**3GPP TSG-RAN WG2 Meeting #118-e R2-220xxxx**

**Electronic Meeting, 09 - 20 May, 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **38.323** | **CR** | **-** | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *For* [***HELP***](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:*** | Miscellaneous corrections for MBS 38.323 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Xiaomi Communications | | | | | | | | | |
| ***Source to TSG:*** | R2 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | NR\_MBS-Core | | | | |  | ***Date:*** | | | 2022-05-14 |
|  |  | | | |  | |  | | |  |
| ***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-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Cyphering/deciphering and integrity protection/verification in PDCP is not applicable for MRBs.  UDC support for MRB is missing.  Window\_Size is not missing for the receving PDCP entity of MRB.  According to the RAN2 agreement as quoted below, the Initial RX\_DELIV should be calculated as follows:   * Go for Option 2   Initial RX\_DELIV is configured by RRC: SN(RX\_DELIV) = SN\_ref and HFN(RX\_DELIV) = HFN\_initial where HFN\_initial and SN\_ref are provided by RRC for multicast. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | In section 5.8 and 5.9, MRB is clarified as not applicable for cyphering/deciphering and integrity protection/verification.  In section 5.14.2, 5.14.3 and 6.2.3.4, MRB is added for UDC.  In section 7.2, MRB is added for Window\_Size.  In section 6.3.5 and 7.1, for multicast MRB, the initial value of SN/HFN of RX\_DELIV is set by the RRC configuration, and the initial value of HFN of RX\_NEXT is set by the RRC configuration. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Cyphering/deciphering and integrity protection/verification which is not applicable for MRB is still applied in the PDCP procedure.  UDC is not applied for MRB.  Window\_Size is not defined for MRB. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.8, 5.9, 5.14.2, 5.14.3, 6.2.3.4, 6.3.5, 7.1, 7.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

*First Modified Subclause*

## 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 as specified in TS 38.321 [4]) and DIRECTION (which value shall be set is specified in TS 33.536 [14]) as input.

The ciphering and deciphering are not applied to MRB and sidelink SRB4.

## 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] for NR and in TS 33.401 [17] for E-UTRA/EPC.

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] or TS 33.401 [17] 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]) or TS 33.401 [17]. 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] or TS 33.401 [17]. 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 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.

The integrity protection and verification are not applied to MRB and sidelink SRB4.

*Next Modificatcion*

### 5.14.2 Configuration of UDC

The PDCP entities associated with DRBs/MRBs can be configured by upper layers, see TS 38.331 [3], to use UDC. If UDC is configured, the UE shall apply UDC compression function (details see clause X.1) to process the received PDCP SDU from upper layers corresponding to the configured DRB/MRB. The size of compression buffer is configured by upper layer via *bufferSize*. If pre-defined dictionary is configured by upper layers, the UE shall first set the compression buffer to all zeros and then prefill the configured pre-defined dictionary in the compression buffer upon configuration of UDC. If pre-defined dictionary is not configured by upper layers, UE shall set the compression buffer to all zeros.

### 5.14.3 UDC header

UDC header (1 byte) is added in UDC compression function followed by UDC data block. The UDC header contains the information about whether the current PDCP SDU is compressed by UDC protocol or not. Only the compressed packets are stored in the buffer. The UDC header also contains a reset bit to inform the decompressor that the compression buffer has been reset. The validation bits (checksum) of the compression buffer are also contained in UDC header. Checksum mechanism could be used to resolve miss-match (if any) between the compression and de-compression buffers. If both SDAP and UDC are configured for a DRB/MRB, the UDC header shall be located after the SDAP header. Figure 5.14.3-1 shows the location of the UDC header in a PDCP data PDU.



Figure 5.14.3-1: Location of UDC header in a PDCP Data PDU

*Next Modificatcion*

#### 6.2.3.4 PDCP Control PDU for UDC feedback packet

Figure 6.2.3.4-1 shows the format of the PDCP Control PDU carrying one UDC feedback. This format is applicable for AM DRBs/MRBs.



