**3GPP TSG-SA3 Meeting #124 S3-253730**

**Wuhan, China, 13 – 17 October 2025 *(revision of S3-253238)***

**Source: Sateliot, Novamint**

**Title: Solution to KI#1: Separate NAS COUNT pairs per satelliteID**

**Document for: Approval**

**Agenda item: 5.2.9**

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

**Version: 0.1.0**

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

# 1 Decision/action requested

***Approve the pCR below***

# 2 References

# 3 Rationale

This pCR is a solution proposal to solve Key Issue #1: “Authenticated UE to exchange NAS messages with multiple satellites in split-MME architecture”

# 4 Detailed proposal

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

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 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** |  |
| **1** |  |  |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |  |  |
| **3** |  |  |  |  |  |  |  |  |
| **4** |  |  |  |  |  |  |  |  |
| **Y** | X |  |  |  |  |  |  |  |

## 6.Y Solution #Y: Separate NAS COUNT pair per SatelliteID within an EPS Security Context

### 6.Y.1 Introduction

This solution addresses Key Issue #1.

This solution is based on using separate pairs of NAS counters per Satellite ID in the EPS security context when the UE is served by multiple satellites operating in S&F mode and the UE registration remains valid even the serving satellite changes over time (i.e., the UE is not required to attach/detach in each satellite pass). The list of SatelliteID(s) in which the registration is valid is provided to the UE using the S&F Monitoring List.

### 6.Y.2 Solution details

This solution applies to a satellite network operating in S&F mode and, it’s especially relevant for deployments based on the split MME architecture (see TS 23.402 Annex O.2) in which a UE registration remains valid across multiple satellites (unlike a full EPC deployment, where registration is only valid in one satellite).

The solution consists of enabling an option for the UE to use separate pairs of NAS counters (i.e. *UL\_NAS\_Count* and *DL\_NAS\_Count*) per SatelliteID within its EPS security context, where:

* *SatelliteID* is an identifier uniquely indicating an MME-onboard. The SatelliteID identifier of a given satellite is broadcast by the eNB within the SIB31 and the SatelliteID identifiers of the satellites that might be serving a given UE are included within the S&F Monitoring List, which is sent by the MME to indicate the satellite(s) that the UE may (re)-attempt NAS procedures (TS 23.401 clause 4.13.9.1)
* *UL\_NAS\_Count* is the uplink NAS counter related to the uplink NAS messages sent to the MME-onboard associated with *SatelliteID*.
* *DL\_NAS\_Count* is the downlink NAS counter related to the downlink NAS messages received from the MME-onboard associated with *SatelliteID*.

On the network side, this solution allows each MME-onboard to independently maintain its own pair of NAS counters*,* which shall no longer to be synchronised across the subset of theMME-onboard instances (identified each by a SatelliteID) that belong to the same logical MME in charge of the registered UE. This is depicted in Figure 6.Y.2-1, which is based on Figure O.2-1: "Split-MME" architecture for supporting Store and Forward Satellite operation for SMS and CP CIoT services” in Annex O.2 in TS 23.401.

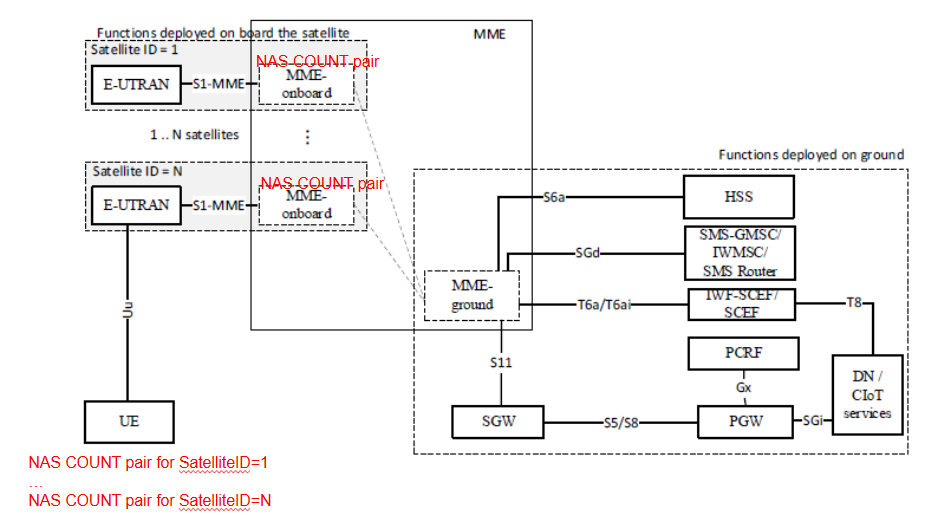


Figure 6.Y.2-1: Illustration of the solution consisting on using separate NAS COUNT pairs per SatelliteID

Given Rel-19 UEs will still assume that NAS counters are synchronised across the satellites of the S&F Monitoring List, the proposed solution should be introduced as an optional capability. Therefore, UE is expected to indicate to the network that UE supports separate NAS counters per SatelliteID and the network (NW) should be able to indicate the UE whether this option is activated (i.e. the UE should use separate NAS counters per SatelliteID) or deactivated (i.e. the UE shall assume NAS counters are kept synchronised).

Finally, another element to consider in this solution is the use of the “SatelliteID” value as part of the NAS COUNT 32-bit value. For example, the padding bits of the NAS Count can be filled with the SatelliteID, as illustrated in Figure 2. In this way, a NAS message used between the UE and a given satellite cannot be replayed with another satellite.

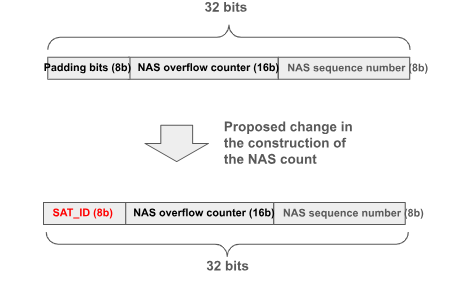


Figure 6.Y.2-2: Filling NAS COUNT padding bits with SatelliteID

Editor’s Note: FFS whether the solution should also consider the use of the “SatelliteID” value as part of the NAS COUNT 32-bit value so that NAS count values are never reused.

Editor’s Note: How to address the wrap-around issue of independent COUNTs is FFS.

Editor’s Note: How to activate the security context between the SAT (e.g. SAT#2, SAT#n) and UE is FFS.

Editor’s Note: FFS whether the capability to indicate the UE should use separate NAS counters per SatelliteID is optional or mandatory

### 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 \* \* \* \*