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

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

**Source: Ericsson, Huawei, HiSilicon, Beijing Xiaomi Mobile Software, Apple, ZTE Corporation, InterDigital France R&D SAS, Samsung, Nokia, Guangdong OPPO Mobile Telecom**

**Title: New Security Areas on 6G RAN Architecture Security, Secure RRC connection setup procedure, UE Initial message security and privacy, Lower Layer Security , MAC layer 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 security of RAN architecture, protocol stack, interfaces, procedures, key derivation and key distribution among RAN nodes for protecting communication over the air

X) RAN security area deals with various security aspects related to the access stratum in 6G network, i.e., evaluate and investigate possible security enhancements of the existing access stratum security mechanism.

X) Security area of RAN Architecture Security deals with all the security aspects introduced by the enhancement of 6G RAN architecture.

X) RAN security deals with any potential vulnerability or enhancement on the AS layer messages which are not protected in 5G.

X) RAN security deals with the security aspects of the 6G RAN, including radio interface protection, RAN node security and low-layer security.

X) **The RAN-security area** addresses confidentiality, integrity, availability, and privacy of control-plane and user-plane communications over the 6G radio interface, including support for advanced spectrum, NTN access, and new air interface technologies.

X) RAN security deals with the security for 6G radio interface and radio access network, UE to radio access network security, radio access network to core network security, lower layer security and AS security.

X) Protection of initial RRC messages exchanged between UE and BS.

X) Lower layer security deals with security threats in MAC layer, PHY layer, and their combination.

X) MAC layer security deals with any potential vulnerability or enhancement on the MAC layer which is not protected in 5G.

## 4.2 Potential high level security requirements

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

6G system should support the security mechanism to enhance the interaction between UE and RAN.

6GS shall ensure security of initial RRC messages exchanged between UE and BS for RRC connection setup.

6G system should support the security mechanism to protect the MAC layer.

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

# 5 Key issues and solutions

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

### 5.x.1 Introduction

Purpose is to study potential attack vectors, vulnerabilities, security risks, impact and mitigations for 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, 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.

The RAN security is a very important security area for 6G network. The RAN study item [xx] already include references to various security related topics. For example, the new 6G RAN design requires the development of related access security mechanism. The access stratum security aspects will impact the overall design of Radio interface protocol architecture and procedures for 6G.

Therefore, the RAN security area should consider all security aspects and identify the potential key issues, solutions to provide security protection for access stratum. In particular this security area deals with aspects such as:

- Security protection of control plane data and user plane data between the UE and RAN, for e.g., key hierarchy, security algorithm selection, security activation, mobility security.

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

- Security mechanisms for the interfaces connecting RAN nodes, including the protection of control plane data and user data transmission.

The evolution of RAN architecture is the primary motivation for investigating 6G RAN architecture security. The study of this security area depends on the progress of 6G RAN architecture design. The following parts could be included:

* AS security, including the key handling in mobility scenarios;
* Uu UP security;
* Lower-layer security;
* Security aspect of interface(s) between the 6G RAN and 6G CN and inside the 6G RAN.

The design of 6G AS security, including 6G AS key hierarchy, 6G AS security context handling, and 6G AS security establishment, etc, is closely tied to the deployment and functionality of the 6G CU and 6G DU. If the 6G CU and 6G DU are deployed separately or their protocol stacks are redesigned in 6G RAN, the AS security mechanisms need to be enhanced for accommodation. Furthermore, the security enhancement supporting UE mobility should also be studied, considering more flexible mobility cases in 6G (e.g. between terrestrial access and non-terrestrial access). How to ensure security during UE mobility while achieving fast handover remains a constant objective in 6G.

Another part of the study is the enhancement of the user plane security over Uu interface. Considering the split of CU-CP and CU-UP, UP security enhancement e.g. key isolation may need to be introduced. Also, the finer granularity of user plane security protection needs to be taken into account, since the 6G system as a complex ecosystem, is expected to have more flexible security design.

One more critical aspect of RAN architecture security is lower-layer security (e.g. MAC layer security). During the study of 5G LTM, several security threats due to the unprotected MAC CE have been identified. In 6G system, possibly more sensitive information may be transmitted via MAC CE, which further increases the security risk. Addressing these security threats of lower-layer transmission over the air interface is one of the important priorities in this security area.

If the new RAN or CN architecture design impacts the interface(s) between the 6G RAN and 6G CN and inside the 6G RAN, the security of these interfaces will need to be adjusted accordingly. For example, the security of interface between the split CU and DU, or between the split CU-CP and CU-UP, or between the RAN and CN impacts all the data and signaling transmitted over it. Therefore, the security of these interfaces is critical for study in 6G security.

