|  |
| --- |
| 3GPP TR 33.721 V0.2.0 (2024-05) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of 5G Mobile Metaverse services;(Release 19) |
|   |
|  | 3GPP-logo_web |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Security assumptions 7

5 Key issues 7

5.1 Key Issue #1: Authorization supporting spatial localization service 7

5.1.1 Key issue details 7

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key Issue #2: Privacy of user sensitive information 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

5.X Key Issue #X: <Key Issue Name> 9

5.X.1 Key issue details 9

5.X.2 Security threats 9

5.X.3 Potential security requirements 9

6 Solutions 9

6.1 Solution #1: Support for spatial localization service authorization 9

6.1.1 Introduction 9

6.1.2 Solution details 9

6.1.3 Evaluation 10

6.Y Solution #Y: <Solution Name> 11

6.Y.1 Introduction 11

6.Y.2 Solution details 11

6.Y.3 Evaluation 11

7 Conclusions 11

Annex <X> (informative): Change history 12

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

Editor's Note: The introduction clause content is left for future consideration.

# 1 Scope

The present document studies security impacts of the procedures introduced in Study on Application enablement architecture for mobile metaverse services studied in TR 23.700-21[2], specifically, the security aspects that are to be covered in this study are as follows:

- authentication and authorization of digital identity (non-IMS based)

NOTE: The term digital identity is defined in clause 3.1.

- support security aspects of digital asset container

 Editor's Note: Whether the digital asset container is specified in 5GC or in the application layer is under the remit of SA6.

- security and privacy aspects of user sensitive information for Localized Mobile Metaverse Services

NOTE: The potential security requirements will be updated based on the study progress in SA6.

# 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".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**Digital Asset Identifier:** In the context of this TR, digital asset identifier is used to uniquely identify a digital asset across different mobile metaverse services.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

<ABBREVIATION> <Expansion>

clause includes the overview applicable for the study.

# 4 Security assumptions

The following security assumptions are applied to the study:

- The application enabler architecture for mobile metaverse services as described in TR 23.700-21 [2] is taken into account.

Editor’s Note: alignment with TR 23.700-21 is FFS.

- The security architecture, requirements and procedures for SEAL as defined in TS 33.434 [4] are used as a baseline.

Editor's Note: Whether SA6 architecture options are based on SEAL is FFS.

- Digital Asset Identifier is used in this study to identify a digital asset associated with a user.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Authorization supporting spatial localization service

### 5.1.1 Key issue details

In clause 4.1 of TR 23.700-21 [2], enabler support for managing spatial anchors is documented as a key issue, with the open issue regarding the access to spatial anchor as the following:

"*How to discover spatial anchors by the consumer (e.g. UE, VAL server)?*"

In clause 4.2 of TR 23.700-21 [2], exposing spatial map to third parties is documented as a key issue, with the open issue regarding the third party who needs to be authorized as the following:

"*How to expose a spatial map to authorized third parties?*"

Either for discovering spatial anchors or for exposing spatial maps, authorization of the consumer (e.g. UE, VAL server) needs to be considered. This key issue focuses on the authorization aspect supporting spatial localization service.

### 5.1.2 Security threats

Spatial map or spatial anchor could be a piece of information sensitive to the operator or the operator’s customer or the users in the map. If the consumer (e.g. UE, VAL server) is not authorized for obtaining the spatial map or accessing the spatial anchor, such sensitive information could be leaked to an undesired party. Further, the operator will not be able to correctly charge the consumer (e.g. UE, VAL server) for using spatial localization service supporting localized mobile metaverse services.

Editor’s Note: What sensitive information is for an operator or operator’s customer is FFS.

### 5.1.3 Potential security requirements

The 5G system shall provide a means to authorize a consumer (e.g. UE, VAL server) for accessing spatial localization services (e.g. spatial map obtaining, spatial anchor accessing).

Editor’s Note: The requirement details with respect to the potential consumers of localized mobile metaverse services, the host of such service and exposed information via such service is subject to SA6 progress.

