**3GPP TSG-CT WG1 Meeting #134-eC1-22xxxx**

**E-Meeting, 17th – 25th February 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Introducing the 5G ProSe direct link re-keying procedure**

**Spec: 3GPP TS** **TS 24.554 V1.1.0**

**Agenda item: 17.2.18**

**Document for: Agreement**

**1. Reason for Change**

Stage-2 security spec for 5G ProSe TS 33.503 states the following:

*6.2.2 Security requirements*

*(…)*

*The system shall support means for a secure refresh of the UE security context.*

*NOTE: The security context refresh may be triggered based on various options (e.g. validity time etc.)*

*6.2.3 Security procedures*

*The unicast mode security mechanism defined in clause 5.3 of TS 33.536 [6] is reused in 5G ProSe to provide unicast mode 5G ProSe Direct communication security.*

The above statements indicate the need to introduce a re-keying procedure, similar to the re-keying procedure that was used for V2X services in 5G system in TS 24.587.

Hence this pCR introduces the 5G ProSe direct link re-keying procedure, where the V2X 5G re-keying procedure is reused for that purpose, with the following modifications:

1- Changing "PC5 unicast link re-keying" to "5G ProSe direct link re-keying".

2- Defining the timer T50zy for the 5G ProSe direct link re-keying procedure.

3- Changing "DIRECT LINK REKEYING REQUEST" to "PROSE DIRECT LINK REKEYING REQUEST".

4- Changing "DIRECT LINK REKEYING RESPONSE" to "PROSE DIRECT LINK REKEYING RESPONSE".

5- Correcting references and clauses numbering.

6- Adding an Editor's note to indicate that any possible changes to the 5G ProSe direct link re-keying procedure due to the security requirements of 5G ProSe layer-2 UE-to-network relay or 5G ProSe layer-3 UE-to-network relay are FFS and waiting for SA3 conclusion.

**2. Proposal**

It is proposed to agree the following changes to 3GPP TS 24.554 V1.1.0.

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

### 7.2.1 Overview

This clause describes the PC5 signalling protocol procedures between two UEs for one-to-one (i.e., unicast) mode of ProSe direct communication. The following PC5 signalling protocol procedures are defined:

a) 5G ProSe direct link establishment;

b) 5G ProSe direct link modification;

c) 5G ProSe direct link release;

d) 5G ProSe direct link identifier update;

e) 5G ProSe direct link keep-alive; and

f) 5G ProSe direct link re-keying.

Each 5G ProSe direct link is associated with a 5G ProSe direct link context. For 5G ProSe UE-to-network relay, the 5G ProSe direct link context includes:

a) user info ID and layer-2 ID of 5G ProSe remote UE;

b) user info ID and layer-2 ID of 5G ProSe UE-to-network relay UE;

c) relay service code; and

d) in the case of 5G ProSe Layer-3 UE-to-network relay, the network layer protocol and the information about PC5 QoS flow(s).

The 5G ProSe direct link context shall be created during a 5G ProSe direct link establishment procedure, be updated accordingly after a 5G ProSe direct link modification procedure or 5G ProSe direct link identifier update procedure, and be deleted during the 5G ProSe direct link release procedure or during a local release of 5G ProSe direct link as specified in clause 7.2.

\* \* \* Next Change \* \* \* \*

### 7.2.x 5G ProSe direct link re-keying procedure

#### 7.2.x.1 General

The purpose of the 5G ProSe direct link re-keying procedure is to derive a new KNRP-sess and, optionally, a new KNRP for an existing PC5 unicast link. The UE sending the PROSE DIRECT LINK REKEYING REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

NOTE 1: There is no benefit in performing the 5G ProSe direct link re-keying procedure when using the null integrity protection algorithm, hence it is recommended not to trigger it when using the null integrity protection algorithm.

Editor's note: Any possible changes to the 5G ProSe direct link re-keying procedure due to the security requirements of 5G ProSe layer-2 UE-to-network relay or 5G ProSe layer-3 UE-to-network relay are FFS and waiting for SA3 conclusion.

#### 7.2.x.2 5G ProSe direct link re-keying procedure initiation by the initiating UE

The initiating UE shall meet the following pre-condition before initiating the 5G ProSe direct link re-keying procedure:

a) there is a PC5 unicast link between the initiating UE and the target UE; and

1) if the session key KNRP-sess used to protect PC5 unicast link needs to be refreshed and neither timer T5089 nor T50zy are running;

2) if the UE wants to refresh KNRP and neither timer T5089 nor T50zy are running; or

3) if the lower layers indicate that a 5G ProSe direct link re-keying procedure needs to be performed.

