**3GPP TSG-SA3 Meeting #108Adhoc-e *draft\_S3-222479-r1***

**e-meeting, 10th - 14th October 2022**

**Source: Huawei, HiSilicon**

**Title: Update to Solution#1**

**Document for: Approval**

**Agenda Item: 5.17**

# 1 Decision/action requested

***Approve the updated solution proposal to TR 33.891***

# 2 References

N/A

# 3 Rationale

The contribution proposes to update the solution #1. This aims to further add descriptions about the security policies used during PC5 communications for direct C2 or unicast DAA scenarios. The security policy mechanism reuses the existing mechanism in eV2X and 5G ProSe.

# 4 Detailed proposal

\*\*\*BEGINNING OF THE 1st CHANGE\*\*\*

## 6.1 Solution #1: Security establishment and link security protection of unicast PC5 communication

### 6.1.1 Introduction

This solution addresses the direct PC5 communication (unicast) for both the direct C2 and unicast DAA scenarios as specified in Key Issue #1 and Key Issue #2, respectively. Generally, unicast security establishment specified in eV2X TS 33.536 [6] and 5G ProSe TS 33.503 [7] is reused as the baseline.

### 6.1.2 Solution details

The unicast PCF communication establishment starts with a Direct Communication Request (DCR) message to send the initiating UE’s security capabilities and to trigger the mutual authentication and key establishment. After mutual authentication and key establishment, 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 unicast PC5 communication establishment procedures.

The signalling and user plane security protection are protected based on the detailed negotiation procedures:

0. UAS security-related parameter (for unicast secure communication over PC5) pre-configuration and previsioning, the signalling messages are integrity protected and the signalling ciphering protection is a configuration option.

NOTE 1: Step 0 is done only in coverage.

1. UAS discovery procedures may happen for the UAV and UAVC to find each other in direct C2 scenario.

NOTE 2: whether or not the UAV needs to discover the UAVC or vice versa will align with the decision in SA2.

2. The initiating UE (UAV or UAVC) starts DCR message contains its security capabilities and signalling security policy. The security capabilities are the confidentiality and integrity protection algorithms that the initiating UE accepts for this connection. The security capabilities are reused as specified in 33.536 [6] and 33.503 [7]. The direct C2 or unicast DAA service use the ‘REQUIRED’ signalling security protection policies if the service needs security protection.

3. To generate the PC5 root key to protect the PC5 connection, 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 integrity protects the Direct Security Mode Command message before sending it to the initiating UE.

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

6. The receiving replies the DCA message to accept the DCR message and the unicast PC5 communication establishment including the user plane security indication. The user plane security protection methods (the user plane with or without confidentiality and/or integrity protection) are explicitly indicated by using the user plane security indication.

### 6.1.3 Evaluation

FFS

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