**3GPP TSG-SA3 Meeting #124 S3-253227r1**

**Wuhan, China, 13 – 17 October 2025 merger of S3-253154, S3-253227, S3-253354**

**Source: Apple, Interdigital, Xiaomi**

**Title: New Security Area on Privacy**

**Document for: Approval**

**Agenda item: 5.3.1**

**Spec: 3GPP TR 33.801-01**

**Version: 0.1.0**

**Work Item: FS\_6G\_SEC**

**Comments**

This contribution proposes a new security area for TR 33.801-01.

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

# 4 Security areas and high level security requirements

## 4.1 Security areas

Editor's Note: This clause further clarifies the scope of the study by listing the security areas that SA3 is working on.

This document includes the following security areas:

1. Privacy deals with any potential vulnerability that may weaken the user privacy and provide streamlined and unified privacy control for an increasing number of 6G features to protect the ID privacy and data privacy across all security domains.

## 4.2 Potential high level security requirements

Editor's Note: This clause will document high-level requirements that guide the study.

6G system should support the mechanisms to enhance the SUCI.

6G system should consider to design a consistent, unified, dynamic user consent framework to avoid user data sharing being abused.

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

# 5 Key issues and solutions

## 5.x Security area #x: Privacy

### 5.x.1 Introduction

Editor's Note: Detailed description of the security area

Privacy protection is an indispensable component of 6G security study, particularly given the possibly various data types collected by the network for 6G features and high sensitivity of personal data.

Firstly, identity privacy protection requires reassessment and enhancement. While the UE permanent identifier (e.g., SUPI) is protected during over-the-air transmission in 5G, its exposure outside the home network remains unprotected. By re-considering the trust relationship between PLMNs or across different network partitions (e.g. between PLMN and PNI-NPN) in the 6G security architecture, the exposure of UE permanent ID and other identifiers (e.g. user ID, digital ID) may need to be re-evaluated.

Secondly, the existing 5G privacy protection relies on disparate approaches (e.g. user consent-based approach or privacy profile-based approach) and enforcement points (e.g. GMLC for LCS service, NWDAF for AI service) for different 5G features, which results in complexity and redundancy of protection mechanisms. These privacy control mechanisms need to be enhanced in 6G system, so as to provide a streamlined and unified privacy control for an increasing number of 6G features.

Particularly, one of the work tasks of the Study on Architecture for 6G System is to study data framework for all aspects related to efficient and scalable data handling including e.g. data collection, distribution, processing, storage, data access and data exposure. The work task will also consider access control/user consent and privacy where relevant and study any potential enhancements on system and procedure needed for user consent framework. In order to support such work task of the 6G architecture study, it is necessary to study in the present document how the current privacy control mechanisms can be enhanced by incorporating user consent to provide protection for data privacy in 6G data framework, depending on the progress in SA2 or SA5.

The Privacy security area in the 6G security framework addresses the protection of personally identifiable information (PII), user identities, and sensitive metadata across the mobile network ecosystem. As a horizontal domain, Privacy intersects with vertical areas such as RAN security, Core Network security, Authentication and Key Agreement (AKA), Authorization, Security Context and Key Management, and Service-Based Architecture (SBA) security. Its responsibilities include identifying privacy-related Key Issues, analyzing threats and attack vectors, defining privacy requirements, and proposing technical solutions that ensure confidentiality, unlinkability, and user control over personal information. Potential solutions may range from enhanced identifier protection mechanisms and pseudonymization techniques to differential privacy, federated learning, and decentralized identity frameworks.

In 6G, privacy challenges are expected to become more complex due to massive device density, AI-native networks, non-terrestrial access, and emerging service paradigms such as digital twins and metaverse applications. These developments introduce new risks of identity correlation, profiling, and cross-domain data leakage. It is therefore necessary to study how privacy requirements can be strengthened across protocol layers, domains, and use cases, and to assess how privacy-preserving mechanisms can be integrated into the 6G architecture to ensure consistent protection for all users and services.

The Security Area Privacy contain the below aspects, but not limited to:

- SUCI enhancement. 5G introduced SUCI as a significant feature to protect the security of the permanent identity SUPI/IMSI. In 6G, the SUCI faces some limitation when it comes to quantum resistant requirement. FS\_PQC is addressing the issue on updating the SUCI to PQC, e.g. updating the profiles with PQC algorithms/profiles. Besides, any other potential enhancements on the mechanisms will he handled here.

- User consent framework enhancement. In 5G, there is a user consent framework defined in TS 33.501 Annex V. However the framework is not complete and only covers the UDM storage part and not specifying any protocol or procedure on user consent collection/obtaining from the UE. Besides, there is no generic revocation procedure defined for the UE to dynamically change the user consent status, nor the protocol defined for data processing after consent revocation. There are other confusions across the 3GPP-wide WGs, different user consent solutions have been used for different features in the past (e.g. positioning AI/ML), leading to inconsistency in how user consent and privacy are treated in the same network entity. Data collection have been specified in many features, e.g. NWDAF analytics, legacy and AI/ML-based positioning, Sensing, etc, 6G system shall consider the requirement to design a consistent, unified, dynamic user consent framework to avoid user data sharing being abused.

Editor’s Note: Other aspects under Privacy area to be added are FFS.

### 5.x.2 Security assumptions

It is assumed that 6G networks will continue to expose both permanent and temporary identifiers in signaling, requiring mechanisms to minimize identity exposure and provide unlinkability and untraceability against passive and active adversaries.

It is assumed that location, mobility, and service usage data may be subject to tracking, inference, or profiling, and that privacy-preserving mechanisms will be needed across different protocol layers and domains.

It is assumed that AI/ML-based analytics and optimization will be integral to 6G networks, and that privacy protections must be in place to prevent misuse of sensitive user data during training, inference, or sharing.

It is assumed that multi-domain environments, including non-terrestrial networks, IoT, and edge services, will increase the risk of cross-domain data leakage, requiring common privacy requirements and solutions across heterogeneous infrastructures.

It is assumed that user consent and control over the collection, processing, and sharing of personal information will remain a key principle, and that technical solutions will need to support regulatory compliance in different jurisdictions.

It is assumed that new service paradigms such as digital twins and metaverse applications will create additional privacy-sensitive contexts, requiring identity and metadata protection that extends to virtual and immersive interactions.

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