**3GPP TSG-SA3 Meeting #108Adhoc-e *draft\_S3-222478-r1***

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

**Source: Huawei, HiSilicon**

**Title: New solution of security for the Ranging/SL positioning device discovery**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

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

# 2 References

N/A

# 3 Rationale

The contribution proposes to add a new solution to provide secure Ranging/SL positioning service discovery.

# 4 Detailed proposal

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

## 6.X Solution #X: Security of the Ranging/SL positioning device discovery

### 6.X.1 Introduction

This solution addresses the security of the discovery procedures for Ranging/SL Positioning service as specified in Key Issue #3. As per the assumption under clause 4.1, the solution of discovery security reuses the direct discovery security defined for 5G ProSe in TS 33.503 [6] as a baseline and adjusts to the Ranging/SL Positioning scenario.

### 6.X.2 Solution details

The discovery procedure for the Ranging/SL positioning service is classified as restricted discovery, considering the discovery procedures happen between UEs with dedicated Ranging/SL positioning service authorisation (i.e. discover with explicit permission).

The information exchanged during PC5 direct discovery for Ranging/SL Positioning service may include security/privacy sensitive information (i.e. ranging role informtion of Ranging/SL Positioning UE). Thus integrity and confidentiality protections are required by the Ranging/SL positioning discovery. Based on the clause 6.1.3.2.2 in TS 33.503 [6], the solution proposes the following modifications for the Ranging/SL positioning discovery:

* the Code-Sending Security Parameters received from 5G DDNMF always include a DUCK and corresponding Encrypted\_bits\_mask for confidentiality protection, and a DUIK for integrity protection.
* the Code-Receiving Security Parameters received from 5G DDNMF always include a DUCK and corresponding Encrypted\_bits\_mask for confidentiality protection, the the Code-Receiving Security Parameters either include the DUIK, or indicates to use Match Report for MIC checking.

NOTE: whether or not to reuse 5G DDNMF in 5G ProSe to support the Ranging/SL positioning service discovery will be decided by SA2.

### 6.X.3 Evaluation

TBD.

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