**3GPP TSG-CT WG1 Meeting #128-eC1-21xxxx**

**Electronic meeting, 25 February – 5 March 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0182** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Mutual authentication for PC5 unicast link | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2021-02-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) ... Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The PC5 unicast link authentication procedure has two purposes:  1- To perform mutual authentication for two peer UEs.  2- To derive a new KNRP shared between two peer UEs  This can be noticed from TS 24.587 subclause 6.1.2.6.1:  6.1.2.6.1 General  The PC5 unicast 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 PC5 unicast link establishment procedure or a PC5 unicast link re-keying procedure.  SA3 CR0023 (S3-210804) emphasizes on the mutual authentication as a purpose for the Authentication procedure, where it states that the two UEs authenticate each other using the information exchanged in Key\_Est\_Info (i.e. Key establishment information container IE). **It also states that the authentication procedure may fail due to being rejected from either of the UEs to the other UE, due to failure in authenticating that UE.**  Now, as per current stage-3 specification TS 24.587, if the target UE needs to reject the received Authentication Request message due to e.g. invalid authentication parameters in the received Key establishment information container IE (after being validated by upper layers at target UE), then target UE can send DIRECT LINK AUTHENTICATION REJECT message to the initiating UE.  BUT in current specification TS 24.587, there is no way for the initiating UE to reject the Authentication procedure after it has received the Authentication Response message. **As stated above, there can be cases where the upper layers at the initiating UE wants to reject the Key establishment information container received in DIRECT LINK AUTHENTICATION RESPONSE, e.g. due to validation failures for the authentication parameters provided in that container.** This comes from the fact that the initiating UE is in need to authenticate the target UE by checking the parameters in the received response message (where this validation happens at upper layers of the initiating UE). Otherwise the mutual authentication wouldn't be achieved.  To cover this gap and to align with CR0023 (S3-210804), there shall be a new authentication failure message that can be used by initiating UE as a reply to the Authentication Response message in case of failure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Introducing the new message DIRECT LINK AUTHENTICATION FAILURE to cover the case when the initiating UE needs to reject the Authentication procedure in case the Authentication Response message received from the target UE contains invalid authentication information e.g. if the received Key establishment information container in Authentication Response is rejected by upper layers of the initiating UE.  Also it is proposed to include the optional container "Key establishment information container IE" in the DIRECT LINK AUTHENTICATION FAILURE message, which can be used in case the upper layers at the initiating UE want to communication some authentication failure parameters to the upper layer at the target UE.  Please note that, the message type of the new message DIRECT LINK AUTHENTICATION FAILURE is added at end of the table **8.4.1.1** in order to keep the current message type values without any change, for not causing any backward compatibility issue. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There will be no possibility for the initiating UE to reject the Authentication procedure in case the received Authentication Response message from the target UE contains invalid authentication information e.g. if the received Key establishment information container in Authentication Response is rejected by upper layers of the initiating UE due to failure in authenticating the target UE.  Also, misalignment between stage 2 and stage 3 specs will remain.  **Backward compatibility analysis:**  The CR is backward compatible, since there are no previous releases available for this protocol, plus this CR fixes a gap in the functionality. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.6.2, 6.1.2.6.4, 6.1.2.6.5A (new), 6.1.2.11.3, 7.3.24 (new), 7.3.24.1 (new), 7.3.24.2 (new), 8.4.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TS 33.536 CR 0023 (S3-210804) | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Revision 1:  Clarifying in subclause 6.1.2.6.5A that UE shall stop timer T5006.  Adding subclause 7.3.24.2.  Modifying the figure in subclause 6.1.2.6.2. | | | | | | | | |

\*\*\*\*\* First change \*\*\*\*\*

6.1.2.6.2 PC5 unicast 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 PC5 unicast link authentication procedure:

a) the target UE has initiated a PC5 unicast link establishment procedure toward the initiating UE by sending a DIRECT LINK ESTABLISHMENT REQUEST message and:

1) the 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 V2X service identified by the V2X service identifier in the DIRECT LINK ESTABLISHMENT REQUEST message; and

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

b) the target UE has initiated a PC5 unicast link re-keying procedure toward the initiating UE by sending a DIRECT LINK REKEYING REQUEST message and the DIRECT LINK REKEYING REQUEST message includes a Re-authentication indication.

