**3GPP TSG-CT WG1 Meeting #126-eC1-206xxx was C1-206200**

**Electronic meeting, 15-23 October 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0131** | **rev** | **1** | **Current version:** | **16.2.1** |  |
|  | | | | | | | | |
| *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:*** | Target UE’s layer-2 ID replacement during PC5 unicast link establishment procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-09-24 |
|  |  | | | |  | |  | | |  |
| ***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 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | During PC5 unicast link establishment procedure, the initial UE transmits the DIRECT LINK ESTABLISHMENT REQUEST message with the initiating UE’s layer-2 ID and the destination layer-2 ID used for unicast initial sigaling. The destination layer-2 ID is specified in TS 24.587 v16.2.0, which is as follows:  “d) *the link layer identifier for the unicast initial signaling (i.e. destination layer-2 ID used for unicast initial signaling) is available to the initiating UE (e.g. pre-configured, obtained as specified in clause 5.2.3 or known via prior V2X communication);*  *NOTE: In the case where different V2X services are mapped to distinct default destination layer-2 IDs, when the initiating UE intends to establish a single unicast link that can be used for more than one V2X service types, the UE can select any of the default destination layer-2 ID for unicast initial signalling.”*  After the target UE accepts the DIRECT LINK ESTABLISHMENT REQUEST message, the target UE will generate a new target UE’s layer-2 ID to replace the origial target UE’s layer-2 ID as we see in TS in TS 24.587 v16.2.0:  *“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. ”*  But the current TS 24.587 v16.2.1 did not specify how to replace the original target UE’s layer-2 ID with the new assigned layer-2 ID. The new assigned target UE’s layer-2 ID is generated after the target UE accepts the PC5 unicast link establishment message. But at this moment, if target UE use the assigned target UE’s layer-2 ID and source layer-2 ID as the link identifier to transmit DIRECT LINK ESTABLISHMENT ACCEPT message, the initiating UE will be ignorant of the new assigned layer-2 ID. So the target UE should use the original target UE’s layer-2 ID and source layer-2 ID as the link identifier to transmit DIRECT LINK ESTABLISHMENT ACCEPT message. At the same time, the DIRECT LINK ESTABLISHMENT ACCEPT message should include the new assigned target UE’s layer-2 ID to implement the replacement of the original target UE’s layer-2 ID with new assiged target UE’s layer-2 ID at the initiating UE.  Seemingly, all above analysis is reasonable until now. But it should be undermined that initiating target UE’s layer-2 ID is default. Multiple target UE may respond the request with security mode command(as figure 5.3.3.1.2.3-1, TS 33.535 16.1.0 described) and following PC5 unicast link accept message. If target UE does not change the default target UE’ layer-2 ID immediately, initiating UE’s layer-2 ID will be confused about multiple target UE’s response message. For example, there are multiple response message with initiating UE layer-2 ID, default target UE layer-2 ID, security information. So it is proposed that the target UE should generate the new targe UE’s layer-2 ID after receiving and getting interested in the request message. Then the target UE should include the new assigned target UE’s layer-2 ID in the message to initiating as soon as possible.  So it is proposed to include the new assigned target UE’s layer-2 ID in DIRECT LINK SECURITY MODE COMMAND message. But if PC5 unicast link authentication procedure precedes PC5 unicast link security mode control procedure, the new assigned target UE’s layer-2 ID should be preferentially included in DIRECT LINK AUTHENTICATION REQUEST message.  After receiving the message involving new assigned target UE’s layer-2 ID at the lower layer of the initiating UE, the initiating UE should forward the  message with the origial target UE’s layer-2 ID and source layer-2 ID. The initiating UE will store the new assigned target UE’s layer-2 ID and source layer-2 ID and send the response message with the new assigned target UE’s layer-2 ID and source layer-2 ID.  And in TS 23.287, it is also stated that target UE’s layer-2 ID should be included in received security establishment procedure message.  *“……*  *4b. If the Target User Info is not included in the Direct Communication Request message, the UEs that are interested in using the announced V2X service type(s) over a PC5 unicast link with UE-1 responds by establishing the security with UE-1.*  *NOTE 2: The signalling for the Security Procedure is defined in TS 33.536 [26].*  *When the security protection is enabled, UE-1 sends the following information to the target UE:*  *- If IP communication is used:*  *- IP Address Configuration: For IP communication, IP address configuration is required for this link and indicates one of the following values:*  *- "IPv6 Router" if IPv6 address allocation mechanism is supported by the initiating UE, i.e., acting as an IPv6 Router; or*  *- "IPv6 address allocation not supported" if IPv6 address allocation mechanism is not supported by the initiating UE.*  *- Link Local IPv6 Address: a link-local IPv6 address formed locally based on RFC 4862 [21] if UE-1 does not support the IPv6 IP address allocation mechanism, i.e. the IP Address Configuration indicates "IPv6 address allocation not supported".*  *- QoS Info: the information about PC5 QoS Flow(s) to be added. For each PC5 QoS Flow, the PFI, the corresponding PC5 QoS parameters (i.e. PQI and conditionally other parameters such as MFBR/GFBR, etc.) and the associated V2X service type(s).*  *The source Layer-2 ID used for the security establishment procedure is determined as specified in clauses 5.6.1.1 and 5.6.1.4. The destination Layer-2 ID is set to the source Layer-2 ID of the received Direct Communication Request message.*  *Upon receiving the security establishment procedure messages, UE-1 obtains the peer UE's Layer-2 ID for future communication, for signalling and data traffic for this unicast link.*  *……”* | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. The target UE will replace the original targe UE’s layer-2 ID with the new assigned target UE’s layer-2 ID if necessary, which should be included in the DIRECT LINK AUTHENTICATION REQUEST message(if available) or DIRECT LINK SECURITY MODE COMMAND message. 2. Target UE’s layer-2 ID should replace the original target UE’s layer-2 ID with new assigned target UE’s layer-2 ID if available and initiate to transfer the message to peer with the new target UE’s layer-2 ID. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Missing the target UE’s layer-2 ID replacement during PC5 unicast link establishment procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.2.3, 6.1.2.6.2, 6.1.2.6.3, 6.1.2.7.2, 6.1.2.7.3, 7.3.10.1, 7.3.10.x, 7.3.13.1, 7.3.10.y | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\* 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 assign a layer-2 ID for this PC5 unicast link, may initiate PC5 unicast link authentication procedure as specified in clause 6.1.2.6 and shall initiate PC5 unicast link security mode control procedure as specified in clause 6.1.2.7. After successfully finishing PC5 unicast link authentication procedure if necessary and PC5 unicast link security mode control procedure, the target UE shall uniquely assign a PC5 link identifier, create a PC5 unicast link context 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.

