**3GPP TSG-SA3 Meeting #124 draft\_S3-253725-r2**

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

**Source: ZTE**

**Title: New solution on Derivation of Satellite-Specific NAS keys for S&F Operation**

**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: Derivation of Satellite-Specific NAS keys for S&F Operation

### 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 to derive unique NAS integrity and encryption keys for each satellite by using the satellite ID as an additional input parameter during the NAS key derivation.

### 6.Y.2 Solution details

In this solution, it is proposed to derive distinct set of NAS keys for each satellite from the common root key KASME. The satellite-specific NAS keys are derived by the UE and the network using the KDF as specified in TS 33.220 [x].

For a serving Satellite n, the NAS integrity key KNASint and the NAS encryption key KNASenc are derived from the KASME with the following parameters as input:

- FC = 0xxx

- P0 = algorithm type distinguisher

- L0 = length of algorithm type distinguisher (i.e. 0x00 0x01)

- P1 = algorithm identity

- L1 = length of algorithm identity (i.e. 0x00 0x01)

- P2 = Satellite ID n.

- L2: length of Satellite ID n.

Where Satellite ID is an identifier uniquely indicating an MME-onboard. The Satellite ID of a given satellite is broadcast by the eNB within the SIB31 and the Satellite ID 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).

As a result of using satellite-specific keys, the UE and each MME-onboard maintain independent pairs of NAS COUNT for their mutual communication. The NAS COUNTs are not synchronized with other satellites.

Editor’s Note: When the NAS keys are generated in UE and MME-onboard is FFS.

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.

Editor’s Note: How to indicate to the UE whether the solution of the separate NAS keys is implemented or not is FFS.

### 6.Y.3 Evaluation

TBD

Editor’s Note:The impact for key generation on MME-onboard is FFS.

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