**3GPP TSG-SA3 Meeting #124 draft\_S3-253727-r1**

**Wuhan, China 13th - 17th October 2025**

**Source: ZTE, OPPO**

**Title: New solution on NAS Security Context Isolation via Satellite-Specific NAS COUNT**

**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**

The contribution proposes to add a new solution for key issue #1.

**Proposed Changes**

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.Y Solution #Y: NAS Security Context Isolation via Satellite-Specific NAS COUNT

### 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 proposes a mechanism ensuing different satellite using different COUNT to protect NAS message and therefore eliminates the need for real-time NAS COUNT synchronization across satellites.

### 6.Y.2 Solution details

This solution is based on the following assumptions and principles:

- the UE and each MME-onboard maintain independent pairs of NAS COUNTs (one for uplink, one for downlink) for their mutual communication. The NAS COUNTs are not synchronized with other satellites.

Based on the above principle, the existing procedures are reused to protect the NAS message between the UE and the network. The NAS integrity and confidentiality protection algorithms are same as defined in TS 33.401 [x], with the following modification to the construction of the 32-bit COUNT input parameter:

For a serving Satellite n:

COUNT := Satellite ID n || NAS OVERFLOW || NAS SQN

Where

- Satellite ID n is the 8-bit ID of Satellite n which is an identifier uniquely indicating an MME-onboard coded as a binary coded integer value from 0 to 255 as specified in 3GPP TS 24.301 [x]. 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)

- NAS OVERFLOW is a 16-bit value which is incremented each time the NAS SQN is incremented from the maximum value. It is maintained for the connection with Satellite n.

- NAS SQN is the 8-bit sequence number carried within each NAS message between UE and MME-onboard n. It is maintained for the connection with Satellite n.

All other input parameters (KEY=KNASint/KNASenc, BEARER, DIRECTION, LENGTH) and the algorithm execution remain unchanged.

Editor’s Note: How to deal with the warp around case is FFS.

Editor’s Note: How the MME-ground manages and reconciles the multiple UE security context of the same UE for multiple satellites is FFS.

### 6.Y.3 Evaluation

TBD

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the first change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\* \* \* Second 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".

[2] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

[x] 3GPP TS 24.301: " Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

\* \* \* End of Change \* \* \* \*