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

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

**Source: Nokia, Nokia Shanghai Bell, InterDigital**

**Title: Introducing the 5G ProSe direct link authentication 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 mutual authentication between two ProSe-enabled UEs during PC5 unicast shall be supported.*

*(…)*

*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 an authentication 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 authentication procedure, where the V2X 5G authentication procedure is reused for that purpose, with the following modifications:

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

2- Defining the timer T50aa for the 5G ProSe direct link authentication procedure.

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

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

5- Correcting references and clauses numbering.

6- Adding an Editor's note to indicate that possible changes to the 5G ProSe direct link authentication procedure due to supporting 5G ProSe layer-3 UE-to-network relay are FFS.

7- Adding a NOTE to indicate that 5G ProSe direct link authentication procedure is also applicable for 5G ProSe layer-2 UE-to-network relay case without extra modifications in the procedure, as indicated in TS 33.503 clause 6.3.4 as following:

*6.3.4 Security for 5G ProSe Communication via 5G ProSe Layer-2 UE-to-Network Relay*

*(…)*

*The remote UE and the relay UE shall establish security for PC5 connection as specified in clause 6.2.*

**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 authentication.

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.y 5G ProSe direct link authentication procedure

#### 7.2.y.1 General

The 5G ProSe direct link authentication procedure is used to perform mutual authentication of UEs establishing a PC5 unicast link and to derive a new KNRP shared between two UEs during a 5G ProSe direct link establishment procedure or a 5G ProSe direct link re-keying procedure. After successful completion of the 5G ProSe direct link authentication procedure, the new KNRP is used for security establishment during the 5G ProSe direct link security mode control procedure as specified in clause 7.2.10. The UE sending the PROSE DIRECT LINK AUTHENTICATION REQUEST message is called the "initiating UE" and the other UE is called the "target UE".

NOTE: The 5G ProSe direct link authentication procedure is not applicable for 5G ProSe layer-3 UE-to-network relay.

#### 7.2.y.2 5G ProSe direct link authentication procedure initiation by the initiating UE

The initiating UE shall meet one of the following pre-conditions if signalling integrity protection is activated based on the decision of the initiating UE, before initiating the 5G ProSe direct link authentication procedure:

a) the target UE has initiated a 5G ProSe direct link establishment procedure toward the initiating UE by sending a PROSE DIRECT LINK ESTABLISHMENT REQUEST message and:

1) the PROSE DIRECT LINK ESTABLISHMENT REQUEST message:

i) includes a target user info IE which includes the application layer ID of the initiating UE; or

ii) does not include a target user info IE and the initiating UE is interested in the ProSe service identified by the ProSe identifier in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message; and

2) the KNRP ID is not included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE does not have an existing KNRP for the KNRP ID included in PROSE DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE derives a new KNRP; or

b) the target UE has initiated a 5G ProSe direct link re-keying procedure toward the initiating UE by sending a PROSE DIRECT LINK REKEYING REQUEST message and the PROSE DIRECT LINK REKEYING REQUEST message includes a Re-authentication indication.

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

a) shall include the key establishment information container IE.

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

After the PROSE DIRECT LINK AUTHENTICATION 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.

The initiating UE shall start timer T50aa. The UE shall not send a new PROSE DIRECT LINK AUTHENTICATION REQUEST message to the same target UE while timer T50aa is running.



Figure 7.2.y.2.1: 5G ProSe direct link authentication procedure

#### 7.2.y.3 5G ProSe direct link authentication procedure accepted by the target UE

Upon receipt of a PROSE DIRECT LINK AUTHENTICATION REQUEST message, if a new assigned initiating UE's layer-2 ID is included, the target UE shall replace the original initiating UE's layer-2 ID with the new assigned initiating UE's layer-2 ID for unicast communication. If the target UE determines that the PROSE DIRECT LINK AUTHENTICATION REQUEST message can be accepted, the target UE shall create a PROSE DIRECT LINK AUTHENTICATION RESPONSE message. The target UE shall check if the number of established PC5 unicast links is less than the implementation-specific maximum number of established NR PC5 unicast links allowed in the UE at a time. In this message, the target UE:

a) shall include the Key establishment information container IE.

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

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

#### 7.2.y.4 5G ProSe direct link authentication procedure completion by the initiating UE

Upon receiving a PROSE DIRECT LINK AUTHENTICATION RESPONSE message, if the initiating UE determines that the PROSE DIRECT LINK AUTHENTICATION RESPONSE message can be accepted, the initiating UE shall stop timer T50aa.

NOTE: When the initiating UE derives the new KNRP during the 5G ProSe direct link authentication procedure depends on the authentication method in use.

#### 7.2.y.5 5G ProSe direct link authentication procedure not accepted by the target UE

If the PROSE DIRECT LINK AUTHENTICATION REQUEST message cannot be accepted, the target UE shall create a DIRECT LINK AUTHENTICATION REJECT message. In this message, the target UE shall include a PC5 signalling protocol cause IE indicating one of the following cause values:

#6: authentication failure;

#5: lack of resources for PC5 unicast link.

If this 5G ProSe direct link authentication procedure is triggered during the 5G ProSe direct link establishment procedure and the implementation-specific maximum number of established NR PC5 unicast links has been reached, then the target UE shall send a DIRECT LINK AUTHENTICATION REJECT message containing PC5 signalling protocol cause value #5 "lack of resources for PC5 unicast link".

After the DIRECT LINK AUTHENTICATION REJECT 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.

The target UE shall abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link authentication procedure if the ongoing procedure is the 5G ProSe direct link establishment procedure and the Target user info is included in the PROSE DIRECT LINK ESTABLISHMENT REQUEST message.

Upon receipt of the DIRECT LINK AUTHENTICATION REJECT message, the initiating UE shall stop timer T50aa and abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link authentication procedure.

#### 7.2.y.6 5G ProSe direct link authentication procedure not accepted by the initiating UE

If the PROSE DIRECT LINK AUTHENTICATION RESPONSE message cannot be accepted, the initiating UE shall stop timer T50aa and create a DIRECT LINK AUTHENTICATION FAILURE message. In this message, the initiating UE may include the Key establishment information container IE if provided by upper layers.

After the DIRECT LINK AUTHENTICATION FAILURE 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.

The initiating UE shall abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link authentication procedure.

Upon receipt of the DIRECT LINK AUTHENTICATION FAILURE message, the target UE shall abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link authentication procedure and shall indicate to upper layers that authentication has failed.

#### 7.2.y.7 Abnormal cases

##### 7.2.y.7.1 Abnormal cases at the initiating UE

a) Timer T50aa expires.

 The initiating UE shall retransmit the PROSE DIRECT LINK AUTHENTICATION REQUEST message and restart timer T50aa. After reaching the maximum number of allowed retransmissions, the initiating UE shall abort the 5G ProSe direct link authentication procedure and shall abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link authentication 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 authentication procedure is completed.

 The initiating UE shall abort the 5G ProSe direct link authentication procedure and shall abort the ongoing procedure that triggered the initiation of the 5G ProSe direct link authentication 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; ormay 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 10mNOTE 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 messageUpon 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 |
| T50aa | 2s | Upon sending a PROSE DIRECT LINK AUTHENTICATION REQUEST message | Upon receiving a PROSE DIRECT LINK AUTHENTICATION RESPONSE or DIRECT LINK AUTHENTICATION REJECT message from the target UE | Retransmission of PROSE DIRECT LINK AUTHENTICATION 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 \* \* \* \*