In 4G/5G, AS security (encryption and integrity protection at PDCP) is activated only after the AS SMC procedure, leaving earlier AS messages (e.g., SIB/MIB, RRC Setup, RRC Reconfiguration, and initial NAS transport) unprotected.

The exposure will lead to security risks including: 1) DoS attack on UE, in which the attackers attempt to hinder the UEs' access to the network. for example, modify system information to misdirect UEs to malicious cells, enabling man-in-the-middle (MitM) attacks; Forge RRC reconfiguration commands to force UEs into insecure modes (e.g., disabling 6G advanced security features). 2) DoS attack on network, in which the attackers attempt to hinder the network's ability to provide services to the UEs. 3) Rogue services, in which the attackers attempt to deliver unauthorized or unsolicited services (e.g., SMS and calls) to the UEs. 4) Subscriber privacy attack, in which the attacker attempt to identify subscriptions or trace the UEs.

When considering the enhancement on the RAN security using asymmetric cryptos, it is necessry to consider the PQC for future proof. Even though the PQC algorithms may introduce longer signture (e.g. ML-DSA(Module Lattice-Based Digital Signature Algorithm) signature is 2410Byte~4627 byte), 6G system shall ensure the new designed mechanism to defend long-term threats.

In 4G/5G, AS security (encryption and integrity protection at PDCP) is activated only after the AS SMC procedure, leaving earlier AS messages (e.g., SIB/MIB, RRC Setup, RRC Reconfiguration, and initial NAS transport) unprotected.

The exposure will lead to security risks including: 1) DoS attack on UE, in which the attackers attempt to hinder the UEs' access to the network. for example, modify system information to misdirect UEs to malicious cells, enabling man-in-the-middle (MitM) attacks; Forge RRC reconfiguration commands to force UEs into insecure modes (e.g., disabling 6G advanced security features). 2) DoS attack on network, in which the attackers attempt to hinder the network's ability to provide services to the UEs. 3) Rogue services, in which the attackers attempt to deliver unauthorized or unsolicited services (e.g., SMS and calls) to the UEs. 4) Subscriber privacy attack, in which the attacker attempt to identify subscriptions or trace the UEs.

When considering the enhancement on the RAN security using asymmetric cryptos, it is necessry to consider the PQC for future proof. Even though the PQC algorithms may introduce longer signture (e.g. ML-DSA(Module Lattice-Based Digital Signature Algorithm) signature is 2410Byte~4627 byte), 6G system shall ensure the new designed mechanism to defend long-term threats. The security area “RAN security” covers security aspects related to 6GR based on study progress in TR 38.xxx.

Editor’s note: The TR number is to be updated when the 6G RAN study specification is available.

In particular, this security area deals with aspects such as:

* Protection of control plane and user plane between the UE and the RAN.
* Protection of control plane and user plane between the RAN and CN.
* Protection of control plane and user plane between base stations.
* Protection of low-layer protocols including MAC layer.

RAN Security addresses the protection of information exchanged over the Uu interface, including confidentiality, integrity, replay protection, and associated key management functions (agreement, derivation, and change). In 5G, Access Stratum (AS) security is applied at the PDCP layer located in the CU, which allows protection of higher-layer signaling such as RRC messages and user-plane data, but does not cover lower-layer information elements such as MAC Control Elements (MAC CEs). Consequently, current 5G AS security provides protection only for dedicated RRC messages in RRC\_CONNECTED mode and for user-plane traffic, while other control information remains unprotected.

For 6G, it may be necessary to study the location and granularity of security mechanisms across RAN protocol layers. In particular, procedures such as L1/L2-Triggered Mobility (LTM), which rely heavily on MAC CEs, may benefit from protection at the MAC layer. Introducing security functions at this level could enable either selective protection of individual MAC information elements or protection of the entire MAC payload, potentially leading to the definition of a third security stratum (MAS). It is also desirable to study mechanisms that allow more flexible and fine-grained establishment of security contexts than currently available, so that bearer configuration, key management, and security policy can be aligned with the varying capabilities of UEs and RAN nodes.

This security area addresses 6G Radio Access Network security which includes end-to-end security protection of communication between UE and 6G RAN nodes i.e., protection of control plane and user plane traffic between UE and 6G RAN, enhancement to user plane security policy, protection of control and user plane traffic between 6G RAN node and core network and security for split 6G RAN architecture. This security area further deals with aspects such as AS security context management, security algorithm negotiation for AS security establishment and handling of AS security context for mobility, handovers and so on.

