**3GPP TSG-SA3 Meeting #123 draft\_S3-252748-r3**

**Goteborg, Sweden, 25 - 29 August 2025** *revision of* *S3‑252625, S3‑252744, S3‑252748, S3‑252776*

**Source: CATT, Sateliot, Novamint, ZTE, OPPO, Huawei, HiSilicon**

**Title: New KI for TR Satellite Phase 4**

**Agenda Item: 6.1.10**

# 1 Decision/action requested

***Approve the pCR below***

# 2 References

# 3 Rationale

# 4 Detailed proposal

#### \*\*\* BEGIN CHANGES \*\*\*

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.2 Key Issue #X: Authenticated UE to exchange NAS messages with multiple satellites in split-MME architecture

### 5.2.1 Key issue details

One of the architectural assumptions for Store and Forward Satellite operation is that when the service link is available, there is no feeder link and inter satellite link. There are two example deployment options for Store and Forward Satellite operation given in Annex O of TS 23.401 [i1], i.e. Split MME architecture and Full EPC in each satellite.

For the split-MME architecture, S&F Satellite operation may involve multiple satellites allocated by an S&F Monitoring List. In this scenario, the UE context needs to be synchronized between the multiple MME-onboard(s) and the associated MME-ground. The synchronization of UE context between the MME-ground and MME-onboard(s) is out of the scope of 3GPP.

According to Annex N of TS 33.401 [i2], regular LTE procedures are used to provide security between UE and network for the split-MME architecture. This means that once the UE completes an interaction with a satellite, the UE context in the satellite must be synchronized to other satellites before these satellites can perform any subsequent S&F Satellite operations with the UE. This significantly reduces the data exchange efficiency of the entire system.

Ideally, for an IoT device, once it is registered in the network and its UE context has been distributed to the satellites included in the S&F Monitoring List, the UE can exchange data with these satellites without the need for UE context synchronization between the satellites.

This key issue focuses on solutions that meet the following conditions:

- The UE context of the UE registered in the network has been provided to the satellites included in the S&F Monitoring List;

- The UE can perform Mobile Originated (MO) or Mobile Terminated (MT) data transmission with the satellites that have the UE context;

- The UE context does not need to be synchronized across the multiple satellites for supporting the MO/MT data transmissions. However, UE context synchronization may still be required for other changes not being associated with the MO/MT data transmission.

### 5.2.2 Security threats

If the NAS COUNTs are not synchronized across multiple satellites, an attacker may intercept and replay previously transmitted NAS messages. Since different satellites may accept outdated NAS COUNT values, the replay protection mechanism could be bypassed, leading to unauthorized actions.

Key stream may be reused if the security contexts are not well-managed across multiple satellites, for example, a single NAS COUNT is reused for all satellites, or same security key/keyset is shared among all satellites.

If same security materials are shared among all satellites and one of these satellites is compromised, the security materials would have to be re-established in all other satellite.

### 5.2.3 Potential security requirements

The 3GPP system shall support means to prevent the key stream reuse in store and forward satellite operations.

#### \*\*\* NEXT 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".

[i1] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[i2] 3GPP TS 33.401: "3GPP System Architecture Evolution: Security Architecture".

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

#### \*\*\* END OF CHANGES \*\*\*