**3GPP TSG-CT WG1 Meeting #136-eC1-22abcd**

**E-Meeting, 12th – 20th May 2022 (was C1-223733)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0247** | **rev** | **1** | **Current version:** | **17.5.0** |  |
|  | | | | | | | | |
| *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:*** | Clarification on Null security algorithms | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI17 | | | | |  | ***Date:*** | | | 2022-05-05 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | As described by the discussion paper in C1-223730, RAN5 has sent an LS to CT1 on V2X PC5 link for unicast communication with null security algorithm.  According to specifications (TS 33.536, TS 38.331) the use of null security algorithms (i.e., in 5GS NEA0 and NIA0) are in fact security algorithms used for integrity and/or ciphering of messages. However, when applied they cannot provide any encryption protection or integrity protection for the control plane signalling messages. So when the null security algorithm(s) are selected and in use the control plane signalling messages will be sent unprotected. In short, security is activated (security context is established and integrity and/or ciphering using Null security algorithm is used) as a result of successful security control mode procedure but the messages are sent unprotected.  The important part to clarify in TS 24.587 is that if the null security algorithms are used, then messages are sent unprotected. Hence, there is no security keys are used for performing integrity or ciphering protection of the messages. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarification is done in the specification to avoid any misunderstanding regarding the use of null security algorithms for PC5 control signalling. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misunderstanding about the use of null security algorithm for PC5 control signalling remains. RAN5 doubts how to define their formal conformance testing based on the specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.6.2, 6.1.2.7.1, 6.1.2.7.2, 6.1.2.7.3, 6.1.2.11.1, 6.1.2.11.2.1, 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 \* \* \* \*

##### 6.1.2.6.2 PC5 unicast link authentication procedure initiation by the initiating UE

The initiating UE shall meet one of the following pre-conditions when establishing the non-null signalling integrity protection based on the decision of the initiating UE, before initiating the PC5 unicast link authentication 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 KNRP ID is not included in the DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE does not have an existing KNRP for the KNRP ID included in DIRECT LINK ESTABLISHMENT REQUEST message or the initiating UE derives a new KNRP; 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 the DIRECT LINK REKEYING REQUEST message includes a Re-authentication indication.

In order to initiate the PC5 unicast link authentication procedure, the initiating UE shall create a DIRECT LINK AUTHENTICATION REQUEST message. In this message, the initiating UE:

a) shall include the key establishment information container IE.

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

After the DIRECT LINK AUTHENTICATION 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.

The initiating UE shall start timer T5006. The UE shall not send a new DIRECT LINK AUTHENTICATION REQUEST message to the same target UE while timer T5006 is running.



Figure 6.1.2.6.2: PC5 unicast link authentication procedure

\* \* \* 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 their associated keys if null integrity algorithm or null ciphering algorithm is not used 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".

\* \* \* 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 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 and null integrity protection algorithm or null ciphering protection algorithm is not used, 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 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 messages of the PC5 unicast link are sent unprotected. 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 \* \* \* \*

##### 6.1.2.11.1 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 described in 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 clause, 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 \* \* \* \*

###### 6.1.2.11.2.1 General

The security parameters for authentication, integrity protection and ciphering are tied together in a PC5 unicast security context and identified by a KNRP-sess identifier (KNRP-sess ID). The relationship between the security parameters is defined in 3GPP TS 33.536 [20]. The KNRP-sess ID is self-assigned by the UEs.

Before security using non null security protection algorithms can be established, the UEs establishing a PC5 unicast link need to establish a PC5 unicast security context. The PC5 unicast security context is created as the result of a PC5 unicast link authentication procedure and PC5 unicast link security mode control procedure between the UEs.

The PC5 unicast security context is taken into use by the UEs when one of the UEs initiates a PC5 unicast link security mode control procedure.

The creation of a security context also results in the establishment of a key KNRP and its identifier KNRP ID at the UEs.

The PC5 unicast security context can be created using KNRP when a new PC5 unicast link is established without executing a new PC5 unicast link authentication procedure (see clause 6.1.2.11.2.2). For this purpose, the DIRECT LINK ESTABLISHMENT REQUEST message contains a KNRP ID indicating the PC5 unicast security context.

\* \* \* 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, the UE shall not process the PC5 signalling messages that are not integrity protected:

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;

f) DIRECT LINK SECURITY MODE REJECT message; and

g) DIRECT LINK AUTHENTICATION FAILURE 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:

a) null integrity protection algorithm and null ciphering protection algorithm are not used; or

b) non null integrity protection algorithm and null ciphering protection algorithm are used;

any PC5 signalling message that 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 \* \* \* \*