**3GPP TSG-CT WG1 Meeting #125-eC1-20XXXX**

**Electronic meeting, 20-28 August 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **24.587** | **CR** | **0089** | **rev** | **1** | **Current version:** | **16.1.1** |  |
|  |
| *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:***  | Clarification on integrity protection and ciphering of PC5 signalling and user plane |
|  |  |
| ***Source to WG:*** | Huawei, Hisilicon |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | eV2XARC |  | ***Date:*** | 2020-08-13 |
|  |  |  |  |  |
| ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Whether the integrity protection and ciphering of the PC5 signalling messages, and possible integrity protection and ciphering of PC5 user plane data are needed, depends on the security policies of two UEs when establishing a PC5 unicast link.More clarifications need to be added to clause 6.1.2.7 and clause 6.1.2.11, as current specification is based on the pre-condition that both integrity protection and ciphering protection are activated. However, this pre-condition statement is nowhere to find in many security related clauses in the current specification. Current specification also lacks description of no security protection condition (i.e. no integrity protection and no ciphering protection) and partial security condition (e.g. only integrity protection).During the PC5 unicast link security mode control procedure, the target UE shall first check the chosen algorithms to determine whether security protection is needed, and then begins to derive the keys. However, current specification does follow such sequence in subclause 6.1.2.7.3.Besides, if the security policy for a PC5 unicast link indicates no integrity protection, then all PC5 signalling messages of this PC5 unicast link should be processed without integrity protection. However, current specification does follow this way in subclause 6.1.2.11. |
|  |  |
| ***Summary of change:*** | 1. Clarifications on scenarios that without signalling integrity protection (unprotected unicast link) or with partial security condition (e.g. only integrity protection) during the security mode control procedure, to make it clear when actions are needed to derive keys and how to select corresponding security algorithms.
2. Corrected sequence of checking whether security protection is needed and deriving the correponding keys during the security mode control procedure.
3. Clarification on checking of PC5 singalling messages, to make it clear that all messages are processed without integrity protection if integrity protection is not activated.
 |
|  |  |
| ***Consequences if not approved:*** | Incomplete technical specification, and confusing for UE implementation when security is not needed or only partially needed (e.g. only integrity protection) |
|  |  |
| ***Clauses affected:*** | 6.1.2.7.1, 6.1.2.7.2, 6.1.2.7.3, 6.1.2.7.4, 6.1.2.11.1, 6.1.2.11.3 |
|  |  |
|  | **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 PC5 unicast link security mode control procedure

##### 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. Security is not established if the UE PC5 signalling integrity protection is not activated. 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".

Editor’s note: It is FFS whether the user plane is protected by the security association.

##### 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 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 if a new KNRP has been derived at the initiating UE;

3) shall include a Nonce\_2 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 KNPR-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 KNPR-sess ID from the 8 MSBs of KNPR-sess ID received in the DIRECT LINK ESTABLISHMENT REQUEST message or DIRECT LINK REKEYING REQUEST message and the 8 LSBs of KNPR-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

##### 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 PC5 unicast link security mode control procedure was triggered during a PC5 unicast link establishment procedure, the target UE shall first 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, the target UE shall check that the 8 LSBs of KNPR-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.

If the selected integrity protection algorithm is not the null integrity protection algorithm, then 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,

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

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.

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

##### 6.1.2.7.4 PC5 unicast link security mode control procedure completion by the initiating UE

Upon receiving a DIRECT LINK SECURITY MODE COMPLETE message, the initiating UE shall stop timer T5007. If the selected integrity protection algorithm is not the null integrity protection algorithm, the UE checks the integrity of the DIRECT LINK SECURITY MODE COMPLETE message. If the integrity check passes, the initiating UE shall then continue the procedure which triggered the PC5 unicast link security mode control procedure. If the selected integrity protection algorithm is the null integrity protection algorithm, the UE continues the procedure without checking the integrity protection.

\* \* \* Next Change \* \* \* \*

6.1.2.11.1 Overview

This clause describes the principles for the handling of PC5 unicast security contexts in the UE and the procedures used for the security protection of PC5 signalling messages exchanged between UEs over a PC5 unicast link. Based on the security policies of UEs, security protection for a PC5 unicast link involves integrity protection and ciphering of the PC5 signalling messages, and integrity protection and ciphering of PC5 user plane data. The use of integrity protection and ciphering over a PC5 unicast link is optional (see 3GPP TS 33.536 [20]).

The signalling procedures for the control of PC5 unicast security are part of the PC5 signalling protocol and are described in detail in clause 6.1.2.

NOTE: It is recommended to set the UE PC5 unicast signalling integrity protection policy to "signalling integrity protection required" in order to guarantee security protection over PC5. In this subclause, for the ease of description, it is assumed that integrity protection and ciphering are used, unless explicitly indicated otherwise. Operation of a PC5 unicast link without integrity protection or ciphering is achieved by configuring the UE so that it always selects the "null integrity protection algorithm", 5G-IA0, or the "null ciphering algorithm", 5G-EA0.

\* \* \* Next Change \* \* \* \*

6.1.2.11.3 Checking of PC5 signalling messages in the UE

If the signalling integrity protection is not activated for PC5 unicast link, all PC5 signalling messages are processed by the UE without integrity protection.

If the signalling integrity protection is activated for PC5 unicast link, except the messages listed below, no PC5 signalling messages that is not integrity protected shall be processed by the UE:

a) DIRECT LINK ESTABLISHMENT REQUEST message;

b) DIRECT LINK ESTABLISHMENT REJECT message;

c) DIRECT LINK AUTHENTICATION REQUEST message;

d) DIRECT LINK AUTHENTICATION RESPONSE message;

e) DIRECT LINK AUTHENTICATION REJECT message; and

f) DIRECT LINK SECURITY MODE REJECT message.

NOTE: These messages are accepted by the receiving UE without integrity protection, as in certain situations they are sent by the peer UE before security can be activated.

Once the secure exchange of PC5 signalling messages has been established, the receiving UE shall not process any PC5 signalling message that does not successfully pass the integrity check. The DIRECT LINK SECURITY MODE COMMAND message shall be processed as specified in clause 6.1.2.7.3. If any PC5 signalling message is received as not integrity protected and not ciphered even though the secure exchange of PC5 signalling messages has been established, then the receiving UE shall discard this message.

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