**3GPP TSG-SA3 Meeting #110Adhoc-e *S3-231895-r5***

**e-meeting, April 17-21, 2023**

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

**Title:** **update to solution 15**

**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] TR 23.700-86

# 3 Rationale

Considering the Group member ID generated by the UE may cause collision, this approach is not recommended. Protection of messages between UEs is not complete. It’s proposed to update this part.

# 4 Detailed proposal

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

## 6.15 Solution #15: Protection of information over group communication for Ranging/SL Positioning service

### 6.15.1 Introduction

This solution addresses the Key Issue #1 (second requirement) and #5.

This solution provides a security mechanism in SLPP layer to protect the information exchanged between UEs using group communication. The mechanism proposes to provision security materials to the UEs which belongs to a particular group for a SL positioning service. By using the provisioned security materials, a UE in the group can send confidentiality and integrity protected messages that include information related to the SL positioning service, and other UEs in the same group can undo the protection of the received messages. Note that this solution supports both in-coverage and out-of-coverage UEs by provisioning multiple sets of security materials associated with different expiry times.

### 6.15.2 Solution details

#### 6.15.2.1 Security flows



Figure 6.15.2.1-1: Security flows for Sidelink Positioning group communication

0a and 0b. The UE is pre-configured with the Group ID of a SL Positioning service.

Editor’s Note: Whether and how the Group ID of a SL Positioning service is pre-configured on the UE is FFS.

Steps 1 – 3 refer to a sending UE.

1a. The UE establishes a secure connection with the Sidelink Positioning Key Management Function (SLPKMF) based on the security procedures specified in clause 5.2.5 of TS 33.503 [6]. The UE sends a Key Request message to Sidelink Positioning Key Management Function (SLPKMF) including the Group ID of the Ranging and SL positioning service.

1b. The SLPKMF replies with the Key Response message containing the Sidelink Positioning Group Key (SLPGK), the key ID (SLPGK ID), the validity time, and the chosen ciphering and integrity algorithms. In addition, the Key Response message can include multiple SLPGK and SLPGK ID pairs with different validity times. Group member ID can be either assigned by the SLPKMF or generated at the UE. In the former case, the Group member ID is included in the Key Response message. In the latter case, the UE generates a Group member ID randomly so that it is uniquely identified in a group.

NOTE: The length of a Group member ID will be determined during the normative work. When the Group member ID is randomly generated by the UE, its length should be long enough to avoid collision.

2. Upon receiving the Key Request message, the UE derives the Sidelink Positioning Traffic Key (SLPTK) from SLPGK using Group ID, Group member ID, and SLPTK ID. SLPTK ID is a counter set to a unique value in the sending UE that has not been previously used together with the same SLPGK and the associated SLPGK ID. The UE further calculates the Sidelink Positioning Encryption Key (SLPEK) and Sidelink Positioning Integrity Key (SLPIK) from SLPTK using the chosen algorithm IDs, respectively.

3. The UE protects the messages as described in clause 6.15.2.2.1, and sends the messages to the group.

Steps 4 – 5 refer to receiving UEs.

4. The UE performs a Key Request procedure to get security materials from the SLPKMF. This step is same as the step 1.

5. Upon receiving the message from sending UE in the group, the UE calculates SLPTK, SLPEK and SLPIK. The derivation of security keys is same as the step 3 except that the UE takes Group ID, SLPGK ID, SLPTK ID and Group member ID (if it is included) in the received message as input parameters for key derivation. Then, the UE unprotects the message and verifies the integrity of the message as described in clause 6.15.2.2.2.

Editor’s Note: It is FFS how the receiving UE gets security materials when the sending UE and receiving UE are subscribed in different PLMNs.

Editor’s Note: Whether group member ID is self-selected is FFS.

Editor’s Note: Whether the group ID and group member ID are carried SLPP message is FFS.

#### 6.15.2.2 Protection of messages between UEs

##### 6.15.2.2.1 Message processing in the sending UE

The UE sending a message to the group does the following steps:

1. Form message header that contains Group ID, Group member ID, SLPGK ID, SLPTK ID, and Counter. Then, append the Payload to it as illustrated in figure 6.15.2.2.1-1.

2. If the network configuration is to use integrity protection, calculate MAC of the message header and the Payload based on the chosen integrity algorithm. The integrity algorithms specified in Annex D in TS 33.501 [16] are used to calculate MAC. If the network configuration is not to use integrity protection, then the sending UE shall set the MAC to all zeroes or randoms in the message header.

NOTE: setting the MAC to all zeroes is less preferred.

3. If the network configuration is to use confidentiality protection, add confidentiality to the Payload and MAC based on the chosen ciphering algorithm. The ciphering algorithms specified in Annex D in TS 33.501 [8] are used for the confidentiality protection. NOTE: the details of input parameters to the integrity algorithms and ciphering algorithms will be specified in normative work.



Figure 6.15.2.2.1-1: SLPP message format for Sidelink Positioning group communication

Editor’s Note: As the message header containing group ID, group member ID, etc. is not encrypted, it is FFS how to prevent one UE from impersonating another UE in the same group.

##### 6.15.2.2.2 Protected message processing in the receiving UE

The UE receiving a message does the following steps:

1. If the network configuration is to use confidentiality protection, undo confidentiality protection based on the chosen ciphering algorithm.

2. If the network configuration is to use integrity protection, verify the integrity of the received message by checking MAC based on the chosen integrity algorithm.

### 6.15.3 Evaluation

TBA

Editor’s Note: Whether this solution is only applicable to groupcast is FFS.

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