**3GPP TSG-CT WG1 Meeting #124-eC1-20xxxx**

**Electronic meeting, 2-10 June 2020 (was C1-203118)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0005** | **rev** | **3** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *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:*** | Adding general subclause on security of PC5 signalling messages | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eV2XARC | | | | |  | ***Date:*** | | | 2020-05-20 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | At SA3#99e, SA3 agreed S3-201338 (TS 33.536 v1.2) with further specifying procedures for key derivation and security establishment for the PC5 unicast link.  It is proposed to add a general subclause on PC5 unicast security in TS 24.587 to specify which PC5 signalling messages can be sent unprotected and which PC5 signalling messages can only be sent protected, similar to subclause 4.4 in TS 24.301 and subclause 4.4 in TS 24.501. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | A general subclause on PC5 unicast security to specify which PC5 signalling messages can be sent unprotected and which PC5 signalling messages can only be sent protected was added to TS 24.587. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Which PC5 signalling messages can be sent unprotected and which PC5 signalling messages can only be sent protected will remain unspecified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.1a (New), 6.1.2.1a.1 (New), 6.1.2.1a.2 (New), 6.1.2.1a.2.1 (New), 6.1.2.1a.2.2 (New), 6.1.2.1a.2.3 (New), 6.1.2.1a.3 (New) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 uses a reference to 3GPP TS 33.536 [yy] which is added by CR 0002 to TS 24.587 (C1-202104). | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Revision 2 (CT1#124-e):   * Added “possible” in front of “integrity protection and ciphering of PC5 user plane data” in subclause 6.1.2.1a.1 * Removed the Editor’s note in subclause 6.1.2.1a.1 about the integrity protection and ciphering of PC5 user plane data being FFS * Added a NOTE in subclause 6.1.2.1a.1   Revision 3 (CT1#124-e):   * PC5 unicast security (integrity protection, ciphering) is optional * Add NOTE to address recommendation of PC5 unicast security in order to guarantee security protection. | | | | | | | | |

\*\*\* First change \*\*\*

#### 6.1.2.1a PC5 unicast security

##### 6.1.2.1a.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. Security protection involves integrity protection and ciphering of the PC5 signalling messages, and possible 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 [yy]).

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.

##### 6.1.2.1a.2 Handling of PC5 unicast security contexts

###### 6.1.2.1a.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 [yy]. The KNRP-sess ID is self-assigned by the UEs.

Before security can be activated, 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 6.1.2.1a.2.2). For this purpose, the DIRECT LINK ESTABLISHMENT REQUEST message contains a KNRP ID indicating the PC5 unicast security context.

###### 6.1.2.1a.2.2 Establishment of secure exchange of PC5 signalling messages

Secure exchange of PC5 signalling messages over a PC5 unicast link is established during the PC5 unicast link establishment procedure by initiating a PC5 unicast link security mode control procedure. After successful completion of the PC5 unicast link security mode control procedure, all PC5 signalling messages exchanged between the UEs are sent integrity protected using the PC5 unicast security algorithms, and except for the DIRECT LINK SECURITY MODE COMMAND message, all PC5 signalling messages exchanged between the UEs are sent ciphered using the PC5 unicast security algorithms. The security exchange of PC5 signalling messages is maintained for the lifetime of the PC5 unicast link.

###### 6.1.2.1a.2.3 Change of security keys

When one of the UEs using the PC5 unicast link initiates a PC5 unicast link re-keying procedure to create a new PC5 unicast security context, the PC5 signalling messages exchanged during the PC5 unicast link authentication procedure, if any, are integrity protected and ciphered using the old PC5 unicast security context, i.e. the PC5 unicast security context that was in use before the start of the PC5 unicast link re-keying procedure.

Both UEs shall continue to use the old PC5 unicast security context until the UE which has received the DIRECT LINK REKEYING REQUEST message initiates a PC5 unicast link security mode control procedure. The UE shall send the DIRECT LINK SECURITY MODE COMMAND message integrity protected with the new PC5 unicast security context, but unciphered. When the peer UE responds with a DIRECT LINK SECURITY MODE COMPLETE message, it shall send the message integrity protected and ciphered with the new PC5 unicast security context.

##### 6.1.2.1a.3 Checking of PC5 signalling messages in the UE

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 \*\*\*