**3GPP TSG-CT WG1 Meeting #134-eC1-221abc**

**E-Meeting, 17th – 25th February 2022 (was C1-221468)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0227** | **rev** | **1** | **Current version:** | **16.7.0** |  |
|  | | | | | | | | |
| *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:*** | Correction to the PC5 unicast link security mode control procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2022-02-23 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to TS 24.587 clauses 6.1.2.7.2 and 6.1.2.7.3, during security mode control procedure, the UE can choose the null integrity algorithm for signalling integrity protection, if PC5 unicast signalling integrity protection policy for both initiating UE and target UE are NOT NEEDED.  After security mode control procedure, the V2X layer will consider the security of this PC5 unicast link is using the null integrity algorithm so security is established but because of the nature of the null integrity algorithm, the message is unsecured.  Quotes:  Clause 6.1.2.7.2:  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  [..]  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".  [..]  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.  Also, note that security requirements in TS 33.536 indicates that security mode control procedure can be successful based on a null integrity algorithm.  However, clause 6.1.2.7.1 indicates quote:  Security is not established if the UE PC5 signalling integrity protection is not activated.  Also, clause 6.1.2.7.3:  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. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Correction to the PC5 unicast link security mode control procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment with stage 2 requirements in TS 33.536 and inconsistency in TS 24.587 (with other clauses; 6.1.2.7.2, 6.1.2.7.3). Wrong implementations can be developed as it is not clear whether security is established or not for null integrity algorithm. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.7.1, 6.1.2.7.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

\* \* \* First Change \* \* \* \*

##### 6.1.2.7.1 General

The PC5 unicast link security mode control procedure is used to establish security between two UEs during a PC5 unicast link establishment procedure or a PC5 unicast link re-keying procedure.. After successful completion of the PC5 unicast link security mode control procedure, the selected security algorithms and keys are used to integrity protect and cipher all PC5 signalling messages exchanged over this PC5 unicast link between the UEs and the security context can be used to protect all PC5 user plane data exchanged over this PC5 unicast link between the UEs. The UE sending the DIRECT LINK SECURITY MODE COMMAND message is called the "initiating UE" and the other UE is called the "target UE".

\* \* \* 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 PC5 unicast link is unsecured. 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 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 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 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. 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.

\* \* \* End of Changes \* \* \* \*