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

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.587** | **CR** | **0230** | **rev** | **1** | **Current version:** | **17.4.1** |  |
|  |
| *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:***  | Harmonizing the terminologies of LSB of KNRP-sess ID and MSB of KNRP-sess ID |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | TEI17, eV2XARC |  | ***Date:*** | 2022-01-28 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-17 |
|  | *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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Both the terminologies "LSBs of KNRP-sess ID" and "LSB of KNRP-sess ID" are used in the spec to refer to the same thing, which is the 8 least significant bits of the KNRP-sess ID.Actually "LSB of KNRP-sess ID" is the correct terminology, because LSB is defined as following:LSB Least Significant 8 BitsHence no need to use the plural term (LSBs).So the terminology "LSB of KNRP-sess ID" is the correct one that shall be used across the spec.Also the terminology "8 LSBs of KNRP-sess ID" is not correct, because LSB itself stands for the 8 least significant bits. Hence the "8" should be removed.The same issues above exist for "MSBs of KNRP-sess ID" and "MSB of KNRP-sess ID". |
|  |  |
| ***Summary of change:*** | Correcting the terminology "MSBs of KNRP-sess ID" and "8 MSBs of KNRP-sess ID" to be "MSB of KNRP-sess ID".Correcting the terminology "LSBs of KNRP-sess ID" and "8 LSBs of KNRP-sess ID" to be "LSB of KNRP-sess ID".Also the "16 MSBs of KNRP ID" and "16 LSBs of KNRP ID" are changed to "2 MSBs of KNRP ID" and "2 LSBs of KNRP ID" respectively. |
|  |  |
| ***Consequences if not approved:*** | Inconsistent terminologies stay in the spec, which causes confusion about how many Bits are meant. |
|  |  |
| ***Clauses affected:*** | 6.1.2.2.2, 6.1.2.7.2, 6.1.2.7.3, 6.1.2.7.5, 6.1.2.10.2, 7.3.1.1, 7.3.1.5, 7.3.13.1, 7.3.13.3, 7.3.16.1, 7.3.16.4, 8.4.9, 8.4.16, 8.4.19 |
|  |  |
|  | **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 \*\*\*\*\*

##### 6.1.2.2.2 PC5 unicast link establishment procedure initiation by initiating UE

The initiating UE shall meet the following pre-conditions before initiating this procedure:

a) a request from upper layers to transmit the packet for V2X service over PC5;

b) the communication mode is unicast mode (e.g. pre-configured as specified in clause 5.2.3 or indicated by upper layers);

c) the link layer identifier for the initiating UE (i.e. layer-2 ID used for unicast communication) is available (e.g. pre-configured or self-assigned) and is not being used by other existing PC5 unicast links to the same link layer identifier for the destination UE within the initiating UE;

d) the link layer identifier for the destination UE (i.e. the unicast layer-2 ID of the target UE or the broadcast layer-2 ID) 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 1: 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 identifiers, the UE can select any of the default destination layer-2 ID for unicast initial signalling.

e) the initiating UE is either authorised for V2X communication over PC5 in NR-PC5 in the serving PLMN, or has a valid authorization for V2X communication over PC5 in NR-PC5 when not served by E-UTRA and not served by NR. The UE considers that it is not served by E-UTRA and not served by NR if the following conditions are met:

1) not served by NR and not served by E-UTRA for V2X communication over PC5;

2) in limited service state as specified in 3GPP TS 23.122 [2], if the reason for the UE being in limited service state is one of the following;

i) the UE is unable to find a suitable cell in the selected PLMN as specified in 3GPP TS 38.304 [9];

ii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #11 "PLMN not allowed" as specified in 3GPP TS 24.501 [6]; or

iii) the UE received a REGISTRATION REJECT message or a SERVICE REJECT message with the 5GMM cause #7 "5GS services not allowed" as specified in 3GPP TS 24.501 [6]; or

3) in limited service state as specified in 3GPP TS 23.122 [2] for reasons other than i), ii) or iii) above, and located in a geographical area for which the UE is provisioned with "non-operator managed" radio parameters as specified in clause 5.2.3;

f) there is no existing PC5 unicast link for the pair of peer application layer IDs, or there is an existing PC5 unicast link for the pair of peer application layer IDs and:

1) the network layer protocol of the existing PC5 unicast link is not identical to the network layer protocol required by the upper layer in the initiating UE for this V2X service; or

2) the security policy (either signalling security policy or user plane security policy) corresponding to the V2X service identifier is not compatible with the security policy of the existing PC5 unicast link; and

g) 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.

