**3GPP TSG-SA3 Meeting #100bis-e *draft\_S3-202469-r1***

**e-meeting, 12 -16 October 2020** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: New solution on Key management in discovery procedure**

**Document for: Approval**

**Agenda Item: 2.9**

# 1 Decision/action requested

***Approve this contribution to add a solution to KI #2 in TR33.847***

# 2 References

NA

# 3 Rationale

The contribution proposes a solution to key issue #2: Keys in ProSe discovery scenario.

# 4 Detailed proposal

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | | | | | |
| Solutions | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 |  |  |  |  |  |  |  |  | X |  |
| 2 |  |  |  |  |  |  |  |  |  | X |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
| X |  | X |  |  |  |  |  |  |  |  |

\*\*\* END OF 1st CHANGES \*\*\*

\*\*\* BEGINNING OF 2nd CHANGES \*\*\*

## 6.X Solution #X: Key management in discovery procedure

### 6.X.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.X.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.

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 user plane. 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.

Editor’s Note: The protocol is used between UE and DDNMF and how to secure the protocol is FFS.

### 6.X.3 Solution evaluation

TBD

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