**3GPP TSG-SA3 Meeting #124 draft\_S3-253642-r3**

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

**Source: vivo**

**Title: New Security Area on Security and Privacy of Data Framework**

**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 on security and privacy of data framework for TR 33.801-01.

Security and privacy of data framework deals with framework security of data framework and various protection aspects related to the different type data in data framework, e.g. personal data, network data, AI data, ISAC data, etc..

\* \* \* 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".

[cc] 3GPP TR 22.870: “Study on 6G Use Cases and Service Requirements”.

[dd] 3GPP TR 33.849: “Study on subscriber privacy impact in 3GPP”.

[ee] 3GPP TS 33.501: “Security architecture and procedures for 5G system”.\* \* \* 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. Security and privacy of data framework deals with security architecture enhancement of data framework

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

# 5 Key issues and solutions

## 5.x Security area #x: Security and privacy of data framework

### 5.x.1 Introduction

This security area covers security and privacy aspects of beyond communication service data framework.

Section 5.9.2 of TR 22.870 [cc] highlights the data framework as a part of the beyond communication services. WT 5 of SP-250806 [aa] and WT 8 of RP-251881 [bb] outlines the data framework, which encompasses efficient and scalable data collection, distribution, processing, storage, access, and exposure for various data types, with consideration of access control/user consent and privacy where relevant. The example of data may include AI data and Sensing data, and will study any potential enhancements on system and procedure needed for user consent framework. Additionally, SA5 might initiate a related study regarding the data framework.

NOTE: Coordination with SA2 and SA5 is needed.

The need for this study is motivated by (i) new service data types (e.g. personal data, AI data, compute artifact etc.) and (ii) new data handling patterns (e.g., data processing,etc.) and related exposure (e.g., via NEF/CAPIF).

Thus, the scope of this security area includes:

1. Security architecture enhancement of the data framework, such as ensuring the confidentiality and integrity of data collection, distribution, processing, storage, access and exposure within the data framework.
2. Various protection related to different service data within the data framework, such as enhancing privacy through user consent for personal data.

NOTE: Security architecture enhancement of the data framework needs to be studied based on SA2 and SA5 progress. While security requirements on various protection aspects related to data for different types of servicesuch as user consent for personal data can be studied independently.

### 5.x.2 Security assumptions

UE–network mutual authentication (e.g., 5G‑AKA/EAP‑AKA′) and key hierarchy (e.g., SEAF/AMF anchoring, and derivation of AS/NAS keys) are available.

Inter‑PLMN control‑plane security (e.g., SEPP/N32) and SBA security are assumed to be available as a baseline.

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