**3GPP TSG-SA3 Meeting #108-e draft\_S3-222070-r1**

**e-meeting, 22nd – 26th August, 2022**

**Source:**  **Huawei, HiSilicon**

**Title:** **Addressing the editor's note in key issue#1**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***It is proposed to approve the change described in this document.***

# 2 References

[1] 3GPP TR 33.893: "Study on Security Aspects of Ranging Based Services and Sidelink Positioning".

# 3 Rationale

The transmission of the Ranging/Sidelink positioning signals and discovery are discussed as separate key issues. As decripted in TR 23.700-86, the transmission of the Ranging/Sidelink positioning signals is performed after discovery.

“*To enable a Reference observer UE and a target UE to be able to perform measurement and communicate for delivering measurement data, the UEs have to be discovered by each other first*.”

The editor’s note should be revised accordingly.

# 4 Detailed proposal

\*\*\* 1st CHANGE \*\*\*

## 5.1 Key issue #1: Privacy protection for Ranging/SL Positioning services

### 5.1.1 Key issue details

As the information of almost all Ranging/Sidelink Positioning services is related to location, all the UEs participating in Ranging/Sidelink Positioning, including the reference UE, target UE, assistant UE, etc., may need to disclose its location information to others. If such privacy sensitive information is not well protected, the UE’s privacy could be compromised. Among the requirements defined for Ranging services in clause 6.37.2 of TS 22.261 [7], there are following requirements concerning privacy protection for Ranging services:

*The 5G system shall be able to protect privacy of a UE and its user, ensuring that no identifiable information can be tracked by undesired entities during ranging.*

*The 5G system shall be able to ensure that user privacy is not violated during ranging, e.g., subject to regional or national regulatory requirements.*

Privacy protection is also raised in clause 4.1 of TR 23.700-86 [2] as one of the architecture assumptions for Ranging/SL Positioning services and is tasked for SA3 to study. In multiple solutions (e.g. solutions #6, #9, #13, #18, #21, #23, #24, #25) of TR 23.700-86 [2], privacy is considered as an issue to be addressed, either during discovery, or during Ranging/SL positioning procedure, or for service exposure.

### 5.1.2 Security threats

When UE’s identifiable information is disclosed to undesired/malicious UEs during discovery or during communication for Ranging/SL positioning, the UE’s behaviour will become trackable to others. Hence the UE’s privacy could be violated.

When the UE’s Ranging/SL positioning information (e.g. distance measurement, direction measurement, or both, or assistant data) and/or the associated UE’s identity are disclosed to undesired/malicious UEs or undesired network functions during communication for Ranging/SL positioning, the UE’s whereabouts and/or movements will become traceable to others. Hence the UE’s privacy could be violated.

### 5.1.3 Potential security requirements

The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during discovery for Ranging/SL positioning.

The 5G Ranging/SL Positioning system shall provide means to mitigate trackability and linkability attacks of the UE during communication for Ranging/SL positioning.

\*\*\* END OF 1st CHANGE\*\*\*