**3GPP TSG-SA3 Meeting #109e-AdHoc *draft\_S3-230300-r1***

**e-meeting, 16 - 20 January 2023**

**Source: Qualcomm Incorporated**

**Title: Updates to the Key Issue #4**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***This contribution proposes to update the Key Issue #4 in TR 33.893.***

# 2 References

[1] TR 33.893 v0.4.0

# 3 Rationale

This contribution proposes to update the Key Issue #4 as follows:

First, this contribution proposes to clarify that the first security threat and the first security requirement are for one-to-one communication.

Second, this contribution proposes to correct the parts of first and second security threats to precisely describe the security threats.

Lastly, this contribution proposes to add replay protection in the second security requirement.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [1].

**\*\*\*\*\* START OF CHANGES \*\*\*\*\***

## 5.4 Key issue #4: Protection of unicast direct communication

### 5.4.1 Key issue details

As per TR 23.700-86 [2], for direct communication between the UEs, the architecture and solutions defined for 5G V2X and 5G ProSe will be reused as much as possible. This provides the basis for reusing the direct communication security defined for 5G ProSe in TS 33.503 [6] or for 5G V2X in TS 33.536 [5] to protect the direct communication for Ranging/SL Positioning services.

Although the security mechanisms for direct communication of 5G ProSe or 5G V2X services can be reused for Ranging/SL Positioning services, there are still some scenarios in Ranging/SL Positioning services that are not discussed and studied for 5G ProSe or 5G V2X services. Considering the Ranging/SL Positioning services may have different processing procedures, it’s necessary to study the security of direct communication which is dedicated to the Ranging/SL Positioning services scenario.

In addition, for Ranging/Sidelink Positioning services, the information exchanged during SR5 direct communication between the UEs is location related, which is security/privacy sensitive. This is also an aspect different from 5G ProSe or 5G V2X services which do not always carry security/privacy sensitive information over PC5.

Moreover, as per TR 23.700-86 [2], SR5 is defined in the reference architecture to carry control signalling of Ranging/Sidelink Positioning service. Given that all Ranging/SL positioning capable UEs are also ProSe/V2X capable, the security protection of SR5 direct communication can rely on the existing security protection of PC5 direct communication as specified in TS 33.503 [6] and TS 33.536 [5]. There are options discussed in TR 23.700-86 [2] to use PC5-S or PC5-U to carry SR5 control messages. Then how to protect SR5 control messages also needs to be analysed.

### 5.4.2 Security threats

During direct communication establishment for one-to-one communication, if the UE cannot authenticate the peer UE to be the entity it intends to communicate with, it may lead to the impersonation of the peer UE by an attacker.

Failure to protect the integrity of Ranging/SL Positioning service information during direct communication will open vulnerability for attacks such as fabrication, modification, or removal of the signalling data such as positioning capability, positioning assistance data and location information.

Failure to protect the confidentiality of Ranging/SL Positioning service information during direct communication will open vulnerability for eavesdropping attacks resulting in privacy violations.

In case one UE is communicating with multiple peer UEs for Ranging/SL Positioning service, if there is no security isolation between the PC5 direct links with multiple peer UEs, one compromised peer UE or compromised PC5 link could lead to the compromise of all PC5 links with other peer UEs.

### 5.4.3 Potential security requirements

The 5G system shall support a means for the Ranging-capable UEs to mutually authenticate each other during SR5 one-to-one direct communication of Ranging/SL Positioning service.

The 5G system shall provide a means to support integrity and replay protection of the information transferred during SR5 direct communication for the Ranging/SL Positioning service.

The 5G system shall provide a means to support confidentiality protection of the information transferred during SR5 direct communication for the Ranging/SL Positioning service.

The 5G system shall support a means for the Ranging-capable UE to establish cryptographic separation for each PC5 interface and for each peer UE during the SR5 direct communication establishment of Ranging/SL Positioning service.

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