**3GPP TSG-SA3 Meeting #110 Adhoc-e Draft\_S3-232004-r3**

**Electronic Meeting, 17th – 21th** **April, 2023**

**Source: OPPO**

**Title:** **New solution on security of Ranging/SL positioning groupcast communication**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***This pCR proposes a new solution on*** ***security of Ranging/SL positioning groupcast communication.***

# 2 References

[1] 3GPP TS 33.303.

[2] 3GPP TS 33.503.

# 3 Rationale

It is proposed a new solution on security of Ranging/SL positioning groupcast communication and try to reuse the existing security mechanism for one-to-many ProSe direct communication as much as possible with some modifications.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\* Begin 1st change\*\*\*\*\*\*\*\*\*

6.Y Solution #Y: Security of ranging/SL positioning groupcast communication

6.Y.1 Introduction

This solution addresses the security requirement of KI #1 and protects the ranging/SL positioning groupcast communication. This solution reuses the existing security mechanism of one-to-many ProSe direct communication defined in clause 6.2 of TS 33.303[1] along with some modification to set up the security of ranging/SL positioning groupcast communication.

6.Y.2 Solution details

This solution reuses the existing security mechanism of one-to-many ProSe direct communication defined in clause 6.2 of TS 33.303[1] along with some modification to set up the security of ranging/SL positioning groupcast communication.

The security for ranging/SL positioning establishment follows the procedure below:

* Configuration: The UE participating in the groupcast communication and the PKMF should be pre-configured with the group information for the ranging/SL positioning service, e.g., the Group Identity information including the Group Identity and Group member identity.
* The member UE and the PKMF should establish a security connection to transmit the key request message and key response message as specified in clause 5.2.5 of TS 33.503[2]. The UE uses these messages to request keys for particular groups, while the PKMF uses these messages to provide the UE with its Group member identity and the security algorithms to use with the various groups. The Key Response message is used to transport the group security material from the PKMF to the UE, which contains PGK, identifier of the PGK, and the expiry time.

For roaming scenario, the PKMF in the HPLMN and VPLMN of the UE exchange the Key Request message and Key Response message to provision the member UE with the group security material.

* The sending UE should generate a PTK to further generate the PEK and PIK to protect the groupcast traffic between sending UE and receiving UE, the protection of traffic between UEs is specified in clause 6.2.3.6 of 33.303[1].

The Group Identity and Group member identity are carried in the encrypted payload of PDCP packet, thus preventing the attacker to impersonate any UE in a specific group.

Editor’s Note: How to serve these UEs subscribed with different operators is FFS.

Editor’s Note: Whether PDCP for LTE ProSe one-to-many communication can be used for 5G-capable/V2X-capable UEs is FFS.

6.Y.3 Evaluation

TBA.

\*\*\*\*\*\*\*\*\* End 1st change\*\*\*\*\*\*\*\*\*