**3GPP TSG-SA3 Meeting #124** draft\_S3-253671-r9 merge*S3-253305 in* **S3-253143**

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

**Source: Lenovo, Motorola Mobility, T-Mobile US, Deutsche Telekom, AT&T, SK Telecom, China Mobile, Telefonica, Interdigital, CATT, China Telecom, ZTE, Telecom Italia**

**Title: New Security Area on Security monitoring of UE to network communication**

**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 to address the UE related threat detection and security control. The detailed rationale and the limited support in 5GS is presented in the companion discussion paper in S3-253142.

\* \* \* 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. Security monitoring of UE to network communication deals with collection of information about and handling in case of attacks.

## 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: Security monitoring of UE to network communication

### 5.x.1 Introduction

It is expected that, from the first release of 6G, 6G security needs to consider cyberattacks and malicious abuse. In 5G System, there is limited support specified in 3GPP TS 23.288 [y]. This security area studies threat detection of and protection against attacks towards 6G networks originating from malicious UEs. The assumption is that the manipulated UEs are already successfully authenticated and authorized by the network.

Key issues in this security area are expected to describe the malicious UE originating attack whose evaluation and mitigation they study. The scope is about analysis of necessary information.

NOTE X: Authentication procedure, AS/NAS security establishment, Sensing, and AI security are treated in other security areas.

### 5.x.2 Security Assumptions

TBD

.\* \* \* Next 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".

[y] TS 23.288, 'Architecture enhancements for 5G System (5GS) to support network data analytics services'.

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