After receiving the service data or request from the upper layers, the initiating UE shall derive the PC5 QoS parameters and assign the PQFI(s) for the PC5 QoS flows(s) to be established as specified in clause 6.1.2.12.

In order to initiate the PC5 unicast link establishment procedure, the initiating UE shall create a DIRECT LINK ESTABLISHMENT REQUEST message. The initiating UE:

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

b) shall include the V2X service identifier(s) received from upper layer;

c) shall include the target user info set to the target UE's application layer ID if received from upper layers or if the destination layer-2 ID is the unicast layer-2 ID of target UE;

d) shall include the Key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required" or "signalling integrity protection preferred", and may include the Key establishment information container if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection not needed";

NOTE 2: The Key establishment information container is provided by upper layers.

e) shall include a Nonce\_1 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 UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required" or "signalling integrity protection preferred";

f) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the security establishment of this PC5 unicast link;

g) shall include the MSB of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] if the UE PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required" or "signalling integrity protection preferred";

h) may include a KNRP ID if the initiating UE has an existing KNRP for the target UE; and

i) shall include its UE PC5 unicast signalling security policy. In the case where the different V2X services are mapped to the different PC5 unicast signalling security policies, when the initiating UE intends to establish a single unicast link that can be used for more than one V2X service, each of the signalling security polices of those V2X services shall be compatible, e.g. "signalling integrity protection not needed" and "signalling integrity protection required" are not compatible.

After the DIRECT LINK ESTABLISHMENT 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 destination layer-2 ID used for unicast initial signalling, and start timer T5000. The UE shall not send a new DIRECT LINK ESTABLISHMENT REQUEST message to the same target UE identified by the same application layer ID while timer T5000 is running. If the target user info IE is not included in the DIRECT LINK ESTABLISHMENT REQUEST message (i.e. V2X service oriented PC5 unicast link establishment procedure), the initiating UE shall handle multiple DIRECT LINK ESTABLISHMENT ACCEPT messages, if any, received from different target UEs for the establishment of multiple PC5 unicast links before the expiry of timer T5000.

NOTE 3: In order to ensure successful PC5 unicast link establishment, T5000 should be set to a value larger than the sum of T5006 and T5007.



Figure 6.1.2.2.2: UE oriented PC5 unicast link establishment procedure

Initiating UE

Target UEs

Start T5000

DIRECT LINK ESTABLISHMENT REQUEST

DIRECT LINK ESTABLISHMENT ACCEPT

T5000 expires

DIRECT LINK ESTABLISHMENT ACCEPT

Figure 6.1.2.2.3: V2X service oriented PC5 unicast link establishment procedure

\*\*\*\*\* Next 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 2 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; and

7) shall include the LSB 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.

If the security protection of this PC5 unicast link is activated, the initiating UE shall form the KNRP-sess ID from the MSB of KNRP-sess ID received in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the LSB of KNRP-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message. The initiating UE shall use the KNRP-sess ID to identify 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, NRPIK, NRPEK if applicable, KNRP-sess ID, the selected security algorithm as specified in TS 33.536 [20]; an indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link with the new security context, if applicable, and start timer T5007. The initiating UE shall not send a new DIRECT LINK SECURITY MODE COMMAND message to the same target UE while timer T5007 is running.

NOTE: The DIRECT LINK SECURITY MODE COMMAND message is integrity protected (and not ciphered) at the lower layer using the new security context.

If the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure, the initiating UE shall provide to the lower layers an indication of activation of the PC5 unicast user plane security protection for the PC5 unicast link with the new security context, if applicable, along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication.



