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

<Proposed change in revision marks>

## 6.5 Solution #5: Privacy protection during metaverse service discovery

### 6.5.1 Introduction

This solution addresses Key Issue #2 on privacy of user sensitive information.

According to 4.2 Key Issue #2: Exposure of user sensitive information of TR 23.700-21, ensuring appropriate user consent has been obtained is a critical aspect when handling sensitive information relating to or collected from a user, their devices or the applications installed at their devices. For instance, with the expected capability to access, manage and expose user specific avatar related information through the enabler layer it is of utmost importance to capture the consent of the user.

Spatial anchor, spatial map discovery are supported in solution#1 (clause 7.1) and solution#8 (clause 7.8) of TR 23.700-21 [2], this contribution proposes a solution to check user consent in discovery procedure, and return list of spatial anchors, spatial maps, which match user consent, to the metaverse service consumer or SEAL client.

### 6.5.2 Solution details



Figure 6.5.2-1 Procedure of privacy protection during metaverse service discovery

Precondition:

A list of spatial anchors, spatial maps and avatars are created, personal data required to support each spatial anchor, spatial map or avatar is registered.

The SEAL server is deployed in operator domain and trusted by the 3GPP core network.

1. UE initiates a discovery request to SEAL server to get the list of spatial anchors or spatial maps, AF specific UE Identifier, e.g. GPSI, is included in the request.

2. SEAL server requests the UDM directly to get the user consent for metaverse services based on the GPSI.

3. UDM sends the user consent for the metaverse services to the SEAL server.

Editor’s Note: whether the user consent information in the UDM can be specific for metaverse services is FFS.

4. SEAL server processes the user consent along with the personal data required to support registered spatial anchors or spatial maps.

5. SEAL server sends a list of spatial anchors or spatial maps which personal data requirements satisfy UE consent.

Editor’s Note: Whether user consent or resource owner authorization is most suitable to be used in this solution is FFS.

### 6.5.3 Evaluation

The solution addresses requirements of Key issue #2 to support privacy protection of user sensitive information during exposure of user specific information (e.g. user identity, user location) in localized mobile metaverse services through the application enabler layer.

UDM needs to enhance to support user consent retrieving and checking for protection of user sensitive information in metaverse services.

The solution assumes that the SEAL server is deployed in operator domain and trusted by the 3GPP core network, hence it can get user consent as specified in Annex V of TS 33.501.

Editor’s Note: Whether user consent or resource owner authorization is most suitable to be used in this solution is FFS.

Editor’s Note: whether the user consent information in the UDM can be specific for metaverse services is FFS.

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