In order to initiate the 5G ProSe direct link re-keying procedure, the initiating UE shall create a PROSE DIRECT LINK REKEYING REQUEST message. In this message, the initiating UE:

a) shall include the Key establishment information container IE if the null integrity protection algorithm is not in use;

NOTE 1: The key establishment information container is provided by upper layers.

b) shall include a Nonce\_1 IE set to the 128-bit nonce value generated by the initiating UE for the purpose of session key refresh over this PC5 unicast link if the null integrity protection algorithm is not in use;

c) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the re-keying of this PC5 unicast link;

d) shall include the MSB of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.503 [34] if the null integrity protection algorithm is not in use; and

e) may include a Re-authentication indication if the initiating UE wants to derive a new KNRP.

After the PROSE DIRECT LINK REKEYING REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication, and start timer T50zy. The UE shall not send a new PROSE DIRECT LINK REKEYING REQUEST message to the same target UE while timer T50zy is running.

NOTE 2: In order to ensure successful 5G ProSe direct link re-keying, T50zy should be set to a value larger than the sum of T50aa and T5089.



Figure 7.2.x.2.1: 5G ProSe direct link re-keying procedure

#### 7.2.x.3 5G ProSe direct link re-keying procedure accepted by the target UE

Upon receipt of a PROSE DIRECT LINK REKEYING REQUEST message, if the PROSE DIRECT LINK REKEYING REQUEST message includes a Re-authentication indication, the target UE shall derive a new KNRP. This may require performing one or more 5G ProSe direct link authentication procedures as specified in clause 7.2.z.

NOTE: How many times the 5G ProSe direct link authentication procedure needs to be performed to derive a new KNRP depends on the authentication method used.

Then the target UE shall initiate a 5G ProSe direct link security mode control procedure as specified in in clause 7.2.10

Upon successful completion of the 5G ProSe direct link security mode control procedure, the target UE shall create a PROSE DIRECT LINK REKEYING RESPONSE message.

After the PROSE DIRECT LINK REKEYING RESPONSE message is generated, the target UE shall pass this message to the lower layers for transmission along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication.

#### 7.2.x.4 5G ProSe direct link re-keying procedure completion by the initiating UE

Upon receipt of the PROSE DIRECT LINK REKEYING RESPONSE message, the initiating UE shall stop timer T50zy and check the integrity of the PROSE DIRECT LINK REKEYING RESPONSE message using the new NRPIK.

After receiving the PROSE DIRECT LINK REKEYING RESPONSE message, the initiating UE shall delete the old security context it has for the target UE.

#### 7.2.x.5 Abnormal cases at the initiating UE

The following abnormal cases can be identified:

a) Timer T50zy expires.

The initiating UE shall retransmit the PROSE DIRECT LINK REKEYING REQUEST message and restart timer T50zy. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the 5G ProSe direct link re-keying procedure, shall provide an indication of deactivation of the PC5 unicast security protection and deletion of security context for the PC5 unicast link to the lower layer, if applicable, along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication and may initiate the 5G ProSe direct link release procedure.

NOTE: The maximum number of allowed retransmissions is UE implementation specific.

b) The need to use this PC5 unicast link no longer exists before the 5G ProSe direct link re-keying procedure is completed.

The initiating UE shall abort the procedure and shall provide an indication of deactivation of the PC5 unicast security protection and deletion of security context for the PC5 unicast link to the lower layer, if applicable, along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication.

c) For the same PC5 unicast link, if the initiating UE receives a DIRECT LINK IDENTIFIER UPDATE REQUEST message after initiating the 5G ProSe direct link re-keying procedure, the initiating UE shall stop the timer T50zy, abort the 5G ProSe direct link re-keying procedure and proceed with the 5G ProSe direct link identifier update procedure.

\* \* \* Next Change \* \* \* \*

## 12.3 Timers of 5G ProSe direct link management procedures

NOTE: Timer T3346 is defined in 3GPP TS 24.008 [31].

