**3GPP TSG-SA3 Meeting #101-e *draft\_S3-202956-r2***

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

**Source: Huawei, HiSilicon**

**Title: Update to Sol#7 to address EN and add evaluation**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***Approve this contribution to address EN and add evaluation to solution#7 in TR 33.847***

# 2 References

N/A

# 3 Rationale

The contribution proposes to address EN and add evaluation to solution#7: Security establishment of one-to-one PC5 communication.

# 4 Detailed proposal

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

## 6.7 Solution #7: Security establishment of one-to-one PC5 communication

### 6.7.1 Solution overview

This solution addresses the Key Issue #12: Security of one-to-one communication over PC5.

The initiating UE initiates the one-to-one communication establishment procedures to the receiving UE and the security-related information (e.g. security protection methods, security algorithms, keys if applicable, etc) are confirmed or created during the one-to-one communication establishment procedures.

The one-to-one communication establishment starts with a Direct Communication Request (DCR) message to send the initiating UE’s security capabilities and to trigger the mutual authentication. In order to perform the Direct Communication Request, the ProSe one-to-one communication may happen after discovery procedures, or after one-to-many ProSe communications. After DCR and mutual authentication, the Direct Security Mode Command and the Direct Security Mode Complete messages are emitted to inform the selected security protection algorithms for the connection and the initiating UE’s user plane security policies (i.e. user plane confidentiality and integrity protection policies), respectively. Finally, the receiving UE replies a Direct Communication Accept (DCA) message to confirm the user plane protection methods and finish the one-to-one communication establishment procedures.

### 6.7.2 Solution details

Initiating UE

Receiving UE

2. Direct Communication Request ( Initiating UE's security capabilities )

3. Direct Auth and Key Establishment

4. Direct Security Mode Command( Chosen\_algs, Initiating UE's security capabilities )

5. Direct Security Mode Complete (Initiating UE's user plane security policies)

1. Discovery Procedures, or One-to-Many Communication

6. Direct Communication Accept ( User plane security indication )

0. ProSe Parameter pre-configuration and previsioning

Figure 6.7.2-1 Procedures for one-to-one communication security establishment over PC5

0. ProSe security-related parameter (for one-to-one secure communication over PC5) pre-configuration and previsioning, the signalling integrity protection shall be used and the signalling ciphering protection is a configuration option.

1. Discovery procedures or after one-to-many ProSe communications for getting initial parameters (e.g. L2 IDs).

2. The initiating UE starts Direct Communication Request (DCR) message contains and the initiating UE’s security capabilities. The initiating UE’s security capabilities are the confidentiality and integrity protection algorithms that the initiating UE accepts for this connection.

3. The receiving UE may initiate the Direct authentication and key establishment procedures with the initiating UE.

4. The receiving UE uses the Chosen\_algs to indicate the selected confidentiality and integrity protection algorithms of this link and contains the Chosen\_algs in the Direct Security Mode Command message. The initiating UE’s security capabilities are sent back to the initiating UE to mitigate the bidding down attack. The receiving UE shall integrity protect the Direct Security Mode Command message before sending it to the initiating UE.

5. The initiating UE sends its user plane security policies to the receiving UE by using Direct Security Mode Complete message.

6. The receiving replies the Direct Communication Accept message to accept the DCR message and one-to-one communication establishment including the user plane security indication. The user plane security protection methods (the user plane confidentiality protection activated or not, and the user plane integrity protection activated or not) are explicitly indicated by using user plane security indication.

NOTE: The privacy protection of entities is not addressed in this solution.

### 6.7.3 Solution evaluation

The Solution #7 addresses the security requirements of key issue #12. The mutual authentication between two UEs during one-to-one communication is supported in step 3. MitM attacks during link establishment and bidding-down attacks are mitigated by mandatory activation of the signalling integrity protection. The system supports providing the signalling and user plane security policies to UEs for a particular PC5 one-to-one communication in step 0. According to the step 0 and 5, PC5 signalling and user plane confidentiality protection, integrity protection and anti-replay protection are assumed to be supported by the system as they can be negotiated or pre-configured to be activated.The privacy protection is not addressed in this solution.

Editor’s Note: Futher evaluation is FFS.

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