**3GPP TSG-SA3 #6G Study workshop S3-25xxxx**

**Conference Calls, 6 - 7 August 2025**

**Source: ZTE**

**Title: New Study on MAC layer security**

**Document for: Approval**

**Agenda Item:**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on MAC layer security

Acronym: FS\_MAC-Sec

Unique identifier:

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-20

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  | X | X | X |  |
| No |  |  |  |  |  |
| Don't know | X |  |  |  | X |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

{Tick one or more box(es). The full structure of all existing Work Items is shown in the 3GPP Work Plan in <https://ftp.3gpp.org/Information/WORK_PLAN>}

|  |  |
| --- | --- |
| X | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A |  |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
| N/A |  | {optional free text} |

**Dependency on non-3GPP (draft) specification:**

N/A

# 3 Justification

The MAC layer enables the dynamic management of radio resources and coordination of communication between the UE and base stations by using MAC CEs to carry control information. Unlike higher-layer protocols (e.g., RRC or NAS), MAC CEs are transmitted without encryption or integrity protection, prioritizing low latency and efficiency over security.

According to the LS [1], SA3 agreed to transmit NCC using the LTM cell switch command MAC CE in the inter-CU LTM scenario. However, the lack of protection for the MAC CE makes the NCC susceptible to eavesdropping or manipulation, which increases the likelihood of handover failures.

Given that over 80 distinct MAC CEs are utilized in 5G NR for diverse control functionalities, the number and types of MAC CEs are expected to increase further to support more complex network functions, higher flexibility, and more extreme performance requirements in 6G.  A comprehensive security evaluation is necessary for MAC CEs to determine their security requirements. For instance, MAC CEs that transmit critical control information, such as Timing Advance adjustments and SCell activation/deactivation details, plaintext transmission without integrity and/or confidentiality protection makes the control information easy to be eavesdropped and manipulated by the attackers, leading to privacy leakage and even link interruption [2, 3]. On the other hand, MAC CEs that convey less critical information, like Duplication Activation/Deactivation indications and recommended bit rates, do not present significant security threats in the absence of protection [2]. Therefore, implementing security measures for these types of MAC CEs may be considered optional.

To address these varying security needs, it is important to conduct a systematic security analysis to identify the security requirements for MAC CEs and provide a scalable and lightweight security protection mechanism for critical MAC CEs to balance the need for low latency with security considerations.

1. S3-251124 Reply LS on security handling for inter-CU LTM in non-DC cases
2. TS 38.321
3. Ludant N, Vomvas M, Noubir G. Unprotected 4G/5G Control Procedures at Low Layers Considered Dangerous[J]. arXiv preprint arXiv:2403.06717, 2024.

# 4 Objective

Based on the above justification, the following objectives will be studied:

* WT1: Study threats and security requirements for MAC CE in 6G
  + Identify use cases for MAC CE protection
  + Identify security requirements for MAC CE messages.
* WT2: Study key issues and candidate solutions for MAC CE security protection for 6G

NOTE: The solutions need to consider the forward compatibility due to the continuous expansion of MAC CE types in future 6G releases.

## TU estimates and dependencies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Work Task ID | TU Estimate  (Study) | TU Estimate  (Normative) | RAN Dependency  (Yes/No/Maybe) | Inter Work Tasks Dependency |
| WT #1 | 2 | N/A | Yes | N/A |
| WT #2 | 2 | TBD | Yes | N/A |

Total TU estimates for the study phase: 4

Total TU estimates for the normative phase: TBD

Total TU estimates: TBD

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| Internal TR | 33.XXX | Study on MAC layer security | TSG#110, Dec. 2025 | TSG#111, Mar. 2026 | TBD |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

tbd

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Potential interaction with RAN WGs for RAN related issues.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| ZTE |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |