**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:*** | 2020-08-26 |
|  |  |  |  |  |
| ***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 (**C1-204613**), 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.Security protection of PC5 unicast signalling and PC5 unicast user plane are optional. When the security protection is not activated for the PC5 unicast link, lower layer does not have to perform security protection. Therefore, two explicit indications are required to lower layer:* Security protection activation/deactivation on PC5 unicast signalling
* Security protection activation/deactivation on PC5 unicast user plane

According to RAN2 agreement on R2-2001668, 4 different LCIDs are allocated for the following SL SRBs:*i) The PC5-S signalling that is not protected, e.g., Direct Communication Request.**ii) The PC5-S signalling to activate security, i.e., Direct Security Mode Command and Direct Security Mode Complete.**iii) Other PC5-S signallings that are protected.**iv) PC5-RRC signallings that are protected.*Until the AS layer gets an indication that security has been turned ‘Activated’, it can assume that all PC5-S messages are unprotected, except the Security Mode Command and the Security Mode Complete which are for security activation. After the activation of security protection, all PC5-S msgs are treated as iii).For ii), there are only two PC5-S signalling (Direct Securit Mode Command and Direct Security Mode Complete), therefore, PC5-S message type itself can identify the PC5-S msg is for ii), which does not need an explicit indication.Please note that the security protection is applied per PC5 unicast link. Once the security protection is activated for the PC5 unicast link, lower layer applies the security protection for the PC5 unicast link until V2X layer indicates otherwise or the PC5 unicast link is released.V2X layer needs to provide lower layer with the security materials (e.g., selected algorithms, security keys). Note that the lower layer does security protection and validation, except for Direct Link SMC procedure.For integrity protection of Direct Link Security Mode Command message and integrity protection/ciphering of Direct Link Security Mode Complete message, the V2X needs to provide NRPIK, NRPEK, Knrp-sess ID, and the chosen algorithm during SMC procedure. It is assumed that lower layer applies this security materials for the pair of {Source L2 ID, Destination L2 ID}. After V2X layer assigns PC5 Link Identifier after completion of Direct Link Establishment procedure, V2X layer indicates the activation of security protection (signlaing/user plane respectively). |
|  |  |
| ***Summary of change:*** | When UE initiates Direct Link Security Mode Command, the V2X layer provides lower layer with NRPIK, NRPEK if applicable, KNRP-sess ID and the chosen algorithm.When UE sends Direct Link Securty Mode Complete, the V2X layer provides NRPIK, NRPEK if applicable, KNRP-sess ID and the chosen algorithm.When UE sends Direct Link Establish Accept, the V2X layer provides an indication of PC5 signaling/user plane security protection activation to lower layer.After receving Direct Link Establish Accept, the V2X layer provides an indication of PC5 signalling/user plane security protection activation to lower layer. |
|  |  |
| ***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;

c) Indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link; and

d) Indication of activation of the PC5 unicast user plane security protection 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;

c) Indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link; and

d) Indication of activation of the PC5 unicast user plane security protection 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 \*\*\*\*\*

##### 6.1.2.7.2 PC5 unicast link security mode control procedure initiation by the initiating UE

The initiating UE shall meet the following pre-conditions before initiating the PC5 unicast link security mode control 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 initiating UE has either identified an existing KNRP based on the KNRP ID included in the DIRECT LINK ESTABLISHMENT REQUEST message or derived 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:

1) if the target UE has included a Re-authentication indication in the DIRECT LINK REKEYING REQUEST message, the initiating UE has derived a new KNRP.

If a new KNRP has been derived by the initiating UE, the initiating UE shall generate the 16 MSBs of KNRP ID to ensure that the resultant KNRP ID will be unique in the initiating UE.

The initiating UE shall select security algorithms in accordance with its UE PC5 unicast signalling security policy and the target UE’s PC5 unicast signalling security policy. If the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, the initiating UE shall not select the null integrity protection algorithm if the initiating UE or the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required". If the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure, the initiating UE shall not select the null integrity protection algorithm if the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm.

Then the initiating UE shall:

a) generate a 128-bit Nonce\_2 value;

b) derive KNRP-sess from KNRP, Nonce\_2 and Nonce\_1 received in the DIRECT LINK ESTABLISHMENT REQUEST message as specified in 3GPP TS 33.536 [20];

c) derive the NR PC5 encryption key NRPEK and the NR PC5 integrity key NRPIK from KNRP-sess and the selected security algorithms as specified in 3GPP TS 33.536 [20], and

d) create a DIRECT LINK SECURITY MODE COMMAND message. In this message, the initiating UE:

1) shall include the Key establishment information container if a new KNRP has been derived at the initiating UE and the authentication method used to generate KNRP requires sending information to complete the authentication procedure;

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

2) shall include the MSBs of KNRP ID if a new KNRP has been derived at the initiating UE;

3) shall include a Nonce\_2 set to the 128-bit nonce value generated by the initiating UE for the purpose of session key establishment over this PC5 unicast link if the selected integrity protection algorithms is not the null integrity protection algorithm;

4) shall include the selected security algorithms;

5) shall include the UE security capabilities received from the target UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message;

6) shall include the UE PC5 unicast signalling security policy received from the target UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message;

7) shall include the 8 LSBs of KNPR-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] if the selected integrity protection algorithms is not the null integrity protection algorithm.

The initiating UE shall form the KNPR-sess ID from the 8 MSBs of KNPR-sess ID received in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNPR-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message.

The initiating UE shall not cipher the DIRECT LINK SECURITY MODE COMMAND message but shall integrity protect it with the new security context.

After the DIRECT LINK SECURITY MODE COMMAND 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 T5007. The UE shall not send a new DIRECT LINK SECURITY MODE COMMAND message to the same target UE while timer T5007 is running. The initiating UE shall provide lower layer with NRPIK, NRPEK if applicable, KNRP-sess ID, and the selected security algorithm as specified in TS 33.536 [20].



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

##### 6.1.2.7.3 PC5 unicast link security mode control procedure accepted by the target UE

Upon receipt of a DIRECT LINK SECURITY MODE COMMAND message, if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, the target UE shall check that the 8 LSBs of KNPR-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message are not set to the same value as those received from another UE in response to the target UE’s DIRECT LINK ESTABLISHMENT REQUEST message.

Then the target UE shall:

a) derive KNRP-sess from KNRP, Nonce\_1 and Nonce\_2 received in the DIRECT LINK SECURITY MODE COMMAND message as specified in 3GPP TS 33.536 [20]; and

b) derive NRPEK and NRPIK from KNRP-sess and the selected security algorithms as specified in 3GPP TS 33.536 [20].

The target UE shall determine whether or not the DIRECT LINK SECURITY MODE COMMAND message can be accepted by:

a) checking the integrity of the DIRECT LINK SECURITY MODE COMMAND message using NRPIK;

b) checking that the received UE security capabilities have not been altered compared to the values that the target UE sent to the initiating UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message;

c) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure,

1) checking that the received UE PC5 unicast signalling security policy has not been altered compared to the values that the target UE sent to the initiating UE in the DIRECT LINK ESTABLISHMENT REQUEST message; and

2) checking that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message do not include the null integrity protection algorithm if the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required"; and

d) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure and the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm, checking that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message do not include the null integrity protection algorithm.

If the target UE did not include a KNRP ID in the DIRECT LINK ESTABLISHMENT REQUEST message, the target UE included a Re-authentication indication in the DIRECT LINK REKEYING REQUEST message or the initiating UE has chosen to derive a new KNRP, the target UE shall derive KNRP as specified in 3GPP TS 33.536 [20]. The target UE shall choose the 16 LSBs of KNRP ID to ensure that the resultant KNRP ID will be unique in the target UE. The target UE shall form KNRP ID from the received MSBs of KNRP ID and its chosen LSBs of KNRP ID and shall store the complete KNRP ID with KNRP.

If the target UE accepts the DIRECT LINK SECURITY MODE COMMAND message, the target UE shall create a DIRECT LINK SECURITY MODE COMPLETE message. In this message, the target UE:

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

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

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;

c) if IP communication is used and the IP address configuration IE is set to "IPv6 address allocation not supported", shall include a link local IPv6 address IE formed locally based on IETF RFC 4862 [6];

d) if a new KNRP was derived, shall include the 16 LSBs of KNRP ID; and

e) if the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, shall include its UE PC5 unicast user plane security policy for this PC5 unicast link.

The target UE shall form the KNPR-sess ID from the 8 MSBs of KNPR-sess ID it had sent in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNPR-sess ID received in the DIRECT LINK SECURITY MODE COMMAND message.

The target UE shall cipher and integrity protect the DIRECT LINK SECURITY MODE COMPLETE message with the new security context.

After the DIRECT LINK SECURITY MODE COMPLETE 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. The target UE shall provide lower layer with NRPIK, NRPEK if applicable, KNRP-sess ID, and the selected security algorithm as specified in TS 33.536 [20].\*\*\*\*\* End of change \*\*\*\*\*