**3GPP TSG-RAN WG2 Meeting #111 electronic R2-2008358**

**Online, August 17th - 28th, 2020‎**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **38.323** | **CR** |  | **rev** | **-** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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 | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | ‎‎38.323 corrections‎ on Sidelink | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | CATT, Huawei, HiSilicon, ASUSTeK, vivo | | | | | | | | | |
| ***Source to TSG:*** | R2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_V2X\_NRSL-Core | | | | |  | ***Date:*** | | | 2020-08-30 |
|  |  | | | |  | |  | | |  |
| ***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-12 (Release 12) Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | 1. The ciphering function is not applied to SL-SRB0 and Direct Security Mode Command message; thus a restriction is necessary to avoid misleading reader that SL-SRB0 and Direct Security Mode Command message also enjoy ciphering. 2. PC5 unicast link is a concept only used in the upper layers and is not visible in the AS. What is visible to the AS is only PC5 RRC connection. Therefore, it is inappropriate to use teminology “PC5 unicast link” in any AS specification. 3. The integrity protection functionality for sidelink SRBs on a PC5 RRC connection can be activated or deactivated by the upper layers, instead of being always enabled; thus a restriction is needed to avoid misunderstanding that it is always enabled. 4. The sidelink SRB0 will use the same data PDU format for groupcast and broadcast ‎but can not use the data PDU format of sidelink SRBs for unicast. The current title of Section 6.2.2.4 and figure ‎6.2.2.4-1‎ does not include the sidelink SRB0.‎ | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Change 1) Section 5.8:   * Add “(except for SL-SRB0 and Direct Security Mode Command message)” behind “sidelink SRBs” to exclude the SL-SRB0 and Direct Security Mode Command message from the SL-SRBs able to be ciphered.   Change 2) Section 5.8:   * Change “PC5 unicast link” to “PC5 RRC connection”.   Change 3) Section 5.9:   * Add “(if activated by the upper layers)” behind “integrity protection”, to avoid misunderstanding that intergrity protection is always enabled for SL-SRB1/2/3 for a PC5 RRC connection.   Change 4) Section 6.2.2.4:   * Add “and for the sidelink SRB0‎” in the title ‎of Section 6.2.2.4 and figure ‎6.2.2.4-1‎.   **Impact analysis**  **Impacted functionality**  Sidelink ciphering and integrity protection  **Inter-operability:**  If the UE implements the change but the NW does not, or vice-versa, there is no inter-operability issue, as the security related configurations/operations are completely carried out over PC5 between the two UEs and have nothing to do with RAN.  If the UE implements the change but the other UE does not, there is no inter-operability issue, as security functionalites and parameters used in PDCP are all determined by the upper layers with PDCP only referring to corrsponding operations inSA3 Specs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | There are some incorrect descriptions in the PDCP specification on the security aspects for NR sidelink communication. And it is misleading or not easy to find the data PDU format for the sidelink SRB0.‎ | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.8, 5.9, ‎6.2.2.4‎ | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

START OF CHANGE

5.8 Ciphering and deciphering

The ciphering function includes both ciphering and deciphering and is performed in PDCP, if configured. The data unit that is ciphered is the MAC-I (see clause 6.3.4) and the data part of the PDCP Data PDU (see clause 6.3.3) except the SDAP header and the SDAP Control PDU if included in the PDCP SDU. The ciphering is not applicable to PDCP Control PDUs.

For downlink and uplink, the ciphering algorithm and key to be used by the PDCP entity are configured by upper layers TS 38.331 [3] and the ciphering method shall be applied as specified in TS 33.501 [6].

The ciphering function is activated/suspended/resumed by upper layers TS 38.331 [3]. When security is activated and not suspended, the ciphering function shall be applied to all PDCP Data PDUs indicated by upper layers TS 38.331 [3] for the downlink and the uplink, respectively.

For DAPS bearers, the PDCP entity shall perform the ciphering or deciphering for the PDCP SDU using the ciphering algorithm and key either configured for the source cell or configured for the target cell, based on to/from which cell the PDCP SDU is transmitted/received.

For downlink and uplink ciphering and deciphering, the parameters that are required by PDCP for ciphering are defined in TS 33.501 [6] and are input to the ciphering algorithm. The required inputs to the ciphering function include the COUNT value, and DIRECTION (direction of the transmission: set as specified in TS 33.501 [6]). The parameters required by PDCP which are provided by upper layers TS 38.331 [3] are listed below:

- BEARER (defined as the radio bearer identifier in TS 33.501 [6]. It will use the value RB identity –1 as in TS 38.331 [3]);

- KEY (the ciphering keys for the control plane and for the user plane are KRRCenc and KUPenc, respectively).

For NR sidelink communication, the ciphering algorithm and key to be used by the PDCP entity are configured by upper layers as specified in TS 24.587 [16] and the ciphering method shall be applied as specified in TS 33.536 [14].