Further, ensuring that a UE can verify the legitimacy of its serving base station remains a persistent challenge that was not resolved in 5G. This vulnerability is becoming more critical, as the public release of open-source software for base station implementation, combined with accessible radio hardware, has significantly lowered the technical barrier for attackers to create sophisticated false base stations (FBS). A FBS can impersonate as a legitimate 6G base station to deceive UE into camping on it which opens way for diverse attacks. It is most feasible to undertake this issue and address it at the beginning of a new mobile generation. Other RAN related issues such as unprotected MAC CE (e.g., LTM commands) in 6G creates critical vulnerabilities. Attackers can exploit these gaps to manipulate UE behaviour (e.g., desynchronize timing, force handovers to malicious cells) and trigger service denial. Support for security protection at lower layer in 6G RAN is also scoped under this security area. Further, unprotected messages before security mode command could lead to misconfigured UE, in 6G initial RACH and RRC setup messages needs to be considered.

## 5.x Security area #x: UE Initial message security and privacy

### 5.x.1 Introduction

The initial messages exchanged between the UE and the Base Station is not security protected, until the UE is authenticated, and UE specific AS security is established. This lack of security and privacy for the initial messages creates a problem for the UE from including any sensitive information such as S-NSSAI, device type, location information of the UE etc in the RRC Msg5, which carries the initial NAS REG-REQ message. In many scenarios such parameters are needed from the UE at the network elements such as base station, to route the initial NAS REG-REQ to the proper Network Slice or AMF. Hence providing security between legitimate UEs and any legitimate Base station of the network even before the UE gets authenticated and establishes UE specific AS security context is increasingly becoming important in multiple features such as Non-Terrestrial Networks (NTN), Network Slicing etc.

This security area focusses on security of Msg3, Msg4 and Msg5 exchanged between the UE and the Base Station.

## 5.x Security area #x: MAC layer security

5.x.1 Introduction

Editor's Note: Detailed description of the security area

5G AS security functionality is in PDCP layer and there is no protection in the MAC layer.

The ciphering function in PDCP includes both ciphering and deciphering and is performed in PDCP, if configured. The data unit that is ciphered is the data part of the PDCP Data PDU except the SDAP header and the SDAP Control PDU if included in the PDCP SDU, and the MAC-I. The ciphering is not applicable to PDCP Control PDUs.

The integrity protection function includes both integrity protection and integrity verification and is performed in PDCP, if configured. The data unit that is integrity protected is the PDU header and the data part of the PDU before ciphering. The integrity protection is always applied to PDCP Data PDUs of SRBs. The integrity protection is applied to PDCP Data PDUs of DRBs for which integrity protection is configured. The integrity protection is not applicable to PDCP Control PDUs.

MAC CE is generated directly in MAC layer, thus can not be protected by PDCP layer security even if UE establishes an RRC connection and configures security parameters. A bunch of security issues have been spotted, for example in the LS from GSMA LS [x], UE location information can be leaked to an unauthorized adversary stealthily through the SLIC attack[Y]. The attacker can achieve this by passive eavesdropping - comparing the path an arbitrary user takes to other known paths within a building served with multiple secondary cells connected to a primary cell. Another example is in the LTM feature (Layer 1/Layer 2 triggered mobility), where handover signaling sent by the network to the UE via MAC CE. There are unprotected critical information carried in MAC CE, including the configuration information and key derivation information, which could lead to the tempering and potential attacks.

To address the security risks of MAC layer in 6G, it is proposed to add extra security on the MAC layer, at least on the MAC CE, including confidentiality, integrity, and replay protection.

### 5.x.2 Security assumptions

It is assumed that RAN security shall continue to provide confidentiality, integrity, and replay protection for information exchanged over the Uu interface, with associated support for key management (agreement, derivation, and update).

In current systems, Access Stratum (AS) security is applied at the PDCP layer, protecting RRC signalling and user plane traffic. Other lower-layer elements, such as MAC Control Elements (MAC CEs), are not protected.

For 6G, the placement of security functions across RAN protocol layers may need to be reassessed. It is assumed that protection of MAC-layer information, particularly in procedures such as L1/L2-Triggered Mobility, could be beneficial and may lead to the consideration of a new MAC-layer Access Stratum (MAS).

It is further assumed that more flexible and fine-grained mechanisms for establishing and controlling security contexts may be required, allowing selective protection of individual protocol elements or bearers, in line with the capabilities of UEs and RAN nodes.

\* \* \* 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] S3-211382-FSAG Doc 88\_009-User location identification from Carrier Aggregation secondary cell activation messages

[Y] <https://www.usenix.org/conference/usenixsecurity21/presentation/lakshmanan>

[X] “The Security Overview and Analysis of 3GPP 5G MAC CE”, Jin Cao, yuanyuan Yang, Ruhui Ma, Shen li, Hui Li, June 2025, available at <http://arxiv.org/abs/2506.09502>

[Y] Norbert Ludant, Marinos Vomvas, Guevara Noubir : “Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous” : <https://arxiv.org/html/2403.06717v1>

[Z] Next G Alliance Report: 6G Technologies : <https://nextgalliance.org/white_papers/6g-technologies/>

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