Table 12.3.1: 5G ProSe direct link management timers

| TIMER NUM. | | TIMER VALUE | CAUSE OF START | NORMAL STOP | ON  EXPIRY |
| --- | --- | --- | --- | --- | --- |
| T5080 | | 8s  NOTE 1 | Upon sending a PROSE DIRECT LINK ESTABLISHMENT REQUEST message | Upon receiving a PROSE DIRECT LINK ESTABLISHMENT ACCEPT or PROSE DIRECT LINK ESTABLISHMENT REJECT message from the target UE if the Target user info is included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message | Retransmission of PROSE DIRECT LINK ESTABLISHMENT REQUEST message if the Target user info is included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message; or  may abort the ongoing procedure if the Target user info is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message |
| T5081 | | 5s | Upon sending a PROSE DIRECT LINK MODIFICATION REQUEST message | Upon receiving a PROSE DIRECT LINK MODIFICATION ACCEPT or PROSE DIRECT LINK MODIFICATION REJECT or PROSE DIRECT LINK RELEASE REQUEST message from the target UE | Retransmission of PROSE DIRECT LINK MODIFICATION REQUEST message |
| T5082 | | 2s | Upon sending a PROSE DIRECT LINK IDENTIFIER UPDATE REQUEST message | Upon receiving a PROSE DIRECT LINK IDENTIFIER UPDATE ACCEPT or PROSE DIRECT LINK IDENTIFIER UPDATE REJECT or PROSE DIRECT LINK RELEASE REQUEST message from the target UE | Retransmission of the PROSE DIRECT LINK IDENTIFIER UPDATE REQUEST message |
| T5083 | | 2s | Upon sending a PROSE DIRECT LINK IDENTIFIER UPDATE ACCEPT message | Upon receiving a PROSE DIRECT LINK IDENTIFIER UPDATE ACK message or PROSE DIRECT LINK RELEASE REQUEST message from the initiating UE | Retransmission of the PROSE DIRECT LINK IDENTIFIER UPDATE ACCEPT message |
| T5084 | | 5s | Upon receiving a PC5 signalling message or PC5 user plane data | Upon PC5 unicast link release or upon initiating the PC5 unicast link keep-alive procedure | Initiate the PC5 unicast link keep-alive procedure |
| T5085 | | 5s | Upon sending a PROSE DIRECT LINK KEEPALIVE REQUEST message | Upon receiving a PC5 signalling message or PC5 user plane data | Retransmission of the PROSE DIRECT LINK KEEPALIVE REQUEST message |
| T5086 | | Default 10m  NOTE 2 | Upon receiving a Maximum inactivity period in a PROSE DIRECT LINK KEEPALIVE REQUEST message, receiving a PC5 signalling message or receiving PC5 user plane data | Upon receiving a PC5 signalling message or PC5 user plane data | Either initiate the PC5 unicast link keep-alive procedure or the PC5 unicast link release procedure |
| T5087 | | 5s | Upon sending a PROSE DIRECT LINK RELEASE REQUEST message | Upon receiving a PROSE DIRECT LINK RELEASE ACCEPT message from the target UE | Retransmission of PROSE DIRECT LINK RELEASE REQUEST message |
| T5088 | | As described in clause 7.2.2.5 and clause 7.2.6.3 | Upon receiving a PROSE DIRECT LINK ESTABLISHMENT REJECT message with PC5 signalling protocol cause value set to #13 "congestion situation" and a back-off timer value is provided in the message  Upon receiving a PROSE DIRECT LINK RELEASE REQUEST message with PC5 signalling protocol cause value set to #13 "congestion situation" and a back-off timer value is provided in the message | Upon receiving PROSE PC5 DISCOVERY message from the same UE-to-network relay UE due to starting Announcing UE procedure or Discoveree UE procedure as described in clause 8.2.1.2.1.2 and clause 8.2.1.3.2.2 respectively | Take the peer UE onboard for UE-to-network relay UE discovery and selection |
| T5089 | | 2s | Upon sending a PROSE DIRECT LINK SECURITY MODE COMMAND message | Upon receiving a PROSE DIRECT LINK SECURITY MODE COMPLETE or PROSE DIRECT LINK SECURITY MODE REJECT message from the target UE | Retransmission of PROSE DIRECT LINK SECURITY MODE COMMAND message |
| T50zy | | 8s | Upon sending a PROSE DIRECT LINK REKEYING REQUEST message | Upon receiving a PROSE DIRECT LINK REKEYING RESPONSE message or PROSE DIRECT LINK RELEASE REQUEST message from the target UE | Retransmission of PROSE DIRECT LINK REKEYING REQUEST message |
|  | |  |  |  |  |
| NOTE 1: If the Target user info is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message, then the initiating UE may keep the timer T5080 running upon receiving PROSE DIRECT LINK ESTABLISHMENT ACCEPT message.  NOTE 2: The value of this timer is the privacy timer value which is one of the configuration parameters for 5G ProSe direct communication (see clause 5.2.4) and it is specified in 3GPP TS 24.555 [17] clause 5.4. | | | | | |

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