NOTE: The target UE may reuse the target UE’s layer-2 ID used in the transport of the DIRECT LINK ESTABLISHMENT REQUEST message provided by the lower layers in case that the target UE’s layer-2 ID has been used in previous PC5 unicast link with the same peer.

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 clause 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 PQFI(s), the corresponding PC5 QoS parameters and the V2X service identifier(s) that the target UE accepts;

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, NRPIK, NRPEK if applicable, KNRP-sess ID, and the selected security algorithm as specified in TS 33.536 [20], and shall start timer T5011 if the target UE has the privacy configuration as specified in clause 5.2.3.

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) an indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link, if applicable; and

e) an 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 \*\*\*\*\*

##### 6.1.2.6.2 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; and

x) shall include the new assigned initiating UE’s layer-2 ID if the initiating UE assigns a new initiating UE’s layer-2 ID in case that the PC5 unicast link authentication procedure is triggered by a PC5 unicast link establishment procedure.

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.

NOTEx: The initiating UE’s layer-2 ID is the original initiating UE’s layer-2 ID which was the target UE’s layer-2 ID used in the transport of DIRECT LINK ESTABLISHMENT REQUEST message if the initiating UE assigns a new initiating UE’s layer-2 ID in case that the PC5 unicast link authentication procedure is triggered by a PC5 unicast link establishment procedure.

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

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

##### 6.1.2.6.3 PC5 unicast link authentication procedure accepted by the target UE

Upon receipt of a DIRECT LINK AUTHENTICATION REQUEST message, if the 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 DIRECT LINK AUTHENTICATION REQUEST message can be accepted, the target UE shall create a DIRECT LINK AUTHENTICATION RESPONSE message. 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 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.

\*\*\*\*\* Fourth 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:

i) 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

ii) has decided not to activate security protection based on its UE PC5 unicast signalling security policy and the target UE’s PC5 unicast signalling security policy; 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:

a) 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;

b) shall not select the null ciphering protection algorithm if the ciphering protection algorithm currently in use for the PC5 unicast link is different from the null ciphering protection algorithm;

c) shall select the null integrity protection algorithm if the integrity protection algorithm currently in use is the null integrity protection algorithm; and

d) shall select the null ciphering protection algorithm if the ciphering protection algorithm currently in use is the null ciphering 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 IE 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 IE if a new KNRP has been derived at the initiating UE;

3) shall include a Nonce\_2 IE 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 KNRP-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; and

y) shall include the new assigned initiating UE’s layer-2 ID if the initiating UE assigns a new initiating UE’s layer-2 ID in case that the PC5 unicast link security mode control procedure is triggered by a PC5 unicast link establishment procedure and the PC5 unicast link authentication procedure is not executed.

If the security protection of this PC5 unicast link is activated, the initiating UE shall form the KNRP-sess ID from the 8 MSBs of KNRP-sess ID received in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNRP-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message.

If the security protection of this PC5 unicast link is activated, 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.

