**3GPP TSG-SA3 Meeting #108Adhoc-e *draft\_S3-222477-r1***

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

**Source: Huawei, HiSilicon**

**Title: New solution for protecting direct communication**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***Approve the new solution proposal to TR 33.893***

# 2 References

[1]

# 3 Rationale

The contribution proposes to add a new solution to provide secure direct communications to address KI#4. The 5G V2X/5G ProSe based unicast mechanism will be reused as much as possible in Ranging, these mechanisms allow UEs to establish unprotected unicast link which leads potential bidding down attack:

Based on the unicast mechanism in TS 33.536 [8], a man-in-the-middle attacker can modify the signalling integrity policy of ‘PREFERRED’ to ‘NOT NEEDED’ when an initiate UE sends a Direct Communication Request with a ‘PREFERRED’ signalling integrity policy to a receiving UE. This will cause the receiving UE with ‘PREFERRED’ signalling integrity policy to determine no signalling integrity protection (further leads no security on the entire link) even if the receiving UE has the ability to activate the signalling protection. The attacker can further change the signalling integrity protection from ‘NOT NEEDED’ back to ‘PREFERRED’ in the Direct Security Mode Command message, because there is no integrity protection on the Direct Security Mode Command message.

The bidding down attack on UE capability was fixed by SA3 by introducing a HASH scheme in clause 7.2.4.4 of 33.401 [2]. Similar method can be introduced into the ProSe PC5 one-to-one communication scenario to prevent bidding down attack as UEs can establish shared key by initiating Direct Auth And Key Establishment procedures.

# 4 Detailed proposal

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

## 6.X Solution #X: New solution for protecting direct communication

### 6.X.1 Introduction

This solution addresses the security PC5 direct communication (unicast) for Ranging/SL Positioning service as specified in Key Issue #4. This solution uses the direct communication security defined for 5G ProSe in TS 33.503 [6] and/or for 5G V2X in TS 33.536 [5] as a baseline and adjusts to the Ranging/SL Positioning scenario.

Security flexibility is provided by introducing on-demand PC5 unicast security policies in 5G V2X/5G ProSe. However a man-in-the-middle attacker can modify the signalling integrity policy of ‘PREFERRED’ to ‘NOT NEEDED’ when an initiate UE sends a Direct Communication Request with a ‘PREFERRED’ signalling integrity policy to a receiving UE. This will cause the receiving UE with ‘PREFERRED’ signalling integrity policy to determine no signalling integrity protection even if the receiving UE has the ability to activate the signalling protection, this further leads no mutual authentication and no security on the entire link. The attacker can further change the signalling integrity protection from ‘NOT NEEDED’ back to ‘PREFERRED’ in the Direct Security Mode Command message, because there is no integrity protection on the Direct Security Mode Command message.

The above attack is considered as a bidding down attack which does not fit the following security requirement in the Key Issue #4 (i.e. The 5G system shall support a means for the Ranging-capable UEs to mutually authenticate each other during PC5 direct communication of Ranging/SL Positioning service). Moreover, the information exchanged during PC5 direct communication for Ranging/SL Positioning service is mainly security/privacy sensitive information (e.g. Location information). Thus the bidding down attack also violates the information security and/or privacy if an attacker forces to not activate the security protection. This solution proposes a mechanism to prevent the above bidding down attack.

Editor’s Note: The solution assumes the use of security policies of V2X and ProSe direct communication. The security polices for Ranging/SL positioning services are FFS

### 6.X.2 Solution details

The clause describes how security is established during Ranging/SL Positioning direct communication set-up.

0. Ranging/SL Positioning enabled UEs are provisioned with security-related parameter (for Ranging/SL Positioning direct communication over PC5), including the signalling integrity/confidentiality protection policies and the user plane signalling integrity/confidentiality protection policies.

NOTE: Step 0 is done only in coverage.

1. Discovery procedures between two Ranging/SL Positioning enabled UEs.

2. The initiating UE starts one-to-one communication establishment by sending Direct Communication Request (DCR) message. The DCR message contains the initiating UE’s security capabilities and signalling security policies (signalling integrity protection and confidentiality protection policies). 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.

In the case of the receiving UE decides not to activate signalling security protection based on the signalling security policies from the initiating UE and itself, the receiving UE initiates this procedure to generate KNRP to protect UE\_1’s security capabilities and signalling policy from bidding down attack.

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 and signalling security policies 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 if the receiving UE decides to activate signalling integrity protection.

If the KNRP is generated in step 3 for the purpose of bidding down attack preserving, the receiving UE calculates HASHrec using KNRP as described in 6.X.2.1 and sends the HASHrec to the initiating UE in the Direct Security Mode Command message in order to integrity protect the initiating UE’s security capabilities and signalling security policies, the initiating UE calculates HASHini using KNRP as described in 6.X.2.1 and compare with HASHrec to check the integrity of initiating UE’s security capabilities and signalling security policies. The initiating UE only continues the rest procedure if the integrity check of initiating UE’s security capabilities and signalling security policie passes.

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

6. The receiving UE replies Direct Communication Accept (DCA) 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: Mandatory setting the signalling integrity policy to ‘REQUIRED’ can prevent the bidding-down attack.

#### 6.X.2.1 HASHrec and HASHini

The receiving UE and the initiating UE derive HASHrec and HASHini respectively using the following parameters as input to the KDF given in TS 33.220 [12].

- S = Unprotected security capabilities and signalling security policy of the initiating UE,

- Key = 256-bit KNRP

HASHrec and HASHini are the 64 least significant bits of the 256 bits of the KDF output.

### 6.X.3 Evaluation

TBD.

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