**3GPP TSG-SA3 Meeting #116 *draft\_S3-241940-r1***

**Jeju, Korea, 20 - 24 May 2024**

**Source: OPPO**

**Title: Add evaluation to Solution #12**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

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

# 2 References

[3] 3GPP TS 33.401

# 3 Rationale

This contribution proposes to add evaluation to Solution #12 of TR 33.700-29. As described in the evaluation, this solution fulfils all the potential requirements in key issue #1, thus the second sentence in Clause 6.12.1 is removed.

# 4 Detailed proposal

SA3 is requested to approve the following pCR.

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

## 6.12 Solution #12: Authentication for store and forward satellite operation

### 6.12.1 Introduction

This solution addresses Key Issue#1 on Security protection in Store and Forward Satellite Operation.

The solution is based on the EPS architecture. Considering the feeder link’s intermittent unavailability in the S&F Satellite operation, legacy EPS AKA as described in 3GPP TS 33.401 [3] may not be directly applied to such use case. To provide authentication capabilities when feeder link is not available, one possible approach is to have security credentials on the satellite, which enables the AKA procedure between the UE and the satellite. However, there is a security risk that the user security credentials (e.g. root keys) are stored on multiple satellites, for instance, if a satellite is hijacked, the user security credentials on other satellites can also be compromised. To mitigate this risk, the proposed solution takes into account the idea of subscriber key separation mechanism in Annex F “Isolated E-UTRAN Operation for Public Safety” in TS 33.401[3], where different satellites store different user security credentials.

In addition, due to the limited storage on satellites, storing all user subscription credentials in the onboard HSS is challenging and also difficult to manage. Therefore, it is possible that only a subset of UEs have their security credentials in the onboard HSS. If the UE accesses a satellite which has its security credential, the UE can proceed to run the AKA procedure, otherwise the authentication request is rejected due to the lack of UE security credential. Meanchile, the satellite can record the rejected UE and retrieve its security credentials from the ground HSS when feeder link is available. Then, the UE can access the satellite and continue to perform AKA procedure when the service link is available.

The proposed solution follows the assumptions and principles as below:

- The eNB, MME-NT and HSS-NT are placed on board the same satellite.

- The HSS-NTs for multiple satellites use subscriber key separation mechanism in Annex F in TS 33.401[3].

- The HSS-NT may only have security credentials for a subset of users.

- The HSS-NT retrieve the unstored user security credentials from the ground HSS when feeder link is available.

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

\*\*\* Start of 2nd Change \*\*\*

### 6.12.3 Evaluation

This solution fulfils all the potential requirements in key issue #1 for security protection in S&F Satellite operation.

This solution, by deploying the HSS onboard the satellite, solves the problem of the incomplete AKA procedure due to the feeder link’s intermittent unavailability and enables the regular AKA process between the UE and satellite networks.

This solution proposes to reuse the subscriber key separation mechanism defined in Annex F.4 of TS 33.401[3] for provisioning the different subscriber keys in different satellites for the same UE.

Editor's Note: Further evaluation is FFS.

\*\*\* End of 2nd Change \*\*\*