NOTEx: The initiating UE’s layer-2 ID for unicast communication is the original initiating UE’s layer-2 ID which was the target UE’s layer-2 ID used in the transport of DIRECT LINK ESTABLISHMENT REQUEST message if the initiating UE assigns a new initiating UE’s layer-2 ID in case that the PC5 unicast link security mode control procedure is triggered by a PC5 unicast link establishment procedure and the PC5 unicast link authentication procedure is not executed.



Figure 6.1.2.7.2: PC5 unicast link security mode control procedure

\*\*\*\*\* Fifth 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 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. The target UE shall check the selected security algorithms IE included in the DIRECT LINK SECURITY MODE COMMAND message. If "null integrity algorithm" is included in the selected security algorithms IE, the security of this PC5 unicast link is not activated. If "null ciphering algorithm" and an integrity algorithm other than "null integrity algorithm" are included in the selected algorithms IE, the signalling ciphering protection is not activated. If the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required", the target UE shall check the selected security algorithms IE in the DIRECT LINK SECURITY MODE COMMAND message does not include the null integrity protection algorithm. If the an integrity algorithm other than "null integrity algorithm" is included in the selected security algorithms IE.If the selected integrity protection algorithm is not the null integrity protection algorithm, 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 NRPIK from KNRP-sess and the selected integrity algorithm as specified in 3GPP TS 33.536 [20].

If the KNRP-sess is derived and the selected ciphering protection algorithm is not the null integrityciphering protection algorithm, then the target UE shall derive NRPEK from KNRP-sess and the selected ciphering algorithm 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 that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message only include the null integrity protection algorithm if the target UE’s PC5 unicast signalling integrity protection policy is set to "signalling integrity protection not needed" or "signalling integrity protection notor preferred"; and

b) checking the integrity of the DIRECT LINK SECURITY MODE COMMAND message using NRPIK, if the selected integrity protection algorithm is not the null integrity protection algorithm;

c) 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;

d) 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 8 LSBs of KNRP-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; and

e) 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. In the case where the different V2X services are mapped to the different PC5 unicast user plane security policies, when more than one V2X service identifier is included in the DIRECT LINK ESTABLISHMENT REQUEST message, each of the user plane security polices of those V2X services shall be compatible, e.g. "user plane integrity protection not needed" and " user plane integrity protection required" are not compatible.

If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall form the KNRP-sess ID from the 8 MSBs of KNRP-sess ID it had sent in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNRP-sess ID received in the DIRECT LINK SECURITY MODE COMMAND message.

If the selected integrity protection algorithm is not the null integrity protection algorithm, the target UE shall integrity protect the DIRECT LINK SECURITY MODE COMPLETE message with the new security context. If the selected ciphering protection algorithm is not the null ciphering protection algorithm, the target UE shall cipher 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, NRPIK, NRPEK if applicable, KNRP-sess ID, and the selected security algorithm as specified in TS 33.536 [20].

\*\*\*\*\* Sixth change \*\*\*\*\*

#### 7.3.10.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link authentication procedure is initiated. See table 7.3.10.1.1.

Message type: DIRECT LINK AUTHENTICATION REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.10.1.1: DIRECT LINK AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK AUTHENTICATION REQUEST 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 | M | LV-E | 3-n |
| xx | Source layer-2 ID | Layer-2 ID  8.4.25 | O | TV | 4 |

\*\*\*\*\* Seventh change \*\*\*\*\*

#### 7.3.10.x Source layer-2 ID

The IE is included if the UE assigns a new UE’s layer-2 ID in case that the PC5 unicast link authentication procedure of the UE is triggered by a PC5 unicast link establishment procedure

\*\*\*\*\* Eighth change \*\*\*\*\*

#### 7.3.13.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link security mode control procedure is initiated. See table 7.3.13.1.1.

Message type: DIRECT LINK SECURITY MODE COMMAND

Significance: dual

Direction: UE to peer UE

Table 7.3.13.1.1: DIRECT LINK SECURITY MODE COMMAND message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK SECURITY MODE COMMAND message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | Selected security algorithms | Selected security algorithms  8.4.18 | M | V | 1 |
|  | UE security capabilities | UE security capabilities  8.4.14 | M | LV | 3-9 |
|  | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy  8.4.15 | M | V | 1 |
| 55 | Nonce\_2 | Nonce  8.4.13 | O | TV | 17 |
| 52 | LSBs of KNRP-sess ID | LSBs of KNRP-sess ID  8.4.19 | O | TV | 2 |
| 74 | Key establishment information container | Key establishment information container  8.4.12 | O | TLV-E | 4-n |
| 62 | MSBs of KNRP ID | MSBs of KNRP ID  8.4.20 | O | TV | 3 |
| xx | Source layer-2 ID | Layer-2 ID  8.4.25 | O | TV | 4 |

\*\*\*\*\* Ninth change \*\*\*\*\*

#### 7.3.13.y Source layer-2 ID

The IE is included if the UE assigns a new UE’s layer-2 ID in case that the PC5 unicast link security mode control procedure of the UE is triggered by a PC5 unicast link establishment procedure and the PC5 unicast link authentication procedure is not executed.

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