**3GPP TSG-CT WG1 Meeting #126-eC1-20xxxx was C1-206203**

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0133** | **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:*** | UE PC5 unicast signalling security negotiation | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-09-27 |
|  |  | | | |  | |  | | |  |
| ***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) Rel-17 (Release 17)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 1. During PC5 unicast link establishment procedure, the initiating UE and target UE will negotiate with each other the UE PC5 unicast signaling security policy. As it is showed in TS 33.536 v16.1.0:  “……  3. UE\_2 shall send the Direct Security Mode Command message to UE\_1. This message shall only contain the MSB and of KNRP ID and optionally Key\_Est\_Info if a fresh KNRP is to be generated (see clause 5.3.3.1.3). UE\_2 shall include the Chosen\_algs parameter to indicate which security algorithms the UEs will use to protect the data in the message. The Chosen-algs may only indicate the use of the NULL integrity algorithm if UE\_2's signalling integrity security policy is either NOT NEEDED or PREFERRED. UE\_2 shall also return the UE\_1's security capabilities and UE\_1's signalling security policy to provide protection against bidding down attacks. In the case that the NULL integrity algorithm is chosen, the NULL confidentiality algorithm shall also be chosen and UE\_2 shall set the KNPR-sess ID of this security context to the all zero value.  ……  ”  2. During rekeying procedure, initiating UE’s security capabilities is included in Direct Re-keying Request message and the same initiating UE’s security capabilities should be included in Direct Security Mode Command message. But the initiating UE’s signalling security policy information is not included in both Direct Re-keying Request message and Direct Security Mode Command message because the signalling security policy negotiation has been finished in PC5 unicast link establishment process. As it is showed in TS 33.536 v16.0.0:  “……  1. UE\_1 sends a Direct Rekey Request to UE\_2. This message shall include UE\_1 security capabilities (the list of algorithms that UE\_1 will accept for this connection). In addition, if a non-Null integrity algorithm is in use, the message shall include Nonce\_1 (for session key generation) and the most significant 8-bits of the KNRP-sess ID. These bits are chosen such that UE\_1 will be able to locally identify a security context that is created by this procedure. The message may also include a Re-auth Flag if UE\_1 wants to rekey KNRP. The message also contains Key\_Est\_Info (see clause 5.3.3.1.3.2).  2. UE\_2 may initiate a Direct Auth Key Establish procedure with UE\_1. This is mandatory if UE\_1 included the Re-auth Flag and signalling is needed to establish KNRP.  3. This step is the same as step 3 in clause 5.3.3.1.4.3 except that the chosen integrity algorithm shall only be NULL if and only if the NULL integrity algorithm is currently in use, the chosen confidentiality algorithm shall only be NULL if and only if the NULL confidentiality algorithm is currently in use and UE\_1's signalling security policy is not included in this message.  ……”  But in current TS 24.587 v16.2.1, the PC5 unicast sigaling security policy is mandatory.  “ **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 |   ……” | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. Modify the “Presence” feature of UE security policy related IEs in PC5 unicast link security mode control messages and add a new subclause to specify the existence condition of PC5 unicast sigaling security policy. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 1. Incorrect “Presence” feature of UE PC5 signaling security policy IE in direct link security mode command message | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.7.2, 7.3.2.1, 7.3.13.1, 7.3.13.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 \*\*\*\*\*

##### 6.1.2.7.2 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; and

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.

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.



Figure 6.1.2.7.2: PC5 unicast link security mode control procedure

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

#### 7.3.2.1 Message definition

This message is sent by a UE to another peer UE to accept the received DIRECT LINK ESTABLISHMENT REQUEST message. See table 7.3.2.1.1.

Message type: DIRECT LINK ESTABLISHMENT ACCEPT

Significance: dual

Direction: UE to peer UE

Table 7.3.2.1.1: DIRECT LINK ESTABLISHMENT ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | DIRECT LINK ESTABLISHMENT ACCEPT message identity | PC5 signalling message type  8.4.1. | M | V | 1 |
|  | Sequence number | Sequence number  8.4.2 | M | V | 1 |
|  | Source user info | Application layer ID  8.4.4 | M | LV | 3-253 |
|  | QoS flow descriptions | PC5 QoS flow descriptions  8.4.5 | M | LV-E | 5-65537 |
|  | Configuration of UE PC5 unicast user plane security protection | Configuration of UE PC5 unicast user plane security protection  8.4.23 | M | V | 1 |
| 57 | IP address configuration | IP address configuration  8.4.6 | O | TV | 2 |
| 58 | Link local IPv6 address | Link local IPv6 address  8.4.7 | O | TV | 17 |

\*\*\*\*\* Third 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 |
| xx | UE PC5 unicast signalling security policy | UE PC5 unicast signalling security policy  8.4.15 | O | TV | 2 |
| 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 |

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

#### 7.3.13.y UE PC5 unicast signalling security policy

The UE shall include this IE if the DIRECT LINK SECURITY MODE COMMAND message is triggered by the DIRECT LINK ESTABLISHMENT REQUEST message. The content of the IE is the same as the content of UE PC5 unicast signalling security policy IE in the received DIRECT LINK ESTABLISHMENT REQUEST message in order to provide protection against bidding down attacks. \*\*\*\*\* End of change \*\*\*\*\*