Figure 6.1.2.7.2: PC5 unicast link security mode control procedure

\*\*\*\*\* Next 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 a new assigned initiating UE's layer-2 ID is included and if the authentication procedure has not been executed, 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 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 ciphering 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 does 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";

b) asking the lower layers to check the integrity of the DIRECT LINK SECURITY MODE COMMAND message using NRPIK and the selected integrity protection algorithm, 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 LSB 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 2 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 and the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, 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, the IP address configuration IE is set to "IPv6 address allocation not supported" and the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, 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 2 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 MSB of KNRP-sess ID it had sent in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the LSB of KNRP-sess ID received in the DIRECT LINK SECURITY MODE COMMAND message. The target UE shall use the KNRP-sess ID to identify 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, the selected security algorithm as specified in 3GPP TS 33.536 [20] , and an indication of activation of the PC5 unicast signalling security protection for the PC5 unicast link with the new security context, if applicable.

NOTE: The DIRECT LINK SECURITY MODE COMPLETE message and further PC5 unicast signalling messages are integrity protected and ciphered (if applicable) at the lower layer using the new security context.

If the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure, the target UE shall provide to the lower layers an indication of activation of the PC5 unicast user plane security protection for the PC5 unicast link with the new security context, if applicable, along with the initiating UE's layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication.

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

##### 6.1.2.7.5 PC5 unicast link security mode control procedure not accepted by the target UE

If the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted, the target UE shall send a DIRECT LINK SECURITY MODE REJECT message, and the target UE shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure unless the ongoing procedure is a PC5 unicast link establishment procedure and the Target user info is not included in the DIRECT LINK ESTABLISHMENT REQUEST message. The DIRECT LINK SECURITY MODE REJECT message contains a PC5 signalling protocol cause IE indicating one of the following cause values:

#7: integrity failure;

#8: UE security capabilities mismatch;

#9: LSB of KNRP-sess ID conflict;

#10: UE PC5 unicast signalling security policy mismatch;

#11 lack of resources for PC5 unicast link; or

#111: protocol error, unspecified.

If this PC5 unicast link security mode control procedure is triggered during the PC5 unicast 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 SECURITY MODE REJECT message containing PC5 signalling protocol cause value #5 "lack of resources for PC5 unicast link".

If the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted because the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, that the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message included the null integrity protection algorithm and the target UE's PC5 unicast signalling integrity protection policy is set to "signalling integrity protection required", the target UE shall include PC5 signalling protocol cause #10 "UE PC5 unicast signalling security policy mismatch" in the DIRECT LINK SECURITY MODE REJECT message.

If the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted because the PC5 unicast link security mode control procedure was triggered during a PC5 unicast link re-keying procedure, the integrity protection algorithm currently in use for the PC5 unicast link is different from the null integrity protection algorithm and the selected security algorithms in the DIRECT LINK SECURITY MODE COMMAND message include the null integrity protection algorithm, the target UE, the target UE shall include PC5 signalling protocol cause #10 "UE PC5 unicast signalling security policy mismatch" in the DIRECT LINK SECURITY MODE REJECT message.

If the target UE detects that the received UE security capabilities IE in the DIRECT LINK SECURITY MODE COMMAND message has been altered compared to the latest values that the target UE sent to the initiating UE in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message, the target UE shall include PC5 signalling protocol cause #8 "UE security capabilities mismatch" in the DIRECT LINK SECURITY MODE REJECT message.

If the target UE detects that the LSB of KNRP-sess ID included in the DIRECT LINK SECURITY MODE COMMAND message are set to the same value as those received from another UE in response to the target UE's DIRECT LINK ESTABLISHMENT REQUEST message, the target UE shall include PC5 signalling protocol cause #9 "LSB of KNRP-sess ID conflict" in the DIRECT LINK SECURITY MODE REJECT message.

After the DIRECT LINK SECURITY MODE 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.

Upon receipt of the DIRECT LINK SECURITY MODE REJECT message, the initiating UE shall stop timer T5007, provide an indication to the lower layer of deactivation of the PC5 unicast security protection and deletion of security context for the PC5 unicast link, if applicable and:

a) if the PC5 signalling protocol cause IE in the DIRECT LINK SECURITY MODE REJECT message is set to #9 "LSB of KNRP-sess ID conflict", retransmit the DIRECT LINK SECURITY MODE COMMAND message with a different value for the LSB of KNRP-sess ID and restart timer T5007; or

b) if the PC5 signalling protocol cause IE is set to the value other than #9 "LSB of KNRP-sess ID conflict", abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure.

