**3GPP TSG-SA3 Meeting #115 *draft\_S3-240974-r3***

**Athens, Greece, 26th February - 1st March 2024** **(revision of xx-yyxxxx)**

**Source: Samsung, Nokia, Nokia Shanghai Bell, IIT Delhi, Lenovo, OPPO**

**Title: New SID on security aspects of 5G Mobile Metaverse services**

**Document for: Approval**

**Agenda Item: 6**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on security aspects of 5G Mobile Metaverse services

Acronym: FS\_Metaverse\_Sec\_ph1

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-19

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X |  | X |  |
| No |  |  |  |  |  |
| Don't know | X |  | X |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| NA | NA | NA | NA |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| 1000028 | Mobile Metaverse Services | Related stage-1 Rel-19 3GPP SA1 work item |
| 1010032 | Study on Architecture enhancement for XRM Ph2 | Related stage-2 Rel-19 3GPP SA2 study item |
| 1020063 | Study on User Identities and Authentication Architecture | Related stage-2 Rel-19 3GPP SA2 study item |
| 1020052 | Study on application enablement for Localized Mobile Metaverse Services | Related stage-2 Rel-19 3GPP SA6 study item |

# 3 Justification

The Metaverse is rapidly advancing in research and development even outside of 3GPP today, and it is necessary to first identify the significance of its implementation within the 3GPP ecosystem. 3GPP SA1 has studied and investigated use cases and service requirements for 5GS to support enhanced XR-based services, (as XR-based services are an essential part of "Metaverse" services) as well as potentially other functionality, to offer shared and interactive user experience of local content and services, accessed either by users in the proximity or remotely.

Use cases such as digital asset container information access may require SA3 to analyse the security protection options of the digital asset container (e.g. cannot be spoofed, access control with a policy determined by the user, etc.). Secondly, management of the security aspect of the digital asset container, i.e., security of user managing the digital asset in the digital asset container and authorization of a third party that can retrieve the digital asset (avatar and application specific avatar details), also needs to be analysed.

Further, new SID on application enablement for Localized Mobile Metaverse Services was agreed in SA6 to study enablement support for metaverse application such as managing information related to avatars, managing spatial anchors and associated information and accessing enhanced localization information, e.g. related to spatial map information. Many of the requirements captured in TS 22.156 are subject to operator policy, regulatory requirements and user consent. Each user needs to be in full control of which network and device entities are allowed to access, manage and expose information pertaining to themselves and their devices. Such end user approvals ensure that only legitimate, user trusted, entitles can obtain and utilise information and services involving that user's sensitive information (for eg., User Identity profile, Authentication and authorization results, linking a User Identifier with a subscription).

For these application enablement aspects, it is a necessity for SA3 to determine the potential security requirements and related procedures.

NOTE: Digital ID is different from User ID and there is no overlapping or dependency. User ID is used to identify a user behind the UE. Digital ID is used to identify a digital representation specific to media. For example, in case of avatar representation, the digital ID is basically an avatar ID (in other words, avatar ID is one example of digital ID).

# 4 Objective

This study aims to identify the potential security requirements to support mobile metaverse based on SA1, SA2 and SA6 studies and propose the appropriate security procedure.

The objective of this study are:

WT1. To support digital identity authentication and authorization for non IMS based metaverse services

* To study how to authenticate the digital identity/avatar associated with the subscriber (user)
* To study how to authorize the digital identity/avatar associated with the subscriber (user) to be used in mobile metaverse services
* To study how to ensure privacy aspect associated with avatar

WT2. To support digital asset container in 5GC

* To study how to ensure authenticity of the digital asset associated with the user
* To study security aspect of user storing and managing the digital asset(s) in the digital asset container
* To study how to authenticate and authorize trusted third party to retrieve the digital asset(s) associated with a user, e.g. when the user accesses a specific application

WT3. To support the security aspects and procedure enhancement on application enablement for Localized Mobile Metaverse Services

* To study how to ensure the privacy aspects for exposure of user sensitive information (for e.g., how to control the access of a user’s assets to another user).

Further, SA3 shall have responsibility for the mobile metaverse, as an assessor of the security implications and identifying the potential security requirements based on the study performed by other working groups and define potential solutions to fulfil these requirements.

NOTE: User authentication is not in the scope of the study.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | RAN Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency |
| WT1 | 1.5 | 0.5 | No | No |
| WT2 | 1.5 | 0.5 | No | No |
| WT3 | 1 | 1 | No | No |

Total TU estimates for the study phase: 4

Total TU estimates for the normative phase: 2

Total TU estimates: 6

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | TBD | Study on security aspects of 5G Mobile Metaverse services | SA#105 (Sep 2024) | SA#106 (Dec 2024) |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |

# 6 Work item Rapporteur(s)

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Potential interactions with SA1, SA2, SA6 for the requirement, architectural and service aspects.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Samsung |
| Nokia, Nokia Shanghai Bell |
| IIT Delhi |
| Lenovo |
| OPPO |
| Charter Communications |
| CableLabs |
| CMCC |