**3GPP TSG-SA3 Meeting #124 draft revised S3-253331-r2**

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

**Source: Ericsson, Samsung?, Huawei?, InterDigital?, Xioami?, Apple?, Nokia?, OPPO?**

**Title: New Security Area on 6G RAN Security**

**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.

The evolution of 3GPP RAN security from 2G to 5G represents a significant progression: from limited over-the-air protection for security and privacy to a robust, layered, and flexible security architecture designed for an all-IP and virtualized environment. This shift was driven by the imperative to mitigate increasingly sophisticated attacks, address vulnerabilities in legacy protection measures, and secure a disaggregated architecture where different protocol stack layers are processed across various network elements based on the functional split.

Radio communication remains inherently susceptible to risks such as jamming and spoofing. Specifically, 3GPP SA3 studied technical security risks related to False Base Station attacks, which exploit unprotected broadcast messages. These specific security risks, inherited from legacy radio access technology, are currently untreated by standardized interoperable solutions in 5G and are now entering the standardization phase for 6G radio.

Additionally, RAN Working Groups (WGs) standardized L1/L2 Triggered Mobility (LTM) in Release 18 and Release 19 to reduce overhead and interruption time using lower layer signaling. LTM supports intra-DU, inter-DU, and inter-CU mobility. The Release 19 normative work in SA3 agreed to conclude the Work Item Description (WID) by selecting a solution direction that involves sending the Next-hop Chaining Counter (NCC) unprotected from the serving gNB to the UE in the MAC-CE Cell Switch command. Release 20, therefore, inherits the untreated potential risk associated with an unprotected NCC. If exploited, this could pose threats to other non-security-related functional parameters, potentially leading to masquerading, Denial of Service (DoS) attacks on the UE, and breaches of subscriber privacy.

The RAN plenary approved the Study Item Description (SID) for 6G Radio in RP-251881. Furthermore, the RAN and SA plenaries exchanged liaisons in RP-252891 and SP-251268 for timely coordination and alignment, ensuring SA3 can send requirements to RAN2 that influence the AS protocol stack design for 6G radio.

Our proposal is to expand the 6G RAN security area to be more specific in its scope and prioritize study topic to influence 6G Radio study to be carried out in RAN WGs.

\* \* \* 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 area name> deals with <short description>

X) RAN **security** deals with the Access Statum security aspects of RAN architecture, protocol stack, interfaces, procedures, key derivation and key distribution among RAN nodes for protecting communication over the air

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

# 5 Key issues and solutions

## 5.x Security area #x: RAN security

### 5.x.1 Introduction

Purpose is to study potential attack vectors, vulnerabilities, security and privacy risks, impact and mitigations for future proof secure by design of the control plane and the user plane of the following 6G Radio Access Network areas:

NOTE: To be aligned and in coordination with RAN WG2 and RAN WG3 as 6G RAN study progresses in RAN WGs.

- L1/L2 Triggered Mobility (LTM). E.g., parameters related to functionality and security.

- Initial access procedure, random access procedures, system information and paging. E.g., synchronization, broadcast channel, cell (re) selection, timing advance measurement, access contention, unprotected SIB/MIB, paging channel attacks etc.

- Radio interface protocol architecture and procedures. E.g., functional split, key hierarchy, new interfaces and functions (if any), RRC, UP, PDCP, registration, subscriber privacy over the air etc.

- Mobility for all RRC states (e.g., connected, idle, inactive – as relevant for 6G radio)

Mobility between 5G NR and 6GR. E.g., downgrade, redirection and intergenerational handover.

- Security mechanisms for the interfaces between RAN and core network, including the protection of control plane data and user data transmission.

- Lower layer security for MAC layer, PHY layer, and their combination.

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