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

##### 6.1.2.10.2 PC5 unicast link re-keying procedure initiation by the initiating UE

The initiating UE shall meet the following pre-condition before initiating the PC5 unicast link re-keying procedure:

a) there is a PC5 unicast link between the initiating UE and the target UE; and

1) if the session key KNRP-sess used to protect PC5 unicast link needs to be refreshed and neither timer T5007 nor T5008 are running;

2) if the UE wants to refresh KNRP and neither timer T5007 nor T5008 are running; or

3) if the lower layers indicate that a PC5 unicast link re-keying procedure needs to be performed.

In order to initiate the PC5 unicast link re-keying procedure, the initiating UE shall create a DIRECT LINK REKEYING REQUEST message. In this message, the initiating UE:

a) shall include the Key establishment information container IE if the null integrity protection algorithm is not in use;

NOTE 1: The key establishment information container is provided by upper layers.

b) shall include a Nonce\_1 IE set to the 128-bit nonce value generated by the initiating UE for the purpose of session key refresh over this PC5 unicast link if the null integrity protection algorithm is not in use;

c) shall include its UE security capabilities indicating the list of algorithms that the initiating UE supports for the re-keying of this PC5 unicast link;

d) shall include the MSB of KNRP-sess ID chosen by the initiating UE as specified in 3GPP TS 33.536 [20] if the null integrity protection algorithm is not in use; and

e) may include a Re-authentication indication if the initiating UE wants to derive a new KNRP.

After the DIRECT LINK REKEYING 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, and start timer T5008. The UE shall not send a new DIRECT LINK REKEYING REQUEST message to the same target UE while timer T5008 is running.

NOTE 2: In order to ensure successful PC5 unicast link re-keying, T5008 should be set to a value larger than the sum of T5006 and T5007.



Figure 6.1.2.10.2: PC5 unicast link re-keying procedure

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

#### 7.3.1.1 Message definition

This message is sent by a UE to another peer UE to establish a direct link. See table 7.3.1.1.1.

Message type: DIRECT LINK ESTABLISHMENT REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.1.1.1: DIRECT LINK ESTABLISHMENT REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK ESTABLISHMENT REQUEST message identity | PC5 signalling message type8.4.1 | M | V | 1 |
|  | Sequence number | Sequence number8.4.2 | M | V | 1 |
|  | V2X service identifiers | V2X service identifier8.4.3 | M | LV | 5-253 |
|  | Source user info | Application layer ID8.4.4 | M | LV | 3-253 |
|  | UE security capabilities | UE security capabilities8.4.14 | M | LV | 3-9 |
|  | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy8.4.15 | M | V | 1 |
| 74 | Key establishment information container | Key establishment information container8.4.12 | O | TLV-E | 4-n |
| 53 | Nonce\_1 | Nonce8.4.13 | O | TV | 17 |
| 54 | MSB of KNRP-sess ID | MSB of KNRP-sess ID8.4.16 | O | TV | 2 |
| 28 | Target user info | Application layer ID8.4.4 | O | TLV | 4-254 |
| 52 | KNRP ID | KNRP ID8.4.17 | O | TV | 5 |

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

#### 7.3.1.5 MSB of KNRP-sess ID

The UE shall include this IE if the UE PC5 unicast signalling security policy is set to "signalling integrity protection required" or "signalling integrity protection preferred".

\*\*\*\*\* Next 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 type8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number8.4.2 | M | V | 1 |
|  | Selected security algorithms | Selected security algorithms8.4.18 | M | V | 1 |
|  | UE security capabilities | UE security capabilities8.4.14 | M | LV | 3-9 |
| 59 | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy8.4.15 | O | TV | 2 |
| 55 | Nonce\_2 | Nonce8.4.13 | O | TV | 17 |
| 52 | LSB of KNRP-sess ID | LSB of KNRP-sess ID8.4.19 | O | TV | 2 |
| 74 | Key establishment information container | Key establishment information container8.4.12 | O | TLV-E | 4-n |
| 62 | MSBs of KNRP ID | MSBs of KNRP ID8.4.20 | O | TV | 3 |

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

#### 7.3.13.3 LSB of KNRP-sess ID

The UE shall include this IE if the selected integrity protection algorithms is not the null integrity protection algorithm.

