**3GPP TSG-SA3 Meeting #116  *S3-242059-r1***

**Jeju Island, S.Korea, May 20 – May 24, 2024**

**Source: Intel**

**Title: Updates to Secure Initial Registration for S&F Satellite Operation**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

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

# 2 References

# 3 Rationale

This contribution proposes updates to Satellite solution .

# 4 Detailed proposal

SA3 is requested to approve the following pCR.

\*\*\*\*\*START CHANGE\*\*\*\*\*

6.9 Solution #9: Secure Initial Registration for S&F Satellite Operation

6.9.1 Introduction

This solution specifically addresses the security considerations of Key Issue #1, which pertains to supporting Store and Forward Satellite operations. The Initial Attach / Initial Registration process is crucial for all S&F services. It must ensure the network's integrity and security despite the unique challenges posed by satellite communication, such as intermittent connectivity.

6.9.2 Solution details

Considering a scenario with a single Low-Earth Orbit (LEO) satellite providing intermittent coverage, this solution proposes modified MME functionality: one segment aboard the satellite (MME-SAT) and the other on the ground (MME-GND). This split architecture accommodates satellite coverage's intermittent connectivity and facilitates secure communication between the UE and the network.



**Figure 6.9.2-1: Initial Attach in satellite network for S&F operation**

1-3 Initial Registration Process: Upon entering the satellite's coverage, the UE initiates an Initial Attach Request. The MME-SAT, unable to immediately establish a ground connection, temporarily stores the UE's International Mobile Subscriber Identity (IMSI) and issues an Attach Reject message. The MME-SAT rejects the UE's Initial Attach Request with an Attach Reject message that includes a Cause value indicating that the Attach procedure is suspended, as well as a Timer value(indicating how long the UE should refrain from attempting another Attach).

NOTE: The Cause and the Timer can be protected with a digital signature, which the UE can validate using provisioned root certificates.

Editor’s Note: The impact of using a Certificate is FFS

4-5 Once MME-SAT establishes contact with MME-GND, it forwards the IMSI to request authentication vectors from the Home Subscriber Server (HSS).

6-10 In subsequent coverage, the UE re-initiates the Attach Request. This time, MME-SAT, equipped with the authentication vectors, proceeds to authenticate the UE, leading to a successful Attach Acceptance. Immediately following successful authentication, MME-SAT sends a provisional Update Location Request to the HSS. This update includes an indicator that the location update is provisional and should not be fully processed until a final confirmation is received, optimizing the handling of location data under intermittent connectivity.

11-12 Location Update Process: MME-SAT updates the UE's location with the HSS upon establishing ground connectivity, ensuring the UE's subscription permits service in the attempted location. Any discrepancies trigger a detach procedure during the next satellite contact.

.

6.9.3 Evaluation

The proposed solution effectively addresses the key security issues identified in Key Issue #1, particularly focusing on the challenges of intermittent connectivity inherent to satellite communications.

The solution introduces a split architecture for the MME, with segments aboard the satellite (MME-SAT) and on the ground (MME-GND). This design accommodates the intermittent connectivity of satellite coverage and facilitates secure communication between the UE and the network. By temporarily storing the UE's IMSI and issuing an Attach Reject message with a Cause value and a Timer, the solution ensures that the UE can only attempt re-attachment after a specified period.

Upon establishing contact with MME-GND, MME-SAT requests authentication vectors from the Home Subscriber Server (HSS), enabling the authentication of the UE in subsequent coverage. This process ensures that the communication between the UE and the network is authenticated and secure, addressing the confidentiality and integrity of the messages. The provisional Update Location Request sent to the HSS immediately after successful authentication includes an indicator that the location update is provisional. This approach optimizes the handling of location data under intermittent connectivity, ensuring that the integrity and confidentiality of control-plane messages are maintained.

Based on the choice of operator(Satellite) implementation, The solution's architecture inherently mitigates potential DoS attacks that could arise from the storage capacity being exhausted by spoofed data. By implementing a digital signature for the Attach Reject message, the network ensures that only UEs with valid credentials can re-attempt attachment, reducing the risk of spoofed data flooding the system. However, it does not address the DoS attack on the storage capacity due to the unprotected message in step 1.

Additionally, the provisional Update Location Request mechanism ensures that the network resources are optimally utilized, preventing unauthorized UEs from exhausting the storage resources on the satellite.

Editor’s Note: Further evaluation is FFS.

.

\*\*\*\*\*END CHANGE\*\*\*\*\*