In order to initiate the PC5 unicast link authentication procedure, the initiating UE shall create a 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 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 T5006. The UE shall not send a new DIRECT LINK AUTHENTICATION REQUEST message to the same target UE while timer T5006 is running.

****

**Figure 6.1.2.6.2: PC5 unicast link authentication procedure**

\*\*\*\*\* Next change \*\*\*\*\*

6.1.2.6.4 PC5 unicast link authentication procedure completion by the initiating UE

Upon receiving a DIRECT LINK AUTHENTICATION RESPONSE message, if the initiating UE determines that the DIRECT LINK AUTHENTICATION RESPONSE message can be accepted, the initiating UE shall stop timer T5006.

NOTE: When the initiating UE derives the new KNRP during the PC5 unicast link authentication procedure depends on the authentication method in use.

\*\*\*\*\* Next change \*\*\*\*\*

6.1.2.6.5A PC5 unicast link authentication procedure not accepted by the initiating UE

If the DIRECT LINK AUTHENTICATION RESPONSE message cannot be accepted, the initiating UE shall stop timer T5006 and create a DIRECT LINK AUTHENTICATION FAILURE message. In this message, the target 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 PC5 unicast 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 PC5 unicast link authentication procedure and shall indicate to upper layers that authentication has failed.

\*\*\*\*\* Next change \*\*\*\*\*

6.1.2.11.3 Checking of PC5 signalling messages in the UE

If the signalling integrity protection is not activated for PC5 unicast link, all PC5 signalling messages are processed by the UE without integrity protection.

If the signalling integrity protection is activated for PC5 unicast link, except the messages listed below, no PC5 signalling messages that is not integrity protected shall be processed by the UE:

a) DIRECT LINK ESTABLISHMENT REQUEST message;

b) DIRECT LINK ESTABLISHMENT REJECT message;

c) DIRECT LINK AUTHENTICATION REQUEST message;

d) DIRECT LINK AUTHENTICATION RESPONSE message;

e) DIRECT LINK AUTHENTICATION REJECT message;

f) DIRECT LINK SECURITY MODE REJECT message; and

g) DIRECT LINK AUTHENTICATION FAILURE message.

NOTE: These messages are accepted by the receiving UE without integrity protection, as in certain situations they are sent by the peer UE before security can be activated.

Once the secure exchange of PC5 signalling messages has been established, the receiving UE shall not process any PC5 signalling message that does not successfully pass the integrity check. The DIRECT LINK SECURITY MODE COMMAND message shall be processed as specified in clause 6.1.2.7.3. If any PC5 signalling message is received as not integrity protected and not ciphered even though the secure exchange of PC5 signalling messages has been established, then the receiving UE shall discard this message.

\*\*\*\*\* Next change \*\*\*\*\*

7.3.24 Direct link authentication failure

7.3.24.1 Message definition

This message is sent by a UE to another peer UE to reject a DIRECT LINK AUTHENTICATION RESPONSE message. See table 7.3.24.1.1.

Message type: DIRECT LINK AUTHENTICATION FAILURE

Significance: dual

Direction: UE to peer UE

**Table 7.3.24.1.1: DIRECT LINK AUTHENTICATION FAILURE message content**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **IEI** | **Information Element** | **Type/Reference** | **Presence** | **Format** | **Length** |
|  | DIRECT LINK AUTHENTICATION FAILURE message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | Key establishment information container | Key establishment information container  8.4.12 | O | TLV-E | 4-n |

7.3.24.2 Key establishment information container

The UE shall include this IE if it is provided by upper layers.

\*\*\*\*\* Next change \*\*\*\*\*

8.4.1 PC5 signalling message type

The purpose of the PC5 signalling message type information element is to indicate the type of messages used in PC5 signalling protocol.

