**3GPP TSG-SA3 Meeting #116 *draft\_S3-242545-r2***

Jeju, South Korea, 20th - 24th May 2024 revision of S3-241973

**Source: Huawei, HiSilicon**

**Title: Addressing the editor's note and adding evaluation in solution 18**

**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

There is several Editor’s Notes in the solution 18. This contribution proposes to add clarification on this part.

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

Clarification: it’s left to RAN’s implementation. For example, before the storage of the on-board RAN node reach the warning thredshold, all the data is treated equally. After reaching the warning thredshold, only data after integrity verification will be stored

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

Clarification: it’s left to RAN’s implementation. For example, the stored data will be kept.

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

Reply: No. Whether UP integrity protection is activated or not is decided by RAN. UE will follow the instruction from RAN side. So, UE is not required to be aware of such prioritization behaviour. RAN can decide to release the PDU session or activate the UP integrity protection based on local policy and implementation.

In addition, the evualtion is provided accordingly.

# 4 Detailed proposal

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

## 6.18 Solution #18: Security protection for store and forward satellite operation

### 6.18.1 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).

### 6.18.2 Solution details

In addition to the UP integrity protection policy, the on-board RAN node also considers whether 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 successful integrity verification will be stored with priority in the on-board RAN node. For the priority and process of the data storage, it is left to RAN’s implementation. For example, if the storage of the on-board RAN node doesn’t reach the warning thredshold, the data is treated equally. If the storage of the on-board RAN node reaches the warning thredshold, only data after successful integrity verification will be stored. RAN can decide to release the PDU session without integrity protection or activate the UP integrity protection based on implementation. In addition, the stored data will still be maintained without impact.

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

NOTE y: UE is not required to be made aware of changes in the on-board RAN’s storage behaviour.

### 6.18.3 Evaluation

This solution addresses store and forward Satellite Operation in the delivery of delay-tolerant/non-real-time satellite services. If only data after integrity verification is stored, the fake data from attacker will be discarded. Based on this, the potential DoS attack is mitigated.

Editor’s Note: additional evaluation is FFS

\*\*\* End of 1st Change \*\*\*