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

**E-Meeting, 17th – 25th February 2022 (was C1-221464)**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.587** | **CR** | **0225** | **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:*** | Setting of the MSB of the KNRP-sess ID for the PC5 unicast link identifier update 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:*** | | The PC5 unicast link identifier update procedure may be triggered by several reasons. If it is triggered by a privacy reason, a non-NULL confidentiality algorithm shall be used according security requirements in TS 33.536 clause 5.3.3.2.1.  For other cases (the PC5 unicast link identifier update procedure is triggered by other reason), e.g., TS 23.287 clause 6.3.3.2, the PC5 unicast link identifier update procedure can be executed without security protection (i.e configuring the null integrity algorithm). Hence, since the PC5 unicast link identifier update could be used, new MSB/LSB of KNRP-sess ID could not be generated because KNRP-sess ID is always zero when no securty is used according to TS 33.536 5.3.3.1.4.3 and 5.3.3.1.2.1, quotes:  Clause 5.3.3.1.4.3  3.  UE\_2 shall send the Direct Security Mode Command message to UE\_1. This message shall only contain the MSB of KNRP ID unless the Null integrity algorithm is selected by UE\_2 and optionally Key\_Est\_Info if a fresh KNRP is to be generated (see clause 5.3.3.1.3). UE\_2 shall include the Chosen\_algs parameter to include the selected integrity and confidentiality algorithm. Non-Null security algorithm in the Chosen\_algs indicates the corresponding security protection is activated and the security algorithm the UEs will use to protect the data in the message. Null security algorithm in the Chosen\_algs indicates the corresponding security protection is unprotected. The Chosen\_algs may only indicate the use of the NULL integrity algorithm if UE\_2's signalling integrity security policy is either NOT NEEDED or PREFERRED. UE\_2 shall also return the UE\_1's security capabilities and UE\_1's signalling security policy to provide protection against bidding down attacks. In the case that the NULL integrity algorithm is chosen, the NULL confidentiality algorithm shall also be chosen and UE\_2 shall set the KNRP-sess ID of this security context to the all zero value.  Clause 5.3.3.1.2.1  -    KNRP-sess: This is the 256-bit key that is derived by UE from KNRP and is used derive keys that to protect the transfer of data between the UEs. The KNRP-sess is derived per unicast link. During activated unicast communication session between the UEs, the KNRP-sess may be refreshed by running the rekeying procedure. The actual keys (see next bullet) that are used in the confidentiality and integrity algorithms are derived directly from KNRP-sess. The 16-bit KNRP-sess ID identifies the KNRP-sess.  NOTE 1: A KNRP-sess ID with a zero value indicates that no security is used and hence the UEs do not assign an all zero value of KNRP-sess ID when creating a security context.  However, TS 24.587 in clause mandates to set a new MSB of KNRP-sess ID, quote:  The initiating UE shall initiate the procedure if:  a)  the initiating UE receives a request from upper layers to change the application layer ID and there is an existing PC5 unicast link associated with this application layer ID; or  b)  the privacy timer (see clause 5.2.3) of the initiating UE's layer-2 ID expires for an existing PC5 unicast link.  If the PC5 unicast link identifier update procedure is triggered by a change of the initiating UE's application layer ID, the initiating UE shall create a DIRECT LINK IDENTIFIER UPDATE REQUEST message. In this message, the initiating UE  a)  shall include the initiating UE's new application layer ID received from upper layer;  b)  shall include the initiating UE's new layer-2 ID assigned by itself;  c)  shall include the new MSB of KNRP-sess ID; and  d)  shall include the new IP address/prefix if IP communication is used.  In short, TS 33.536 indicates that the KNRP-sess ID of this security context to the all zero value (it is not actually generated). So again, TS 24.587 needs to be corrected. The specification needs to indicate as per TS 33.536 that the MSB of KNRP-sess ID is all zeros in the DIRECT LINK IDENTIFIER UPDATE REQUEST message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The MSB of KNRP ID is all zeros in the DIRECT LINK IDENTIFIER UPDATE REQUEST message if the KNRP-sess ID of the related security context is not actually generated. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignment with stage 2 requirements in TS 33.536. Not possible to set the MSB of KNRP-sess ID is all zeros. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.1.2.5.2, 8.4.16 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \* \* \* \*

##### 6.1.2.5.2 PC5 unicast link identifier update procedure initiation by initiating UE

The initiating UE shall initiate the procedure if:

a) the initiating UE receives a request from upper layers to change the application layer ID and there is an existing PC5 unicast link associated with this application layer ID; or

b) the privacy timer (see clause 5.2.3) of the initiating UE's layer-2 ID expires for an existing PC5 unicast link.

If the PC5 unicast link identifier update procedure is triggered by a change of the initiating UE's application layer ID, the initiating UE shall create a DIRECT LINK IDENTIFIER UPDATE REQUEST message. In this message, the initiating UE

a) shall include the initiating UE's new application layer ID received from upper layer;

b) shall include the initiating UE's new layer-2 ID assigned by itself;

c) shall include the new MSB of KNRP-sess ID, or set to all zeros if the selected integrity protection algorithm is not the null integrity protection algorithm; and

d) shall include the new IP address/prefix if IP communication is used.

If the PC5 unicast link identifier update procedure is triggered by the expiry of the initiating UE's privacy timer T5011 as specified in clause 5.2.3, the initiating UE shall create a DIRECT LINK IDENTIFIER UPDATE REQUEST message. In this message, the initiating UE

a) shall include the initiating UE's new layer-2 ID assigned by itself;

b) shall include the new MSB of KNRP-sess ID;

c) may include the initiating UE's new application layer ID if received from upper layer; and

d) shall include the new IP address/prefix if IP communication is used and changed.

After the DIRECT LINK IDENTIFIER UPDATE REQUEST message is generated, the initiating UE shall pass this message to the lower layers for transmission along with the initiating UE's old layer-2 ID for unicast communication and the target UE's layer-2 ID for unicast communication, and start timer T5009. The UE shall not send a new DIRECT LINK IDENTIFIER UPDATE REQUEST message to the same target UE while timer T5009 is running.



Figure 6.1.2.5.2.1: PC5 unicast link identifier update procedure

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

### 8.4.16 MSBs of KNRP-sess ID

The purpose of the MSBs of KNRP-sess ID information element is to carry the 8 most significant bits of the KNRP-sess ID.

The MSBs of KNRP-sess ID information element is a type 3 information element with a length of 2 octets.

The MSBs of KNRP-sess ID information element is coded as shown in figure 8.4.16.1 and table 8.4.16.1.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| MSBs of KNRP-sess ID IEI | | | | | | | | octet 1 |
| MSBs of KNRP-sess ID contents | | | | | | | | octet 2 |

Figure 8.4.16.1: MSBs of KNRP-sess ID information element

Table 8.4.16.1: MSBs of KNRP-sess ID information element

|  |
| --- |
| MSBs of KNRP-sess ID contents (octet 2)  This field contains the 8 most significant bits of KNRP-sess ID. |
| NOTE 1: This field is set to all zeros if the KNRP-sess ID is not generated, i.e., the null integrity algorithm is used. |

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