Figure 6.2.3.4-1: PDCP Control PDU format for UDC feedback

*Next Modificatcion*

### 6.3.5 COUNT

Length: 32 bits

The COUNT value is composed of a HFN and the PDCP SN. The size of the HFN part in bits is equal to 32 minus the length of the PDCP SN.



Figure 6.3.5-1: Format of COUNT

NOTE: COUNT does not wrap around.

*Next Modificatcion*

## 7.1 State variables

This clause describes the state variables used in PDCP entities in order to specify the PDCP protocol. The state variables defined in this clause are normative.

All state variables are non-negative integers, and take values from 0 to [232 – 1].

PDCP Data PDUs are numbered integer sequence numbers (SN) cycling through the field: 0 to [2[*pdcp-SN-SizeUL*] – 1] or 0 to [2[*pdcp-SN-SizeDL*] – 1] or 0 to [2[*sl-PDCP-SN-Size*] – 1].

The transmitting PDCP entity shall maintain the following state variables:

a) TX\_NEXT

This state variable indicates the COUNT value of the next PDCP SDU to be transmitted. The initial value is 0, except for SRBs configured with state variables continuation. For target SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding source SRB. For source SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding target SRB.

The receiving PDCP entity shall maintain the following state variables:

a) RX\_NEXT

This state variable indicates the COUNT value of the next PDCP SDU expected to be received. The initial value is 0, except for sidelink broadcast and groupcast, for SRBs configured with state variables continuation, and for MRBs. For NR sidelink communication for broadcast and groupcast or sidelink SRB4 for broadcast and groupcast based sidelink discovery, the initial value of the SN part of RX\_NEXT is (x +1) modulo (2[*sl-PDCP-SN-Size*]), where x is the SN of the first received PDCP Data PDU. For MRBs, the initial value of the SN part of RX\_NEXT is (x +1) modulo (2[*PDCP-SN-Size*]), where x is the SN of the first received PDCP Data PDU. For broadcast MRBs, the initial value of the HFN part of RX\_NEXT is set by UE implementation. For multicast MRBs, the initial value of the HFN part of RX\_NEXT is set to the HFN, as configured by *multicastHFN-AndRefSN*. For target SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding source SRB. For source SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding target SRB.

NOTE: For NR sidelink communication for broadcast and groupcast or sidelink SRB4 for broadcast and groupcast based sidelink discovery, it is up to UE implementation to select the HFN part for RX\_NEXT such that initial value of RX\_DELIV should be a positive value.

b) RX\_DELIV

This state variable indicates the COUNT value of the first PDCP SDU not delivered to the upper layers, but still waited for. The initial value is 0, except for sidelink broadcast and groupcast, for SRBs configured with state variables continuation, and for MRBs. For NR sidelink communication for broadcast and groupcast or sidelink SRB4 for broadcast and groupcast based sidelink discovery, the initial value of the SN part of RX\_DELIV is (x – 0.5 × 2[*sl-PDCP-SN-Size*–1]) modulo (2[*sl-PDCP-SN-Size*]), where x is the SN of the first received PDCP Data PDU. For broadcast MRBs, the initial value of the SN part of RX\_DELIV is set to (x – 0.5 × 2[*PDCP-SN-Size*–1]) modulo (2[*PDCP-SN-Size*]), where x is the SN of the first received PDCP Data PDU, and the initial value of the HFN part of RX\_DELIV is set by UE implementation. For multicast MRBs, the initial value of the SN part of RX\_DELIV is set to the reference PDCP SN, and the initial value of the HFN part of RX\_DELIV is set to the HFN, as configured by *multicastHFN-AndRefSN*. For target SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding source SRB. For source SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding target SRB.

c) RX\_REORD

This state variable indicates the COUNT value following the COUNT value associated with the PDCP Data PDU which triggered *t-Reordering*. For target SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding source SRB. For source SRB configured with state variables continuation, the initial value is the value stored in PDCP entity for the corresponding target SRB.

## 7.2 Constants

a) Window\_Size

This constant indicates the size of the reordering window. The value equals to 2[*pdcp-SN-SizeDL*] – 1 for SRB/DRB/MRB and 2[*sl-PDCP-SN-Size*] – 1 for SLRB.

*End of Modificatcion*