For NR sidelink communication, the ciphering function is activated for sidelink SRBs (except for SL-SRB0 and Direct Security Mode Command message) and/or sidelink DRBs for a PC5 RRC connection by upper layers TS 38.331 [3]. When security is activated for sidelink SRBs, the ciphering function ‎shall be applied to all PDCP Data PDUs for the sidelink SRBs which belong to ‎the PC5 unicast link.‎ When security is activated for sidelink DRBs, the ciphering function ‎shall be applied to all PDCP Data PDUs for the sidelink DRBs which belong to ‎the PC5 unicast link.‎

For NR sidelink communication, the ciphering and deciphering function as specified in TS 33.536 [14] is applied with KEY (NRPEK), COUNT, BEARER (LSB 5 bits of LCID as specified in TS 38.321 [4]) and DIRECTION (which value shall be set is specified in TS 33.536 [14]) as input.

5.9 Integrity protection and verification

The integrity protection function includes both integrity protection and integrity verification and is performed in PDCP, if configured. The data unit that is integrity protected is the PDU header and the data part of the PDU before ciphering. The integrity protection is always applied to PDCP Data PDUs of SRBs. The integrity protection (if activated by the upper layers) is applied to sidelink SRB1, SRB2 and SRB3. The integrity protection is applied to PDCP Data PDUs of DRBs (including sidelink DRBs for unicast) for which integrity protection is configured. The integrity protection is not applicable to PDCP Control PDUs.

For downlink and uplink, the integrity protection algorithm and key to be used by the PDCP entity are configured by upper layers TS 38.331 [3] and the integrity protection method shall be applied as specified in TS 33.501 [6].

The integrity protection function is activated/suspended/resumed by upper layers TS 38.331 [3]. When security is activated and not suspended, the integrity protection function shall be applied to all PDUs including and subsequent to the PDU indicated by upper layers TS 38.331 [3] for the downlink and the uplink, respectively.

NOTE 1: As the RRC message which activates the integrity protection function is itself integrity protected with the configuration included in this RRC message, this message needs first be decoded by RRC before the integrity protection verification could be performed for the PDU in which the message was received.

NOTE 2: As the PC5-S message which activates the integrity protection function is itself integrity protected with the configuration included in this PC5-S message, this message needs first be decoded by upper layer before the integrity protection verification could be performed for the PDU in which the message was received.

For DAPS bearers, the PDCP entity shall perform the integrity protection or verification for the PDCP SDU using the integrity protection algorithm and key either configured for the source cell or configured for the target cell, based on to/from which cell the PDCP SDU is transmitted/received.

For downlink and uplink integrity protection and verification, the parameters that are required by PDCP for integrity protection are defined in TS 33.501 [6] and are input to the integrity protection algorithm. The required inputs to the integrity protection function include the COUNT value, and DIRECTION (direction of the transmission: set as specified in TS 33.501 [6]). The parameters required by PDCP which are provided by upper layers TS 38.331 [3] are listed below:

- BEARER (defined as the radio bearer identifier in TS 33.501 [6]. It will use the value RB identity –1 as in TS 38.331 [3]);

- KEY (the integrity protection keys for the control plane and for the user plane are KRRCint and KUPint, respectively).

For NR sidelink communication, the integrity protection algorithm and key to be used by the PDCP entity are configured by upper layers TS 24.587 [16] and the integrity protection method shall be applied as specified in TS 33.536 [14].

For NR sidelink communication, the integrity protection function is activated for sidelink SRBs and/or sidelink DRBs for a PC5 unicast link ‎by upper layers TS 38.331 [3]. When security is activated for sidelink SRBs, the integrity protection ‎function shall be applied to all PDUs including and subsequent to the PDU for the ‎sidelink SRBs which belong to the PC5 unicast link.‎ When security is activated for sidelink DRBs, the integrity protection ‎function shall be applied to all PDUs including and subsequent to the PDU for the ‎sidelink DRBs which belong to the PC5 unicast link.‎

For the SLRB that needs integrity protection and verification, the parameters that are required by PDCP for integrity protection are defined in TS 33.536 [14] and are input to the integrity protection algorithm. The required inputs to the integrity protection function include the KEY (NRPIK), COUNT, BEARER (LSB 5 bits of LCID as specified in TS 38.321 [4]) and DIRECTION (which value shall be set is specified in TS 33.536 [14]).

At transmission, the UE computes the value of the MAC-I field and at reception it verifies the integrity of the PDCP Data PDU by calculating the X-MAC based on the input parameters as specified above. If the calculated X-MAC corresponds to the received MAC-I, integrity protection is verified successfully.

END OF CHANGE

START OF CHANGE

#### 6.2.2.4 Data PDU for SLRBs for groupcast and broadcast and for the sidelink SRB0‎

Figure 6.2.2.4-1 shows the format of the PDCP Data PDU with 12 bits PDCP SN. This format is applicable for sidelink DRBs for groupcast and broadcast and for the sidelink SRB0.



Figure 6.2.2.4-1: PDCP Data PDU format for SLRBs for groupcast and broadcast and for the sidelink SRB0‎

NOTE: There is no control PDU for SLRBs for groupcast and broadcast. Thus, there is no D/C field in the PDCP Data PDU format for SLRBs for groupcast and broadcast. SDU type is only applicable for sidelink DRB.

END OF CHANGE