**3GPP TSG-CT WG1 Meeting #146C1-240222**

**E-meeting, 22 – 26 January 2024**

**Source: Xiaomi**

**Title: Security for ranging and sidelink positioning UE discovery with 5G ProSe capable UE**

**Spec: 3GPP TS 24.514 v0.5.0**

**Agenda item: 18.2.23**

**Document for: Agreement**

**1. Introduction**

This p-CR provides the procedure of Discovery Key Request/Response to support security for ranging and sidelink positioning UE discovery with 5G ProSe capable UE.

**2. Reason for Change**

Security mechanisms are defined to provide protection for ranging and sidelink positioning UE discovery and ranging and sidelink positioning communication for ProSe capable UE in 3GPP TS 33.533. The security mechanisms for both models of restricted ranging and sidelink positioning UE discovery defined in clause 6.1.3.2 of TS 33.533 are ProSe capable UEs to provide protection for Ranging/SL positioning UE discovery with the following changes:

*- SLPKMF rather than 5G DDNMF/5G PKMF is used to provision discovery security materials for Ranging/SL positioning UE discovery.*

*- Ranging/SL Positioning application identifier (as defined in clause 3.1 of TS 23.586 [2]) instead of the Relay Service Code (RSC) is included in the Discovery Key Request/Response messages.*

*- The SLPKMF of the monitoring/discoverer UE discovers the SLPKMF(s) of potential announcing/discoveree UE(s) supporting the Ranging/SL Positioning application identifier based on a configured list of PLMNs supporting the corresponding Ranging/SL Positioning application.*

So the procedure of Discovery Key Request/Response is proposed to be defined.

**3. Proposal**

It is proposed to agree the following changes to 3GPP TS 24.514 v0.5.0.

\* \* \* First Change \* \* \* \*

### 8.2.1 Security for ranging and sidelink positioning UE discovery with 5G ProSe capable UE

#### 8.2.1.1 General

For ranging and sidelink positioning services provided by network operators, the security procedure for ranging and sidelink positioning UE discovery with 5G ProSe capable UE include the following:

- the ranging and sidelink positioning discovery key request procedure as defined in clause 8.2.1.2.

#### 8.2.1.2 Ranging and sidelink positioning discovery key request procedure

##### 8.2.1.2.1 General

The purpose of the ranging and sidelink positioning discovery key request procedure is for the 5G ProSe capable UE:

- to obtain the ranging and sidelink positioning UE discovery security parameters for 5G ProSe capable UE, applicable when the UE acts as any UE role for ranging and sidelink positioning over user plane as specified in 3GPP TS 33.533 [5].

##### 8.2.1.2.2 Ranging and sidelink positioning discovery key request procedure initiation

The UE shall initiate the ranging and sidelink positioning discovery key request procedure if the UE is authorized to act as any UE role for ranging and sidelink positioning and uses the security procedure over user plane as specified in 3GPP TS 33.533 [5]:

1) when the UE has no ranging and sidelink positioning UE discovery security parameters for 5G ProSe capable UE and the UE is in NG-RAN coverage; or

2) after expiration of timer Tx1, when in NG-RAN coverage or when entering NG-RAN coverage; or

The UE shall initiate the ranging and sidelink positioning discovery key request procedure by sending a PROSE\_SECURITY\_PARAM\_REQUEST message with the <RangingSl-discovery-security-parameters-request> element. In the < RangingSl-discovery-security-parameters-request> element, the UE:

a) shall include a new transaction ID;

b) shall indicate the UE role(s) of the UE requesting the ranging and sidelink positioning UE discovery security parameters for 5G ProSe capable UE;

c) shall include the PC5 UE security capabilities indicating ciphering algorithms supported by the UE; and

d) shall include the ranging and sidelink positioning application identifier.

NOTE: If the requested model is not included in the PROSE\_SECURITY\_PARAM\_REQUEST message, security parameters are requested for both model A and model B of the ranging and sidelink positioning UE discovery over PC5 interface.

Figure 8.2.1.2.2.1 illustrates the interaction of the UE and the SLPKMF in the Discovery key request procedure.



