**3GPP TSG-SA3 Meeting #124 draft S3-253733-r1**

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

**Source: Xiaomi**

**Title: New solution on protection for DL NAS message of authenticated UE in split-MME architecture**

**Document for: Approval**

**Agenda item: 5.2.9**

**Spec: 3GPP TR 33.700-30**

**Version: 0.1.0**

**Work Item: FS\_5GSAT\_Ph4\_SEC**

**Comments**

This contribution proposes to introduce a new solution for FS\_5GSAT\_Ph4\_SEC, which provides a method for protecting the DL NAS messages of authenticated UE in the split-MME architecture.

\* \* \* First Change \* \* \* \*

## 6.Y Solution #Y: Protection for DL NAS message of authenticated UE in split-MME architecture

### 6.Y.1 Introduction

This solution is proposed to address Key Issue #1, providing a protection method for exchanging the NAS message in the Store and Forward satellite operations.

As specified in TS 33.401 [3], the NAS security is terminated on the MME-onboard, and the ground segment of the network ensures that the latest NAS security context of the UE is available at the MME-onboard. When multiple satellites are involved in the Store and Forward satellite operation, the NAS COUNTs should be synchronized to mitigate the replay attack.

This solution proposes that NAS COUNTs are maintained and managed by the UE and MME-ground. When a DL NAS message of authenticated UE is received, the MME-ground is responsible for selecting the MME on-board based on the coverage availability information. In other words, the MME-ground selects the MME on-board that will be available to the UE earliest. For the selected MME on-board, the MME-ground provides the value of DL NAS COUNT together with the DL NAS signaling. Since the selection is based on the coverage availability information, the MME on-board(s) will be available for UE in sequence and the value of DL NAS COUNT will be received in order, which mitigates the replay attack in the Store and Forward satellite operations.

### 6.Y.2 Solution details



Figure 6.Y.2-1: Protection for DL NAS messages of authenticated UE

1. The UE and MME-ground hold the latest NAS COUNTs, including the UL NAS COUNT and DL NAS COUNT.

At Time 1:

1. The MME-ground receives the DL NAS signaling #1 of the authenticated UE from another EPS NF.
2. Based on the coverage availability information, the MME-ground selects one of the MME on-board(s) (e.g. MME on-board the SAT1) to transmit the DL NAS signaling #1.
3. The MME-ground sends the DL NAS signaling #1 together with the latest value of DL NAS COUNT (e.g. DL NAS COUNT #1), and increases the DL NAS COUNT by one.

If the service link is not available, the MME on-board the SAT1 stores the DL NAS COUNT #1 together with the DL NAS signaling #1.

At Time 2:

1. The MME-ground receives the DL NAS signaling #2 of the authenticated UE from another EPS NF.
2. Based on the coverage availability information, the MME-ground selects one of the MME on-board(s) (e.g. MME on-board the SAT2) to transmit the DL NAS signaling #1.
3. The MME-ground sends the DL NAS signaling #2 together with the latest value of DL NAS COUNT (e.g. DL NAS COUNT #2), and increases the DL NAS COUNT by one.

If the service link is not available, the MME on-board the SAT2 stores the DL NAS COUNT #2 together with the DL NAS signaling #2.

At Time 3 and Time 4, the UE can receive the protected DL NAS message in sequence.

1. Once the service link becomes available (Time 3), the MME on-board the SAT1 generates the integrity-protected and confidentiality-protected NAS signaling #1 and sends it to the UE.

NOTE 1: Time 3 may happen before Time 2. In this case, Step #7 is performed before Steps #4-6.

1. Once the service link becomes available (Time 4), the MME on-board the SAT2 generates the integrity-protected and confidentiality-protected NAS signaling #2 and sends it to the UE.

Editor’s Note: The NAS count synchronization when the UE receives messages from multiple MME-onboards is FFS.

Editor’s Note: How to protect UL NAS messages is FFS.

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

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