**3GPP TSG-SA3 Meeting #104e-Ad-hoc** ***draft\_S3-213325-r5***

**meeting, 27 - 30 Sep 2021**

**Source: MITRE**

**Title:** **Updates to conclusions for key issue #2**

**Document for: Approval**

**Agenda Item: 5.2**

1 Decision/action requested

***It is requested to approve the proposed updates to conclusions for key issue #2***

2 Rationale

For key provisioning in public safety discovery scenario, it is proposed to use solution #37 as the basis for normative work.

3 Detailed proposal

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

7.2 Key Issue #2: Keys in ProSe discovery scenario

The conclusions for ProSe direct discovery as follows:

The discovery keys include a cipher key, an integrity key and a scrambling key.

For open discovery, the integrity key will be used to provide integrity protection of the announce message.

For restricted discovery, the cipher key and/or integrity key and/or scrambling key will be used to protect discovery messages based on the requirement of the ProSe Service.

Multiple sets of discovery keys can be provisioned at the UE.

Editor’s Note: Further conclusions on how the discovery keys are generated and provisioned is FFS

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*