**3GPP TSG-SA3 Meeting #115AdHoc-e *S3-241309***

Electronic meeting, online, 15 - 19 April 2024

**Source: Huawei, HiSilicon**

**Title: Solution on the security protection for store and forward Satellite Operation**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

***Approve the pCR to TR 33.700-29***

# 2 References

N/A

# 3 Rationale

For the uplink user plane data, if the on-board RAN node is not able to verify its integrity, it is hard to detect whether the data is sent from genius UE or attacker. All the uplink data need to be stored during the feeder link’s unavailability. Hence, the storage capacity can be easily exhausted by fake data with the attack over the air.

To address the potentioal risk above, it is proposed to activate the user-plane integrity protection as much as possible. In the on-board RAN side, the data with successful verification will be stored with priority

# 4 Detailed proposal

\*\*\* Start of 1st Change \*\*\*

## 6.Y Solution #Y: <Security protection for store and forward Satellite Operation >

### 6.Y.1 Introduction

Key issue#1 is addressed by this solution. Currently, integrity protection of the user data between the UE and the on-board RAN node is optional to use. For example, the integrity protection may be not activated by the on-board RAN node based on the security policy or local configuration. Without integrity verification, fake data may be stored in the on-board RAN node.

This solution addresses store and forward Satellite Operation in the delivery of delay-tolerant/non-real-time satellite services (i.e. CIoT UP Optimizations).

### 6.Y.2 Solution details

In addition to the UP integrity protection policy, the on-board RAN node also considers whther store and forward Satellite Operation is supported or not when activating UP integrity protection. If supported, the integrity protection is activated as much as possible. For example, if the UP integrity protection policy is “preferred”, the integrity protection will be activated.

If the feeder link is not available, the data after integrity verification will be stored with priority in the on-board RAN node. For example, if the storage of the on-board RAN node reach the warning thredshold, only data after integrity verification will be stored.

NOTE: how to prevent DoS attacks before the security context is established between UE and network is out of scope of this solution.

Editor’s Note: details on how data is stored with priority in the on-board RAN node are FFS.

Editor’s Note: how to process the stored data once the warning threshold is reached is ffs.

Editor’s Note: Whether a UE needs to be made aware of changes in the on-board RAN’s storage behaviour is FFS.

### 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 1st Change \*\*\*