**3GPP TSG-SA3 Meeting #119AdHoc-e Draft\_S3-250147-r1**

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Update sol#3 on Authorization supporting spatial localization service with CCF**

**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 the title of solution# 3 of the TR, Solution for KI#1 on Authorization supporting spatial localization service with CAPIF Core Function (CCF), to reflect the case with different resource owners, and add evaluation for the solution.

**Proposed Changes**

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

<Proposed change in revision marks>

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

…

[2] 3GPP TR 23.700-21: "Study on Application enablement architecture for mobile metaverse services".

[3] 3GPP TS 22.156: "Mobile Metaverse Services; Stage 1".

[4] 3GPP TS 33.434: "Security aspects of Service Enabler Architecture Layer (SEAL) for verticals".

[5] 3GPP TS 33.122: "Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs"

[6] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

[7] 3GPP TS 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows"

[8] 3GPP TS 23.438: “Service Enabler Architecture Layer for Verticals (SEAL); Digital Assets”

[xx] 3GPP TS 23.437: “Service Enabler Architecture Layer for Verticals (SEAL); Spatial map and Spatial anchors”

\* \* \* Next Change \* \* \* \*

## 6.3 Solution #3: Solution for KI#1 on Authorization supporting spatial localization service with CAPIF Core Function (CCF) in case of different resource owner

### 6.3.1 Introduction

The solution addresses KI#1 on Authorization supporting spatial localization service.

In Solution #2 of TR 23-700-21, Support for spatial anchor management of 23-700-2, a VAL server may include following information in the request when create a spatial anchor:

- service information of the product to associate it with the spatial anchor,

- access control rules defining which entities are permitted to discover and access the spatial anchor,

- customer premise information (e.g. a residence, office, or shop).

- spatial anchor discoverable visibility levels like universal to facilitate shared spatial anchor discovery

When one VAL server discovers or manages a spatial anchor created by another VAL server, the access control policies from the creating VAL server should be considered to authorize the spatial anchor services to the accessing VAL server.

The solution proposes to authorize one VAL server/SEAL client to access spatial anchor created by another VAL server/SEAL client with considering the access control polices from the creating VAL server.

CAPIF framework is based to authorize spatial localization service consumer in this solution.

NOTE: OAuth 2.0 token based authorization of CAPIF is adopted in this solution.

### 6.3.2 Solution details

A VAL server (VAL server1) creates a spatial anchor in a SEAL server which including access control rules/authorization policies in the creation request and the SEAL server synchronizes authorization policies with CAPIF Core Function (CCF) together with the VAL server1 information. When another VAL server (VAL server 2) requests access token from CCF for the spatial anchor, CCF checks the authorization policy of the spatial anchor. If VAL server2 is allowed to access the spatial anchor, CCF generates an access token and provides it to VAL server2. The VAL server2 initiates a spatial anchor service request along with the access token to the SEAL server. The SEAL server, upon successful validation of access token, provides the spatial anchor service to the VAL server2.

#### 6.3.2.1 Procedure of authorization of spatial anchor service with multiple VAL server



Figure 6.x.2.1-1 Procedure of authorization of spatial anchor service with multiple VAL server

0. VAL server1 and server2 are onboarded to CCF and authenticated with CCF. VAL server1 is authorized by CCF and access token for creation of spatial anchor has been obtained from CCF.

1. VAL server1 sends a spatial anchor creation request to SEAL server with the spatial anchor information and access token obtained from CCF.

2. SEAL server validates the access token against the service request and creates a spatial anchor, e.g. with spatial anchor id set to “anchor\_123”.

3. SEAL server sends spatial anchor creation response to VAL server1.

4. SEAL server publishes the spatial anchor information, e.g. spatial anchor id (anchor\_123), owner of the spatial anchor (VAL server 1) and optionally the authorization policies associated with the spatial anchor to CCF.

5. CCF stores the spatial anchor information in the VAL server1 profile.

6. VAL server 2 sends access token request to CCF to access the spatial anchor (anchor\_123).

7. CCF authorizes the request based on local policies (e.g. if a VAL server is allowed to consume spatial anchor related services) and authorization policies associated with the spatial anchor (e.g. if the anchor\_123 can be read/updated by the VAL server 2) presented in VAL server 1 profile. If VAL server2 is authorized, generates an access token.

NOTE: Optional CCF may implicitly ask authorization from VAL server1 if there's no authorization information associated with the spatial anchor based on local policies.

8. CCF sends the access token to VAL server2.

9. VAL server2 sends request to SEAL server to access the spatial anchor, along with the access token received from CCF.

10. SEAL server validates the access token and service request and perform the request on successful validation.

11 SEAL server sends the spatial anchor response to VAL server2.

Editor’s Note: Alignment with CAPIF is FFS.

### 6.2.3 Evaluation

The solution addresses requirements of Key issue #1 to support authorization of a consumer (e.g. UE, VAL server) for accessing spatial localization services (e.g. spatial map obtaining, spatial anchor accessing) based on CAPIF security mechanism, especially when the consumer of the spatial map/anchor is different to the owner of the spatial map/anchor.

According to TS 23.434 [7] and TS 23.437 [xx], Spatial Anchor/Map Client and Val Server play the role of CAPIF API Invoker, Spatial Anchor/Map plays role of CAPIF AEF, hence CAPIF API Invoker, AEF and Core Function need to enhance to support Spatial Anchor/Map specific authorization, especially in the case that the consumer of the spatial map/anchor is different to the owner of the spatial map/anchor.

The solution is aligned with Localized mobile metaverse services defined in TS 23.437 [xx].

Editor’s Note: Alignment with CAPIF is FFS.

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