## 5.2 Key Issue #2: Privacy of user sensitive information

### 5.2.1 Key issue details

User sensitive information (e.g. relating to user/UE identity, body movement or location, authentication result) needs to be accessed, managed and exposed through the enabler layer for localized mobile metaverse service.

In clause 4.2 of TR 23.700-21 [2], exposure of user sensitive information is documented as a key issue.

This key issue focuses on the privacy aspect of user sensitive information which is transferred within or outside the network.

Editor’s Note: Whether authorization and/or user consent is needed for potentially user sensitive information in this study is to be decided in SA3

Editor’s Note: Whether the RNAA framework is taken into consideration is FFS

### 5.2.2 Security threats

User sensitive information needs to be accessed and exposed through the enabler layer to a non-owner. Without proper protection (e.g. obtaining the owner’s consent), the privacy sensitive information could be leaked to undesired party, leading to privacy violation, trust and reputation impairment, regulatory incompliance, etc. An attacker can avail the user sensitive information to launch targeted attacks that cause data breaches, identity theft, etc.

Editor’s Note: The definition of “owner” or “non-owner” is FFS

### 5.2.3 Potential security requirements

The 5G system shall provide a means for privacy protection of user sensitive information during exposure of user specific information in localized mobile metaverse services through the application enabler layer.

Editor’s Note: What user sensitive information and user specific information in localized mobile metaverse services is FFS.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

6.0 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

**Table 6.0-1: Mapping of solutions to key issues**

|  |  |  |  |
| --- | --- | --- | --- |
| **Solutions** | **KI#1** | **KI#2** | **KI#Z** |
| **Solution #1** | X |  |  |

## 6.1 Solution #1: Support for spatial localization service authorization

### 6.1.1 Introduction

This solution is for KI #1 and addresses the security requirements for authorizing UE to access spatial localization services. This solution is based on the Service Enabler Architecture Layer (SEAL) Location Management (LM) service to provide spatial localization services (e.g. spatial map management, spatial anchor management), and SEAL identity management (SIM) service to perform UE authorization.

###  Solution details

Before getting authorization to specific service, the VAL UE authentication is executed by the SIM-S as described in TS 33.434 [4]. After successful authentication, the SIM-C requests and receives an access token from SIM-S as shown in Figure 6.1.2.1.



**Figure 6.1.2-1: Get Access Token**

1. User Authentication is completed between VAL UE and the SIM-S.
2. The VAL UE sends an access token request to the SIM-S, including the identity of the VAL UE and the specific spatial localization service the UE requests to access.
3. The SIM-S authorizes the VAL UE for the requested service and provides access token for the VAL UE.

With the received access token, the VAL UE can request for spatial localization service from SEAL LM server. The procedure of getting spatial map for metaverse application is shown in Figure 6.1.2.2.



**Figure 6.1.2-2: Get Spatial Map**

1. A secure channel is established between SEAL LM client and SEAL LM server. Subsequent communication makes use of this channel.

1. The VAL UE sends a request message containing the access token to the SEAL LM server to get the spatial map via SEAL LM client.

2. On receiving the service authorization message, the SEAL LM server validates the access token.

3. If the access token is valid, the SEAL LM server provides the spatial map information to the VAL UE via SEAL LM client. Otherwise, the response included the failure cause indicating that the token is invalid.

The same procedure can also be applied for getting spatial anchor and any other spatial localization services provided by SEAL LM server by changing the request service.

Editor’s Note: The application enablement architecture for metaverse services is to be aligned with SA6.

### 6.1.3 Evaluation

 TBD

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115 Adhoc-e | S3-241422 |  |  |  | Skeleton for TR 33.721 | 0.0.0 |
| 2024-04 | SA3#115 Adhoc-e | S3-241632 |  |  |  | S3-241584, S3-241548, S3-241549, S3-241553, S3-241554 | 0.1.0 |
| 2024-05 | SA3#116 | S3-242608 |  |  |  | S3-242583 implemented | 0.2.0 |