**3GPP TSG-SA3 Meeting #116 *draft\_S3-241939-r1***

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

**Source: OPPO**

**Title: Updates 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 is to remove below Editor's Note in Solution #12 by adding the NOTE 1.

Editor’s note: It is FFS whether the solution can support roaming scenarios.

This contribution is also to fix the typo error in Figure 6.12.2-1, where the eNB onboard the SAT#2 instead of the eNB onboard the SAT#1 broadcasts in step 8.

# 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. Specifically, it addresses the first requirement in KI#1: “The 3GPP system shall support mutual authentication between the UE and the 3GPP network in the 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.

### 6.12.2 Solution details



Figure 6.12.2-1: Authentication for Store and Forward Satellite Operation

The authentication solution for Store and Forward Satellite Operation has the following steps:

1. The UE and the HSS-NTs for multiple satellites use subscriber key separation mechanism descriped in Annex F “Isolated E-UTRAN Operation for Public Safety” in TS 33.401 [3]. For each UE, there is a master key MK for S&F Satellite operation. The master key MK is stored in the UICC, but not in any HSS-NTs. Each HSS-NT is only provisioned with the subscriber keys (i.e., long-term key) derived from the master keys MKs for a subset of users. The HSS-T is provisioned with the the subscriber keys (i.e., long-term key) derived from the master key MK for all users.

NOTE 1: The master key MK can be a root key or a dedicated key exclusively for S&F Satellite operation.

NOTE 2: Assume that there are N satellites with different HSS-NTs, HSS-NT\_1, ..., HSS-NT\_N. As part of the provisioning process for HSS-NT\_n (1<=n<=N), a subscriber key K\_n is derived from MK using the key derivation process specified in Annex F of TS 33.401 [3], and all K\_n are different and the knowledge of K\_n does neither allow inferring knowledge about MK nor about any K\_m with m different from n.

NOTE 3: Due to the limited storage capability, the HSS-NT may only have the subscriber keys for a subset of users.

When service link between UE and SAT#1 is available

1. The eNB on the SAT#1 broadcasts that it is in the S&F satellite operation mode.
2. If the UE has the capability to support the S&F satellite operation, it initiates the Attach procedure by transmitting an Attach Request Message to the eNB including the UE ID, e.g., IMSI. Then, the eNB forwards the Attach Request message to MME-NT.
3. The MME-NT on the SAT#1 sends an Authentication Request message to HSS-NT on the SAT#1 including the UE ID.
4. If the subscriber key is not stored in the HSS-NT on the SAT#1, the HSS-NT sends an Authentication Failure Message to the MME-NT on the SAT#1 including a failure indication.
5. The MME-NT on the SAT#1 sends the Attach Reject message to UE.

When the feeder link between SAT#1 and the ground network is available

1. The HSS-NT on the SAT#1 sends the Security Key Request Message to the HSS-T including the rejected UE’s IMSI and current TAI, and retrieves the subscriber key from the HSS-T.
2. The HSS-T sends Security Key Reponse Message to HSS-NT on the SAT#1 with the subscriber key.

When service link between UE and SAT#2 is available

8~10. Step 8~10 are the same as step 1~3.

11~16. The run of an EPS AKA procedure in step 11~16 in the presence of the subscriber key separation mechanism is identical to that without the presence of the mechanism in clause 6.1 in 3GPP TS 33.401 [3], except for the operation of the step 11 and step 14. The modified operation is described as follows:

1. In step 11, If the HSS-NT on the SAT#2 has the the subscriber key, EPS AKA proceeds as described in clause 6.1 in 3GPP TS 33.401 [3], with the subscriber key replacing the permanent subscriber key in all computations;
2. In step 14, when the UE receives an Authentication Request Message from the MME-NT on the SAT#2, the USIM first derive the subscriber key from the master key using the key derivation process specified in Annex F in TS 33.401 [3], which can be locally stored for future use to improve efficiency. Then, EPS AKA proceeds as described in clause 6.1 in 3GPP TS 33.401 [3], with the subscriber key replacing the permanent subscriber key in all computations.
3. MME-NT on the SAT#2 sends an Attach Accept Message to the eNB. Then, the eNB forwards the Attach Accept message to the UE.

Editor’s note: It is FFS whether the solution can support roaming scenarios.

### 6.12.3 Evaluation

TBD

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