**3GPP TSG-SA3 Meeting #124** draft\_S3-253671-r2 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**

**Title: New Security Area on Security Evaluation and Protection for UE involved Connections**

**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 Evaluation and Protection for User Equipment (UE) involves the timely detection of threats and robust access control mechanisms to mitigate UE-specific attacks and prevent malicious exploitation of communication links.

## 4.2 Potential high level security requirements

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

The security architecture for the 6G System must incorporate robust mitigation strategies to defend against User Equipment (UE) initiated threats, UE experienced threats and the malicious exploitation of established communication conduits. This protection scope encompasses the access stratum (AS), the non-access stratum (NAS), and direct peer-to-peer (P2P) UE connectivity.

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

# 5 Key issues and solutions

## 5.x Security area #x: Security Evaluation and Protection for UE involved Connections

### 5.x.1 Introduction

GSMA’s Mobile Economy Forecasts 5G connections to surpass 2 billion in 2025 and enhancing security and protecting against cybersecurity threats ranked as the top digital transformation objective [x]. As 5G/5G-advanced connectivity becomes more fundamental to our daily lives, so as the future 6G systems will be in this trajectory. Despite the telecom security evolution, there is an increasing trend with cyber security threats and attacks over telecom systems. With the increased capacities of end-user devices and connections comes an extended threat surface as there is no guarantee that each and every UE will make responsible use of the established network connections. If the established network connections are abused by a number of UEs, and if such maliciously behaving UEs are left undetected and unhandled it may lead to malicious attacks over the network causing service failure to the other UEs.

In 5G System, there is limited support specified in 3GPP TS 23.288 [y] on the DDoS attack prediction and signalling storm analytics prediction in relation the DDoS Attack. So far, the possible abnormal behaviours of UE from the cyber-attack or security threat perspective are not studied in detail. If a UE is behaving abnormal, we cannot rule out the possibility that a maliciously behaving UE may also abuse direct connections established with other UEs/relay node, and it is not limited to abuse of RAN and Core connections. When a UE performs network‑based roles (e.g., Relay UE, UE‑assisted positioning, aggregation), trust in that UE is not assumed by default; instead, acceptance of such roles may be based on dynamic security evaluation. Alternatively, in case of compromised network, the UEs may also experience abnormal behaviours of network over access or non-access stratum, in such a case abnormal behaviours have to be identified in a timely manner and the UEs should be protected. More importantly it is expected that, from the first release of 6G, 6G security needs to consider cyberattacks and malicious abuse. Hence this security area considers all possible abnormal behaviours related to UE as well as abnormal behaviours experienced by UE from other entities (UE/RAN/Core NF) and a related security handling approach to be studied accordingly.

NOTE X: The scope this study should not overlap with authentication procedure, AS/NAS security establishment and AI security.

### 5.x.2 Security Assumptions

- Authentication alone is not assumed to establish full trust. Trust may be based on dynamic security evaluation..

\* \* \* 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".

[x] GSMA Mobile Economy, 2025, '<https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2025/02/030325-The-Mobile-Economy-2025.pdf>'.

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

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