**3GPP TSG-SA3 Meeting #124 draft S3-253734-r2**

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

**Source: Huawei, HiSilicon, Samsung**

**Title: New Solution for securing NAS messages via using different NAS keys in multiple satellites**

**Document for: Approval**

**Agenda item: 5.2.9**

**Spec: TR 33.700-30**

**Version: 0.0.0**

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

**Comments**

This solution is to addresses “Key issue #1: Authenticated UE to exchange NAS messages with multiple satellites in split-MME architecture”. The basic idea is to use different NAS keys when UE exchanges data with multiple satellites.

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |
| --- | --- |
|  | Key Issues |
| Solutions | 1 | 2 | 3 | 4 | 5 | 6 | 7 |  |
| Y | X |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

\* \* \* Second Change \* \* \* \*

## 6.Y Solution #Y: Secure NAS messages via using different NAS keys in multiple satellites

### 6.Y.1 Introduction

This solution addresses “Key issue #1: Authenticated UE to exchange NAS messages with multiple satellites in split-MME architecture”.

This solution is based on split MME architecture. S&F Satellite operation may involve multiple satellites allocated by an S&F Monitoring List. In order to prevent reusing key stream, one possible approach is to use different NAS keys when UE interacts with different satellites. This solution can improve the data exchange efficiency of the entire system.

### 6.Y.2 Solution details

Based on the existing authentication procedures, this solution proposes to use different NAS keys when UE exchanges data with multiple satellites.



Figure 6.Y.2 Enhanced NAS security for multiple satellites in S&F mode

SAT#1 has available Service Link.

1. The UE sends the Attach Request to SAT#1.
2. If SAT#1 does not have context to authenticate the UE, then sends the Attach Reject.

SAT#1 has available Feeder Link.

1. SAT#1 sends the Attach Request to the MME-ground.
2. The MME-ground obtains authentication data including KASME, as defined in TS 33.401 [3].
3. The MME-ground determines to use SAT#1 to serve UE, then the MME-ground calculates KASME1\* by using KASME and SAT Id of SAT#1.
4. The MME-ground distributes KASME1\* for SAT#1 during the transmission of AV.

SAT#1 has available Service Link.

1. The authentication procedure is completed, as defined in TS 33.401 [3].
2. SAT#1 derives NAS keys based on the KASME1\* using existing mechanism as defined in TS 33.401[3] and sends the NAS security mode command integrity protected.
3. The UE calculates KASME1\* using the same method as the MME-ground in step5, and further derives the NAS keys using existing mechanism as defined in TS 33.401[3], then the UE verifies the NAS security mode command.
4. If successfully verified, the UE sends the NAS security mode complete to SAT#1.
5. After the NAS SMC procedure, the UE and SAT#1 send protected NAS messages.

SAT#2 has available Feeder Link.

1. The MME-ground determines to use SAT#2 to serve the UE, the MME-ground calculates KASME2\* by using KASME and SAT Id of SAT#2.
2. The MME-ground distributes KASME2\* for SAT#2. Then SAT#2 derives the NAS keys by using KASME2\*.

SAT#2 has available Service Link.

1. The UE calculates KASME2\* using the method as the MME-ground in step12, and further derives the NAS keys by using KASME2\*.
2. The UE and SAT#2 send protected NAS messages.

Editor’s Note: Whether and how to activate the new NAS key between the UE and SAT2 is FFS.

Note: As described in TS 23.401[2], the MME-ground together with the associated MME-onboard(s) behave jointly as a single MME entity. For multiple satellites, assume MME-onboards have the same list of ordered NAS security algorithms. After NAS SMC, the selected NAS security algorithms could be synchronized for MME-onboards.

Note: Each satellite/UE pair maintains independent COUNTs.

Editor’s Note: Wrap-around issue for the independent COUNTs is FFS.

Editor’s Note: The detail on securing NAS messages using different NAS keys during handover-like process is FFS.

### 6.Y.3 Evaluation

Editor’s note: Impact for key separation at UE and MME on ground is FFS.

Editor’s note: Whether the UE computes a new NAS security context each time it connects to a new satellite is FFS.

TBD.

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