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

#### 7.3.16.1 Message definition

This message is sent by a UE to another peer UE when a PC5 unicast link re-keying procedure is initiated. See table 7.3.16.1.1.

Message type: DIRECT LINK REKEYING REQUEST

Significance: dual

Direction: UE to peer UE

Table 7.3.16.1.1: DIRECT LINK REKEYING REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK REKEYING REQUEST message identity | PC5 signalling message type8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number8.4.2 | M | V | 1 |
|  | UE security capabilities | UE security capabilities8.4.14 | M | LV | 3-9 |
| 74 | Key establishment information container | Key establishment information container8.4.12 | O | TLV-E | 4-n |
| 53 | Nonce\_1 | Nonce8.4.13 | O | TV | 17 |
| 54 | MSB of KNRP-sess ID | MSB of KNRP-sess ID8.4.16 | O | TV | 2 |
| 56 | Re-authentication indication | Re-authentication indication8.4.24 | O | TV | 2 |

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

#### 7.3.16.4 MSB of KNRP-sess ID

The UE shall include this IE if the null integrity protection algorithm is not in use.

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

### 8.4.9 PC5 signalling protocol cause

The purpose of the PC5 signalling protocol cause information element is to indicate the cause used in the PC5 signalling protocol procedures.

The PC5 signalling protocol cause is a type 3 information element with a length of 2 octets.

The PC5 signalling protocol cause information element is coded as shown in figure 8.4.9.1 and table 8.4.9.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| PC5 signalling protocol cause IEI | octet 1 |
| PC5 signalling cause value | octet 2 |

Figure 8.4.9.1: PC5 signalling protocol cause information element

Table 8.4.9.1: PC5 signalling protocol cause information element

|  |
| --- |
| PC5 signalling cause value (octet 2) |
|  |
| Bits |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |  |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |  | Direct communication to the target UE not allowed |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |  | Direct communication to the target UE no longer needed |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |  | Conflict of layer-2 ID for unicast communication is detected |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |  | Direct connection is not available anymore |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 |  | Lack of resources for PC5 unicast link |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |  | Authentication failure |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 |  | Integrity failure |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |  | UE security capabilities mismatch |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |  | LSB of KNRP-sess ID conflict |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |  | UE PC5 unicast signalling security policy mismatch |
| 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 |  | Required service not allowed |
| 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |  | Security policy not aligned |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |  | Protocol error, unspecified |
|  |  |  |  |  |  |  |  |  |  |
| Any other value received by the UE shall be treated as 0110 1111, "protocol error, unspecified". |

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

### 8.4.16 MSB of KNRP-sess ID

The purpose of the MSB of KNRP-sess ID information element is to carry the 8 most significant bits of the KNRP-sess ID.

The MSB of KNRP-sess ID information element is a type 3 information element with a length of 2 octets.

The MSB of KNRP-sess ID information element is coded as shown in figure 8.4.16.1 and table 8.4.16.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MSB of KNRP-sess ID IEI | octet 1 |
| MSB of KNRP-sess ID contents | octet 2 |

Figure 8.4.16.1: MSB of KNRP-sess ID information element

Table 8.4.16.1: MSB of KNRP-sess ID information element

|  |
| --- |
| MSB of KNRP-sess ID contents (octet 2)This field contains the 8 most significant bits of KNRP-sess ID. |

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

### 8.4.19 LSB of KNRP-sess ID

The purpose of the LSB of KNRP-sess ID information element is to carry the 8 least significant bits of the KNRP-sess ID.

The LSB of KNRP-sess ID is a type 3 information element with a length of 2 octets.

The LSB of KNRP-sess ID information element is coded as shown in figure 8.4.19.1 and table 8.4.19.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| LSB of KNRP-sess ID | octet 1 |
| LSB of KNRP-sess ID contents | octet 2 |

Figure 8.4.19.1: LSB of KNRP-sess ID information element

Table 8.4.19.1: LSB of KNRP-sess ID information element

|  |
| --- |
| LSB of KNRP-sess ID contents (octet 2)This field contains the 8 least significant bits of KNRP-sess ID. |

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