**3GPP TSG-SA3 Meeting #124 S3-253606-r4**

**Wuhan, China, 13 – 17 October 2025**

**Source: Nokia, Samsung, Xiamoi, Interdigital**

**Title: New Security Area on User Consent**

**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 \* \* \* \*

# 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".

[x] General Data Protection Regulation, <https://gdpr-info.eu/>

[y] American Privacy Rights Act, <https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf>

[a] ISO/IEC 27701:2025 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance

[b] ITU-T X.1121 : Framework of security technologies for mobile end-to-end data communications \* \* \* Next 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. User Consent framework would be responsible to ensure consistency among the procedures needed to support Users providing consent for 6G use cases.

## 4.2 Potential high level security requirements

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

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

# 5 Key issues and solutions

## 5.x Security area #x: User Consent

### 5.x.1 Introduction

In 5G, there is a user consent framework defined in TS 33.501 Annex V and covers the UDM storage part, not specifying any protocol or procedure on user consent. Besides, there is no generic revocation procedure 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 is treated in the same network entity.

Additionally, government and/or other international bodies define privacy related regulations, such as GDPR [x] and APRA [y], ISO [a], and ITU-T [b] on how companies must manage the user consent lifecycle. In this context, SA6 and SA2 may define architectural requirements and use cases for user consent. 3GPPP SA3 group will study the provided input, in addition to security driven requirements and use cases, to identify and define the missing procedures in the User consent framework for 6G system. In particular, this security area will not define how the different procedures are applied to the specific use case, but will focus on defining unified procedures to manage User Consent lifecycle.

NOTE: coordination between SA2, SA6 and SA3 is required to ensure consistency among the different WGs.

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