**3GPP TSG-CT WG1 Meeting #127-eC1-207127**

**Electronic meeting, 13-20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0150** | **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:*** | Updates to the PC5 unicast link security mode control procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | vivo, OPPO, Nokia, Nokia Shanghai Bell | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-11-06 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | During the PC5 unicast link security mode control procedure, if the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted,   1. How the target UE sends the DIRECT LINK SECURITY MODE REJECT message is still missing. 2. When the PC5 signalling protocol cause IE in the DIRECT LINK SECURITY MODE REJECT message is not the “#d: LSBs of KNRP-sess ID conflict”, the behaviors of initiating UE are still missing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | During the PC5 unicast link security mode control procedure, if the DIRECT LINK SECURITY MODE COMMAND message cannot be accepted,   1. 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. 2. Upon receipt of the DIRECT LINK SECURITY MODE REJECT message, if the PC5 signalling protocol cause IE in the DIRECT LINK SECURITY MODE REJECT message is not the “#d: LSBs of KNRP-sess ID conflict”, the initiating UE abort the ongoing procedure that triggered the initiation of the PC5 shall abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | 1. The behaivor of how the target UE sends the DIRECT LINK SECURITY MODE REJECT message is still missing. 2. When the PC5 signalling protocol cause IE in the DIRECT LINK SECURITY MODE REJECT message is not the “#d: LSBs of KNRP-sess ID conflict”, how to handle this case for initiating UE is still unclear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.7.5 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

##### 6.1.2.7.5 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 abort the ongoing procedure that triggered the initiation of the PC5 unicast link security mode control procedure. The DIRECT LINK SECURITY MODE REJECT message contains a PC5 signalling protocol cause IE indicating one of the following cause values:

#a: authentication failure;

#b: integrity failure;

#c: UE security capabilities mismatch;

#d: LSBs of KNRP-sess ID conflict;

#e: UE PC5 unicast signalling security policy mismatch; or

#111: protocol error, unspecified.

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 #e "UE PC5 unicast signalling security policy mismatch" in the 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 #e "UE PC5 unicast signalling security policy mismatch" in the 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 and:

a) if the PC5 signalling protocol cause IE in the DIRECT LINK SECURITY MODE REJECT message is set to #d "LSBs of KNRP-sess ID conflict", retransmit the DIRECT LINK SECURITY MODE COMMAND message with a different value for the 8 LSBs of KNRP-sess ID; or

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

\* \* \* End of Change \* \* \* \*