**3GPP TSG-CT WG1 Meeting #125-eC1-205287**

**Electronic meeting, 20-28 August 2020 (was 205003)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.587** | **CR** | 0098 | **rev** | **1** | **Current version:** | **16.1.1** |  |
|  |
| *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:***  | Indication of security protection activation |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eV2XARC |  | ***Date:*** | 2020-07-24 |
|  |  |  |  |  |
| ***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 canbe 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | According to LS R2-2005978 (waiting for CT1 tdoc number), RAN2 would like to request SA3 and CT1 to support an indication for the initiation of security activation and the change of the key due to re-keying procedure. |
|  |  |
| ***Summary of change:*** |  |
|  |  |
| ***Consequences if not approved:*** | Lower layer cannot know whether security protection for the PC5 unicast link is necessary or not. |
|  |  |
| ***Clauses affected:*** | 6.1.2.2.3, 6.1.2.2.4, 6.1.2.7.2, 6.1.2.7.3 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** | Following aspects have been clarified.During SMC, PC5 unicast signalling security protection is activated.At the PC5 Unicast Link Establishment Accept, PC5 unicast user plane security protection is activated. |

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

##### 6.1.2.2.3 PC5 unicast link establishment procedure accepted by the target UE

Upon receipt of a DIRECT LINK ESTABLISHMENT REQUEST message, if the target UE accepts this request, the target UE shall uniquely assign a PC5 link identifier, create a PC5 unicast link context and assign a layer-2 ID for this PC5 unicast link. Then the target UE shall store this assigned layer-2 ID and the source layer-2 ID used in the transport of this message provided by the lower layers in the PC5 unicast link context.

If:

a) the target user info IE is included in the DIRECT LINK ESTABLISHMENT REQUEST message and this IE includes the target UE’s application layer ID; or

b) the target user info IE is not included in the DIRECT LINK ESTABLISHMENT REQUEST message and the target UE is interested in the V2X service(s) identified by the V2X service identifier IE in the DIRECT LINK ESTABLISHMENT REQUEST message;

then the target UE shall either:

a) identify an existing KNRP based on the KNRP ID included in the DIRECT LINK ESTABLISHMENT REQUEST message; or

b) if KNRP ID is not included in the DIRECT LINK ESTABLISHMENT REQUEST message, the target UE does not have an existing KNRP for the KNRP ID included in DIRECT LINK ESTABLISHMENT REQUEST message or the target UE wishes to derive a new KNRP, derive a new KNRP. This may require performing one or more PC5 unicast link authentication procedures as specified in subclause 6.1.2.6.

NOTE: How many times the PC5 unicast link authentication procedure needs to be performed to derive a new KNRP depends on the authentication method used.

After an existing KNRP was identified or a new KNRP was derived, the target UE shall initiate a PC5 unicast link security mode control procedure as specified in subclause 6.1.2.7.

Upon successful completion of the PC5 unicast link security mode control procedure, in order to determine whether the DIRECT LINK ESTABLISHMENT REQUEST message can be accepted or not, in case of IP communication, the target UE checks whether there is at least one common IP address configuration option supported by both the initiating UE and the target UE.

If the target UE accepts the PC5 unicast link establishment procedure, the target UE shall create a DIRECT LINK ESTABLISHMENT ACCEPT message. The target UE:

a) shall include the source user info set to the target UE’s application layer ID received from upper layers;

b) shall include a PQFI and the corresponding PC5 QoS parameters;

c) shall include an IP address configuration IE set to one of the following values if IP communication is used:

1) "IPv6 router" if IPv6 address allocation mechanism is supported by the target UE, i.e. acting as an IPv6 router; or

2) "IPv6 address allocation not supported" if IPv6 address allocation mechanism is not supported by the target UE;

d) shall include a link local IPv6 address IE formed locally based on IETF RFC 4862 [16] if IP address configuration IE is set to "IPv6 address allocation not supported" and the received DIRECT LINK ESTABLISHMENT REQUEST message included a link local IPv6 address IE; and

e) shall include the configuration of UE PC5 unicast user plane security protection based on the agreed user plane security policy, as specified in 3GPP TS 33.536 [20].

After the DIRECT LINK ESTABLISHMENT ACCEPT 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.

After sending the DIRECT LINK ESTABLISHMENT ACCEPT message, the target UE shall provide the following information along with the layer-2 IDs to the lower layer, which enables the lower layer to handle the coming PC5 signalling or traffic data:

a) the PC5 link identifier self-assigned for this PC5 unicast link;

b) PQFI(s) and its corresponding PC5 QoS parameters; and

c) Indication of activation of the PC5 unicast signalling or user plane security protection, or both, the corresponding NRPIK, NRPEK, KNPR-sess ID, and the selected security algorithm for the PC5 unicast link if applicable.

If the target UE accepts the PC5 unicast link establishment request, then the target UE may perform the PC5 QoS flow establishment over PC5 unicast link as specified in clause 6.1.2.12.

\*\*\*\*\* Second change \*\*\*\*\*

##### 6.1.2.2.4 PC5 unicast link establishment procedure completion by the initiating UE

Upon receipt of the DIRECT LINK ESTABLISHMENT ACCEPT message, the initiating UE shall stop timer T5000, uniquely assign a PC5 link identifier and create a PC5 unicast link context for this PC5 unicast link. Then the target UE shall store the source layer-2 ID and the destination layer-2 ID used in the transport of this message provided by the lower layers in the PC5 unicast link context. From this time onward the initiating UE shall use the established link for V2X communication over PC5 and additional PC5 signalling messages to the target UE.

After receiving the DIRECT LINK ESTABLISHMENT ACCEPT message, the initiating UE shall provide the following information along with the layer-2 IDs to the lower layer, which enables the lower layer to handle the coming PC5 signalling or traffic data:

a) the PC5 link identifier self-assigned for this PC5 unicast link;

b) PQFI(s) and its corresponding PC5 QoS parameters; and

c) Indication of activation of the PC5 unicast signalling or user plane security protection, or both, the corresponding NRPIK, NRPEK, KNPR-sess ID, and the selected security algorithm for the PC5 unicast link if applicable.

In addition, the initiating UE may perform the PC5 QoS flow establishment over PC5 unicast link as specified in clause 6.1.2.12.

\*\*\*\*\* Third change \*\*\*\*\*

##### 6.1.2.10.3 PC5 unicast link re-keying procedure accepted by the target UE

Upon receipt of a DIRECT LINK REKEYING REQUEST message, if the 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 PC5 unicast link authentication procedures as specified in subclause 6.1.2.6.

NOTE: How many times the PC5 unicast 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 PC5 unicast link security mode control procedure as specified in in subclause 6.1.2.7.

Upon successful completion of the PC5 unicast link security mode control procedure, the target UE shall create a DIRECT LINK REKEYING RESPONSE message. The target UE shall cipher and integrity protect the DIRECT LINK REKEYING RESPONSE message with the new security context.

After the DIRECT LINK REKEYING RESPONSE message is generated, the target UE shall pass this message and new security context 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.

\*\*\*\*\* Fourth change \*\*\*\*\*

##### 6.1.2.10.4 PC5 unicast link re-keying procedure completion by the initiating UE

Upon receipt of the DIRECT LINK REKEYING RESPONSE message, the initiating UE shall stop timer T5008 and check the integrity of the DIRECT LINK REKEYING RESPONSE message using the new NRPIK and send the new security context to the lower layer with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication.

\*\*\*\*\* End of change \*\*\*\*\*