**3GPP TSG-RAN2 Meeting #117 electronic *R2-2203823***

**Online, 21 Feb – 03 Mar, 2022**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **38.323** | **CR** | **0085** | **rev** | **1** | **Current version:** | **16.6.0** |  |
|  |
| *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:***  | Introducing support of UP IP for EPC connected architectures using NR PDCP |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon, Vodafone, Ericsson, Qualcomm |
| ***Source to TSG:*** | RAN2 |
|  |  |
| ***Work item code:*** | UPIP\_SEC\_LTE-RAN-Core |  | ***Date:*** | 2022-03-01 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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 canbe 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:*** | In RP #94 meeting, User Plane Integrity Protection for EPC connected architectures using NR PDCP (i.e. UP IP applies to EN-DC capable UEs) was agreed to be supported in Rel-17 as in RP-213669. |
|  |  |
| ***Summary of change:*** | * In clause 2, adding reference to TS 33.401;
* In clause 5.9, adding descriptions that parameters used for UP IP in LTE/EPC using NR PDCP is referred to TS 33.401.
 |
|  |  |
| ***Consequences if not approved:*** | UP IP can not be supported for LTE/EPC. |
|  |  |
| ***Clauses affected:*** | 2, 5.9 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS 36.331 CR #4763, TS 38.331 CR #2904, TS 36.300 CR #1353, TS 37.340 CR #0294 |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 38.300: "NG Radio Access Network; Overall description".

[3] 3GPP TS 38.331: "NR Radio Resource Control (RRC); Protocol Specification".

[4] 3GPP TS 38.321: "NR Medium Access Control (MAC) protocol specification".

[5] 3GPP TS 38.322: "NR Radio Link Control (RLC) protocol specification".

[6] 3GPP TS 33.501: "Security Architecture and Procedures for 5G System ".

[7] IETF RFC 5795: "The RObust Header Compression (ROHC) Framework".

[8] IETF RFC 3095: "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP and uncompressed".

[9] IETF RFC 4815: "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095".

[10] IETF RFC 6846: "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)".

[11] IETF RFC 5225: "RObust Header Compression (ROHC) Version 2: Profiles for RTP, UDP, IP, ESP and UDP Lite".

[12] 3GPP TS 36.321: "Evolved Universal Terrestrial Radio Access (E-UTRA) Medium Access Control (MAC) protocol specification".

[13] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[14] 3GPP TS 33.536: "Security Aspect of 3GPP Support for Advanced V2X Services".

[15] IEEE Standard 802.3™-2018: "Ethernet".

[16] 3GPP TS 24.587: "Vehicle-to-Everything (V2X) services in 5G System (5GS), Stage 3".

[xx] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

Next change

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 [xx] 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 [xx] 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 [xx]). 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 [xx]. 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.