**3GPP TSG-SA3 Meeting #110Ad-Hoc-e *draft\_S3-231807-r2***

**Electronic meeting, Online, 17 - 21 April 2023**

**Source: Qualcomm Incorporated**

**Title: Updates on the solution #15**

**Document for: Approval**

**Agenda Item: 5.19**

# 1 Decision/action requested

***This contribution proposes to update the solution #15 in TR 33.893.***

# 2 References

[1] TS 23.586

[2] TS 33.303

[3] TR 33.893

# 3 Rationale

This contribution proposes to update the solution #15.

In particular, this contribution proposes several updates to address the Editor’s Notes.

First, Group refers to the Ranging/SL positioning service. Accordingly, Group ID refers to the Ranging/SL positioning service identifier. In this regard, it is proposed to update step 0a and 0b that the UE is provided with the Ranging/SL positioning application identifier (which is defined in TS 23.586 [1]) during the parameters/policy provisioning procedure. Therefore, we remove the following Editor’s Note.

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

Second, it is proposed to update the step 0a and 0b to describe that the UE is provided with the address of SLPKMF during Ranging/SL positioning Policy/parameters provisioning as specified in clause 5.1 of TS 23.586 [1]. Thus, the following Editor’s Note is removed.

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.

Third, it is proposed to add a NOTE describes whether group member ID is provisioned by the network or self-selected can be indicated by the network and remove the following Editor’s Note.

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

Fourth, it is proposed to add a NOTE describes whether to include group ID and group member ID in the SLPP message will be decided during normative work. Thus, the following Editor’s Note is removed.

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

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.

Fifth, the above Editor’s Note is formulated incorrectly as impersonation of other UE is not relevant to the encryption of identifiers in the SLPP message. Therefore, it is proposed to reformulate the Editor’s Note as follows.

Editor’s Note: privacy for the Group ID and Group member ID is FFS.

This solution applies to one-to-many communication as specified in TS 33.303 [2]. It is independent of cast type. Therefore, the following Editor’s Note is removed.

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

Lastly, it is proposed to add an evaluation of this solution based on the proposed updates.

# 4 Detailed proposal

It is proposed that SA3 approve the below pCR for inclusion in the TR [3].

**\*\*\*\*\* START OF 1st CHANGES \*\*\*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-86: "Study on Architecture Enhancement to support Ranging based services and sidelink positioning"

[3] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[4] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[5] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[6] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[7] 3GPP TS 22.261: "Service requirements for the 5G system".

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[10] 3GPP TR 38.859: "Study on expanded and improved NR positioning".

[xx] 3GPP TS 23.586: “Architectural Enhancements to support Ranging based services and Sidelink Positioning”

**\*\*\*\*\* END OF 1st CHANGES \*\*\*\*\***

**\*\*\*\*\* START OF 2nd CHANGES \*\*\*\*\***

## 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 belong 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 one-to-many communication

0a and 0b. The UE is provided with the Ranging/SL positioning application identifier during the parameters/policy provisioning for Ranging/SL positioning service as specified in clause 5.1 of TS 23.586 [xx].

NOTE 1: The SLPP one-to-many communication can use either broadcast or groupcast at the AS layer.

NOTE 2: For ProSe UEs, the Ranging/SL positioning application identifier is the ProSe identifier [xx].

NOTE 3: For V2X UEs, the Ranging/SL positioning application identifier is the V2X service type [xx].NOTE x: Whether to include group ID and group member ID in the SLPP message will be decided during normative work.

Editor’s Note: whether V2X UEs can support the same procedure would be determined by SA2.

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 Ranging /SL positioning application identifier.

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 x: In case the SLPLMF of a receiving UE is different from the SLPKMF of a sending UE, the provisioning of security materials as specified in clause 6.1.3.2 in TS 33.503 [6] is reused.

NOTE x: Group refers to the Ranging/SL positioning service. Accordingly, Group ID refers to the Ranging/SL positioning application identifier and Group member ID refers to the identifier of the UE that is authorized to receive the Ranging/SL positioning service.

NOTE x: 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.

NOTE x: Whether group member ID is provisioned by the network or self-selected will be decided during normative work.

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.

#### 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 [8] are used to calculate MAC.

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 x: 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: privacy for the Group ID and Group member ID is FFS.

##### 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

This solution addresses the second security requirement in Key Issue #1 (privacy protection during communication for Ranging/SL positioning) and all the security requirements in Key Issue #5 (Confidentiality, integrity, and replay protection of SLPP signaling over groupcast and broadcast).

This solution supports both in-coverage and out-of-coverage UEs.

Editor’s Note: Further evaluation is FFS.

**\*\*\*\*\* END OF 2nd CHANGES \*\*\*\*\***