**3GPP TSG-SA3 Meeting #101-e *draft\_S3-202957-r3***

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

**Source: Huawei, HiSilicon**

**Title: Propose to resolve EN in the security requirement of KI#12**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to resolve EN in the security requirement of KI#12 in TR 33.847***

# 2 References

N/A

# 3 Rationale

The contribution proposes to resolve EN in the security requirement of key issue#12, this involves a new threat and a new security requirement. The contribution also captures a minor editorial change.

# 4 Detailed proposal

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

## 5.12 Key Issue #12: Security of one-to-one communication over PC5

### 5.12.1 Key issue details

One-to-one ProSe communication is realised by establishing a secure link over PC5 between initiating UE and peer UE, it is used by two UEs that want to directly exchange traffic or when a remote UE attaches to ProSe relay.

Editor’s Note: the one-to-one communication policy/parameter provisioning procedure shall inline with SA2.

Editor’s Note: it’s FFS whether this KI covers the out-of-coverage scenario.

The LTE ProSe one-to-one communication may happen after discovery procedures, or after one-to-many ProSe communications. The detailed one-to-one (i.e. unicast) communication and the corresponding security aspects are defined for LTE ProSe in 3GPP TS 23.303 [5] and TS 33.303 [6], respectively. 2The architecture study in the TR 23.752 [2] proposes to introduce new features to 5G ProSe from 5G V2X, this may protentially reuse the security meshanisms from 5G V2X as defined in TS 33.536 [8]. Although the 5G V2X and the ProSe one-to-one communications both rely on the PC5 reference point, the ProSe may not be able to fully reuse the security mechanisms from 5G V2X scenario which is due to the fact that they may use different processing procedures. For this reason, it’s necessary to study the security of one-to-one communication which is dedicated for 5G ProSe scenario. 5G ProSe needs a reliable mechanism to establish and to use one-to-one communication over PC5.

### 5.12.2 Security threats

If the two UE cannot be mutually authenticated during one-to-one communication, a peer may connect to an attacker.

The signalling and user plane message exchanges during one-to-one communication may be seen in cleartext, modified or replayed by an attacker if lack of confidentiality protection and integrity protection.

If one-to-one communication (unicast) mechanism in 5G V2X is reused, an attacker may deploy bidding-down attack to force establishing unprotected connection between initiating UE and peer UE.

Failure to secure protect the security context refreshing may introduce potential vulnerability.

### 5.12.3 Potential security requirements

The initiating UE shall establish a different security context for each peer UE during the PC5 one-to-one communication establishment if the security is activated.

The mutual authentication between two UEs during one-to-one communication shall be supported.

The one-to-one communication link security establishment shall be protected from MitM attacks.

The PC5 one-to-one communication signalling shall support confidentiality protection, integrity protection and anti-replay protection.

The PC5 one-to-one communication user plane shall support confidentiality protection, integrity protection and anti-replay protection.

The system shall support means of providing the signalling and user plane security policies to UEs for a particular PC5 one-to-one communication.

The initiating UE and peer UE shall provide a means to mitigate establishing unprotected connection caused by bidding-down attack.

The system shall support means for a secure refresh of the UE security context.

NOTE: The security context refresh may be triggered based on various options (e.g. validity time etc.)

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