**3GPP TSG-SA3 Meeting #101e S3-202971**

**e-meeting, 9 – 20 November 2020 Revision of S3-20xxxx**

**Source: Huawei, HiSilicon**

**Title: Delete Editor’s Note in solution #9**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to add a solution in TR33.818***

# 2 References

[1]

# 3 Rationale

This contribution propose to delete an Editor’s NOTE:

 Editor’s Note: What protocol is used between UE and 5G DDNMF and how to secure the protocol are FFS.

The protocoal used in control plane architecture needs to be defined when the solution is adopted as basis for normative work, otherwise we don’t need to waste time on it.

The protocol used in user plane architecture is based on ua\* protocol that is used in AKMA.

# 4 Detailed proposal

pCR

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

## 6.9 Solution #9: Key management in discovery procedure

### 6.9.1 Solution overview

This solution addresses the key issue #2: Keys in ProSe discovery scenario.

This solution proposes to generate discovery root key from AUSF and the 5G DDNMF derives the discovery keys. At the UE side, UE generates both discovery root key and discovery keysl.

### 6.9.2 Solution details

In control plane architecture as illustrated in clause 4.1.1, a UE reaches the 5G DDNMF via AMF. The 5G DDNMF allocates the Prose APP code and gets the discovery root key from AUSF. The AUSF will generate the discovery root key based on the KAUSF. The 5G DDNMF will further generate discovery IK based on the discovery root key for open discovery and will further generate discovery IK and discovery CK for restricted discovery. The 5G DDNMF will send the key material to the UE via AMF. On UE side, the UE will generate the same keys as the network side based on the key material sent from the 5G DDNMF. The 5G DDNMF and AMF will relay on the security of SBI.

NOTE: the detail of SBI used between 5G DDNMF and AMF is not introduced in this solution.

In user plane architecture as illustrated in clause 4.1.2, a UE reaches the 5G DDNMF via user plane. The 5G DDNMF allocates the Prose APP code and gets the discovery root key from AAnF. The AAnF will generate the discovery root key based on the KAKMA as described in TS 33.535[7]. The 5G DDNMF will further generate discovery IK based on the discovery root key for open discovery and will further generate discovery IK and discovery CK for restricted discovery. The 5G DDNMF will send the key material to the UE via Ua\* protocol. On UE side, the UE will generate the same keys as the network side based on the key material sent from the 5G DDNMF

Editor’s Note: The details of key derivation for both CP and UP solutions are FFS.

### 6.9.3 Solution evaluation

This solution does not specifiy the protocol used between UE and 5G DDNMF.

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