**3GPP TSG-SA3 Meeting #104 *S3-212465-r1***

**meeting, 16 - 27 Aug 2021**

**Source: MITRE**

**Title: Update to KI #17**

**Document for: Approval**

**Agenda Item: 5.9**

1 Decision/action requested

***It is requested to approve the proposed updates to Key Issue#2***

2 Rationale

The key issue #17 only addresses policy provisioning. To enable out of coverage ProSe discovery, parameters must also be securely provisioned to the UE. TR 23.752 has a key issue where both policy and parameters are provisioned together: namely, KI#8 “Support of PC5 Service Authorization and Policy/Parameter Provisioning”. This approach where both policy and parameters are provisioned together is preserved in the normative stage (TS 23.304).

3 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.847.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Begin 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

5.2 Key Issue #2: Keys in ProSe discovery scenario

5.2.1 Key issue details

In TS 33.303[6], the Prose Function sends a discovery key to announce UE for calculating MIC in open discovery. In Restricted discovery, Prose Function also may send DUCK, DUIK, and DUSK to UEs.

In 5G, the functions of the Prose Function are split into different network functions along with different network architecture approaches. Meanwhile, AKMA has been defined in TS 33.535[7], and GBA is under study to adapt to 5G system. The elements above have to be considered to calculate and share discovery key(s) to UEs in 5G Prose.

Following issues need to be addressed in this key issue:

- Which network function derives the discovery key.

- How to send the keys to the UEs.

- Provisioning of keys to support discovery when the UE is out of coverage.

5.2.2 Security threats

Not applicable

5.2.3 Potential security requirements

Not applicable

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*