**3GPP TSG-SA3 Meeting #119 S3-245213**

**Orlando, USA 11 – 15 November 2024** *revision of S3-244955*

**Source: Qualcomm Incorporated**

**Title: Proposed addition to the split MME conclusion for key issue #1**

**Document for: Approval**

**Agenda Item: 5.7**

1 Decision/action requested

***This contribution proposes an additional conclusion for key issue #1 for split MME.***

2 References

[1] S3-243827 draft TR 33.700-29

3 Rationale

The current conclusion for key issue #1 is not clear that the legacy security procedure will be used, e.g. AKA and NAS security mode command procedure. It is proposed to add that text.

4 Detailed proposal

It is proposed to approve the below for inclusion in [1].

**\*\*\*\* START OF CHANGES \*\*\*\***

7.1 Conclusions for Key Issue #1: Security protection in Store and Forward Satellite Operation

For the HSS on the satellite deployment, the following conclusions are made:

- The normal security procedures are used as security can be established using legacy security procedures (e.g. AKA, NAS security mode command, etc.) using the security credentials in the HSS onboard the satellite;

- As an option for the operator, IOPS-based keying which is captured in the informative Annex F in TS 33.401 [3] can be used to limit the impact of exposing the long-term key in the HSS in the satellite; and

NOTE 1: Any related enhancements of IOPS-based keying agreed during the normative phase are to be captured in the informative Annex F in TS 33.401 [3].

- The security of communications between the proxies on satellite and ground is out of 3GPP scope.

The following principles are agreed for supporting Store and Forward operation with a split MME architecture:

- Mutual authentication between the UE and the 3GPP network in S&F operations may require the involvement of more than one MME on-board a satellite, in which case the ground network is responsible for the selection and provisioning of MMEs on-board the same, or another satellite with the necessary information to perform or finish a mutual authentication procedure.

-

- It has to be ensured that the latest NAS security context of the UE is available at the MME on-board which processes the NAS security;

- The security of communications between the proxies on satellite and ground is out of 3GPP scope.

- The normal security procedures are used as security can be established using legacy security procedures (e.g. AKA, NAS security mode command, etc.) for both single and multiple satellite use cases.

NOTE 2: The above conclusion and below conclusion do not clash as the below relates to before security establishment.

- Enhancements to provide protection against DoS attacks before a security context is established are to be determined during normative work based on the solution(s) captured in this document.

Editor’s Note: Further conclusions are FFS.

**\*\*\*\* END OF CHANGES \*\*\*\***