The value part of the PC5 signalling message type information element used in the PC5 signalling messages is coded as shown in table 8.4.1.1.

The PC5 signalling message type is a type 3 information element, with the length of 1 octet.

**Table 8.4.1.1: PC5 signalling message type**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Bits | | | | | | | | | | | | | | |  | |  | |
| 8 | 7 | | 6 | | 5 | | 4 | | 3 | | 2 | | 1 | |  | |  | |
| 0 | 0 | | 0 | | 0 | | 0 | | 0 | | 0 | | 1 | |  | | DIRECT LINK ESTABLISHMENT REQUEST | |
| 0 | 0 | | 0 | | 0 | | 0 | | 0 | | 1 | | 0 | |  | | DIRECT LINK ESTABLISHMENT ACCEPT | |
| 0 | 0 | | 0 | | 0 | | 0 | | 0 | | 1 | | 1 | |  | | DIRECT LINK ESTABLISHMENT REJECT | |
| 0 | 0 | | 0 | | 0 | | 0 | | 1 | | 0 | | 0 | |  | | DIRECT LINK MODIFICATION REQUEST | |
| 0 | 0 | | 0 | | 0 | | 0 | | 1 | | 0 | | 1 | |  | | DIRECT LINK MODIFICATION ACCEPT | |
| 0 | 0 | | 0 | | 0 | | 0 | | 1 | | 1 | | 0 | |  | | DIRECT LINK MODIFICATION REJECT | |
| 0 | 0 | | 0 | | 0 | | 0 | | 1 | | 1 | | 1 | |  | | DIRECT LINK RELEASE REQUEST | |
| 0 | 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 0 | |  | | DIRECT LINK RELEASE ACCEPT | |
| 0 | 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 1 | |  | | DIRECT LINK KEEPALIVE REQUEST | |
| 0 | 0 | | 0 | | 0 | | 1 | | 0 | | 1 | | 0 | |  | | DIRECT LINK KEEPALIVE RESPONSE | |
| 0 | | 0 | | 0 | | 0 | | 1 | | 0 | | 1 | | 1 | |  | | DIRECT LINK AUTHENTICATION REQUEST |
| 0 | | 0 | | 0 | | 0 | | 1 | | 1 | | 0 | | 0 | |  | | DIRECT LINK AUTHENTICATION RESPONSE |
| 0 | | 0 | | 0 | | 0 | | 1 | | 1 | | 0 | | 1 | |  | | DIRECT LINK AUTHENTICATION REJECT |
| 0 | | 0 | | 0 | | 0 | | 1 | | 1 | | 1 | | 0 | |  | | DIRECT LINK SECURITY MODE COMMAND |
| 0 | | 0 | | 0 | | 0 | | 1 | | 1 | | 1 | | 1 | |  | | DIRECT LINK SECURITY MODE COMPLETE |
| 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 0 | |  | | DIRECT LINK SECURITY MODE REJECT |
| 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 0 | | 1 | |  | | DIRECT LINK REKEYING REQUEST |
| 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 1 | | 0 | |  | | DIRECT LINK REKEYING RESPONSE |
| 0 | | 0 | | 0 | | 1 | | 0 | | 0 | | 1 | | 1 | |  | | DIRECT LINK IDENTIFIER UPDATE REQUEST |
| 0 | | 0 | | 0 | | 1 | | 0 | | 1 | | 0 | | 0 | |  | | DIRECT LINK IDENTIFIER UPDATE ACCEPT |
| 0 | | 0 | | 0 | | 1 | | 0 | | 1 | | 0 | | 1 | |  | | DIRECT LINK IDENTIFIER UPDATE ACK |
| 0 | | 0 | | 0 | | 1 | | 0 | | 1 | | 1 | | 0 | |  | | DIRECT LINK IDENTIFIER UPDATE REJECT |
| 0 | 0 | | 0 | | 1 | | 0 | | 1 | | 1 | | 1 | |  | | DIRECT LINK AUTHENTICATION FAILURE | |
|  | | | | | | | | | | | | | | | | | | |

\*\*\*\*\* End of changes \*\*\*\*\*