**3GPP TSG-SA3 Meeting #102-e S3-210494-r1**

**e-meeting, 18th - 29th January 2021 Revision of S3-20xxxx**

**Source: Qualcomm Incorporated**

**Title: pCR: Security architecture conclusion for KI #1**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***Approve this contribution to conclude the security architecture for Key issue #1 in TR33.857***

# 2 References

[1] S3-203400 - TR 33.857 v0.3.0

# 3 Rationale

SA2 have started the normative work for eNPN and are awaiting SA3 feedback on security aspects related to key issue #1 (Credentials owned by an external entity). It will be useful for SA2 to progress their work if SA3 can conclude on at least the security architectural aspects of KI #1. SA3 study in [1] has already identified several security solutions (solutions #1 to #7) for KI #1 with many commonalities among them on the security architectural aspects.

For the KI #1 in [1], if the external entity is 5GS aware (e.g., either supports 5G AKA/EAP-AKA’ or supports another EAP method and is capable of deriving 5G key hierarchy (i.e., deriving KAUSF from EMSK)), the resulting SNPN architecture is same as the 5GS roaming architecture. Therefore, it is proposed to conclude that the existing 5GS roaming architecture is reused when the external entity is 5GS aware.

If the external entity is a legacy AAA (non-5GS aware), the SNPN can only receive the MSK resulting from successful EAP authentication. In this case, an entity in the SNPN should be able to construct the 5G key hierarchy and supply the key to AMF. It is proposed to conclude that an AUSF proxy function (AUSFp) is introduced in the SNPN which performs the necessary 5G key derivation from the MSK received from the legacy AAA server. Furthermore, depending on the trust relationship between the SNPN and the external entity, the AUSFp may either interface directly to the external entity or through another network function for security isolation purposes, which can be left to the SNPN decision.

# 4 Detailed proposal

SA3 is kindly requested to approve the below pCR to [1].

\*\*\* BEGINNING OF CHANGES \*\*\*

## 7.x Conclusions on KI #1: Credentials owned by an external entity

In case that the external entity is 5GS aware (i.e., has the AUSF/UDM and is capable of deriving 5G key hierarchy after a successful primary authentication), it is concluded that the existing 5GS roaming architecture is reused.

In case that the external entity is non-5GS aware (legacy AAA server), the following is concluded:

* The SNPN access with a credential owned by an external entity is performed via an AUSF in the SNPN that is enhanced to interface with the external entity.
* Depending on the trust relationship between the SNPN and the external entity, the enhanced AUSF may either interface directly to the external entity or through another network function for security isolation purposes, which is left to the SNPN decision.

Editor’s Note: Further conclusion(s) are FFS.

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