**3GPP TSG-RAN WG2 #123bis *Draft\_*R2-2311498**

**Xiamen, China, October 9th - 13th, 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **38.323** | **CR** | **X** | **rev** |  | **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 | **X** | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** |  | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | |  |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | |  |
|  | *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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Introduce NR sidelink evolution into PDCP Specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of NR sidelink PDCP duplicaiton feature into PDCP Specification. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Rel-18 NR sidelink evolution is not supported by PDCP. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.2.3, 5.8, 5.9, 5.11.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

|  |
| --- |
| CHANGE START |

### 5.2.3 Sidelink transmit operation

For NR sidelink transmission of the SLRB, the UE shall follow the procedures in clause 5.2.1 with following modification:

- perform the header compression using ROHC as specified in clause 5.7.4, if SDU Type is IP;

- set the PDCP SN of the PDCP Data PDU to TX\_NEXT modulo 2[*sl-PDCP-SN-Size*];

- if the transmitting PDCP entity is associated with two RLC entities, perform transmit operation for PDCP duplication with the associated RLC entities as specified in clause 5.2.1, with the following modifications:

- consider PDCP duplication as activated;

- submit the PDCP control PDU to one of the associated RLC entities.

NOTE X: How to decide to which RLC entity a PDCP control PDU is submitted is left to UE implementation.

|  |
| --- |
| NEXT 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/or sidelink DRBs for a PC5 unicast ‎link by upper layers, as specified in TS 38.331 [3]. When security is activated for sidelink SRBs, the ciphering function ‎shall be applied to all PDCP Data PDUs (except for carrying Direct Security Mode Command message as specified in TS 33.536 [14]) 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 with values 1 to 19 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 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, as specified in 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 with values 1 to 19 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.

|  |
| --- |
| NEXT CHANGE |

### 5.11.2 Duplicate PDU discard

For the PDCP entity configured with *pdcp-Duplication* or for the PDCP entity associated with two RLC entities for an SLRB, the transmitting PDCP entity shall:

- if the successful delivery of a PDCP Data PDU is confirmed by one of the associated AM RLC entities:

- indicate to the other AM RLC entities to discard the duplicated PDCP Data PDU;

- if the deactivation of PDCP duplication is indicated for the DRB:

- indicate to the RLC entities other than the primary RLC entity to discard all duplicated PDCP Data PDUs;

- if the deactivation of PDCP duplication is indicated for at least one associated RLC entities:

- indicate to the RLC entities deactivated for PDCP duplication to discard all duplicated PDCP Data PDUs.

|  |
| --- |
| CHANGE END |

# Appendix: Related agreements for PDCP duplication

*List of RAN2 agreements on L2 operation of PDCP duplication with impacts to PDCP Spec*

**RAN2 #123bis**

**Agreements on need of primary leg**

1. Not to define primary leg, RLC entity
2. PDCP control PDU is sent over one leg, RLC entity, determined by UE implementation.

**Agreements on duplicated PDU discard**

1. Duplicate PDU discard procedure applied to the Uu PDCP entity associated with AM RLC entities is reused for SL PDCP duplication in unicast.

**Agreements on SRBs**

1. SL PDCP duplication can be applied to SL-SRB3 only after receiving RRCReconfigurationCompleteSidelink.
2. SL PDCP duplication can be applied to SL-SRB1/2 only after receiving RRCReconfigurationCompleteSidelink.

**Agreements on PDCP duplication activation/deactivation SL MAC CE**

1. Not to define separate PDCP duplication activation/deactivation SL MAC CE (including Uu MAC CE).

**Agreements on security**

1. Small LCID (between 1 to 19) among all LCIDs associated with PDCP entity is used in security handling for PDCP duplication.