Figure 8.2.1.2.2.1: Discovery key request procedure

##### 8.2.1.2.3 Ranging and sidelink positioning discovery key request procedure accepted by the SLPKMF

Upon receiving a PROSE\_SECURITY\_PARAM\_REQUEST message with the <RangingSl-discovery-security-parameters-request> element, if the PROSE\_SECURITY\_PARAM\_REQUEST message is received over a TLS tunnel established by a UE authorized to act as any UE role for ranging and sidelink positioning the SLPKMF shall send a PROSE\_SECURITY\_PARAM\_RESPONSE message containing a <RangingSl-discovery-security-parameters-accept> element. In the <RangingSl-discovery-security-parameters-accept> element, the SLPKMF:

a) shall include the transaction ID set to the value of the transaction ID received in the PROSE\_SECURITY\_PARAM\_REQUEST message;

b) shall include the expiration timer of the ranging and sidelink positioning UE discovery security parameters for 5G ProSe capable UE;

c) for the received ranging and sidelink positioning application identifier for which the UE is authorized to act as any UE role for the ranging and sidelink positioning:

1) shall include the code-receiving security parameters containing one or more of DUSK, DUIK and DUCK with associated encrypted bitmask; and

2) shall include the selected ciphering algorithm;

d) shall include the current time set to the current UTC-based time at the SLPKMF and the max offset.

The SLPKMF of the monitoring or discoverer UE discovers the SLPKMF(s) of potential announcing or discoveree UE(s) supporting the ranging and sidelink positioning based on a configured list of PLMNs supporting the corresponding ranging and sidelink positioning.

##### 8.2.1.2.4 Ranging and sidelink positioning discovery key request procedure completion by the UE

Upon receipt of the PROSE\_SECURITY\_PARAM\_RESPONSE message with the <RangingSl-discovery-security-parameters-accept>, if the transaction ID contained in the <RangingSl-discovery-security-parameters-accept> element matches the value sent by the UE in a PROSE\_SECURITY\_PARAM\_REQUEST message with the <RangingSl-discovery-security-parameters-request> element, the UE:

a) shall store the ranging and sidelink positioning UE discovery security parameters for 5G ProSe capable UE, shall stop timer Tx1 if running, and shall start timer T5x1 with the value of the expiration timer indicated in the ranging and sidelink positioning UE discovery security parameters for 5G ProSe capable UE; and

b) shall set a ProSe clock (see 3GPP TS 33.533 [5]) to the value of the received current time parameter and store the received max offset.

##### 8.2.1.2.5 Ranging and sidelink positioning discovery key request procedure not accepted by the SLPKMF

If the PROSE\_SECURITY\_PARAM\_REQUEST message with the <RangingSl-discovery-security-parameters-request> element cannot be accepted by the SLPKMF, the SLPKMF shall send a PROSE\_SECURITY\_PARAM\_RESPONSE message containing a <RangingSl-discovery-security-parameters-reject> element. In the <RangingSl-discovery-security-parameters-reject> element, the SLPKMF shall include the transaction ID set to the value of the transaction ID received in the PROSE\_SECURITY\_PARAM\_REQUEST message and shall include an appropriate PC8 control protocol cause value.

Upon receipt of the PROSE\_SECURITY\_PARAM\_RESPONSE message with the <RangingSl-discovery-security-parameters-reject> element, if the transaction ID contained in the <RangingSl-discovery-security-parameters-reject> element matches the value sent by the UE in a PROSE\_SECURITY\_PARAM\_REQUEST message with the <RangingSl-discovery-security-parameters-request> element, the UE shall consider the Discovery key request procedure as rejected.

##### 8.2.1.2.6 Abnormal cases in the UE

The following abnormal cases can be identified:

a) Indication from the transport layer of transmission failure of PROSE\_SECURITY\_PARAM\_REQUEST message (e.g. after TCP retransmission timeout).

The UE shall close the existing secure connection to the SLPKMF, establish a new secure connection and then restart the Discovery key request procedure.

b) No response from the SLPKMF after the PROSE\_SECURITY\_PARAM\_REQUEST message has been successfully delivered (e.g. TCP ACK has been received for the PROSE\_SECURITY\_PARAM\_REQUEST message)

The UE shall retransmit the PROSE\_SECURITY\_PARAM\_REQUEST message.

NOTE: The timer to trigger retransmission and the maximum number of allowed retransmissions are UE implementation specific.

##### 8.2.1.2.7 Abnormal cases in the SLPKMF

The following abnormal cases can be identified:

a) Indication from the lower layer of transmission failure of PROSE\_SECURITY\_PARAM\_RESPONSE message.

After receiving an indication from lower layer that the PROSE\_SECURITY\_PARAM\_RESPONSE message has not been successfully acknowledged (e.g. TCP ACK is not received), the SLPKMF shall abort the procedure.

\* \* \* End of Changes \* \* \* \*