**3GPP TSG-SA3 Meeting #101-e *S3-203186-r1***

**e-meeting, 9th - 20th November 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** | **DRAFT CR** | **rev** |  | **Current version:** | 16.4.0 |  |
|  |
| *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:***  | Extend UPIP support in 5GS for all 5GC connected RAN architecture (NG-RAN) options |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eUPIP\_SEC |  | ***Date:*** |

|  |
| --- |
| 2020-10-27 |

 |
|  |  |  |  |  |
| ***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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Extend UPIP support in 5GS for all 5GC connected RAN architecture (NG-RAN) options |
|  |  |
| ***Summary of change:*** | TBD |
|  |  |
| ***Consequences if not approved:*** | UPIP not supported in 5GS when the UE is connected over E-UTRA to 4GC |
|  |  |
| ***Clauses affected:*** | TBD |
|  |  |
|  | **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 changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.2 Requirements on the UE

### 5.2.1 General

The support and usage of ciphering and integrity protection between the UE and the ng-eNB is identical to the support and usage of ciphering and integrity protection between the UE and the eNB as specified in TS 33.401 [10] with the following additional requirement(s):

* The UE shall support the use of integrity protection with the ng-eNB over the Uu interface if it supports E-UTRA connected to 5GC.
* The UE shall indicate its support of integrity protection with the ng-eNB if it supports E-UTRA connected to 5GC.

The PEI shall be securely stored in the UE to ensure the integrity of the PEI.

### 5.2.2 User data and signalling data confidentiality

The UE shall support ciphering of user data between the UE and the gNB.

The UE shall activate ciphering of user data based on the indication sent by the gNB.

The UE shall support ciphering of RRC and NAS-signalling.

The UE shall implement the following ciphering algorithms:

NEA0, 128-NEA1, 128-NEA2 as defined in Annex D of the present document.

The UE may implement the following ciphering algorithm:

128-NEA3 as defined in Annex D of the present document.

The UE shall implement the ciphering algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Confidentiality protection of the user data between the UE and the gNB is optional to use.

Confidentiality protection of the RRC-signalling, and NAS-signalling is optional to use.

Confidentiality protection should be used whenever regulations permit.

### 5.2.3 User data and signalling data integrity

The UE shall support integrity protection and replay protection of user data between the UE and the gNB. The UE shall support integrity protection of user data at any data rate, up to and including, the highest data rate supported by the UE.

The UE shall activate integrity protection of user data based on the indication sent by the gNB.

The UE shall support integrity protection and replay protection of RRC and NAS-signalling.

The UE shall implement the following integrity protection algorithms:

NIA0, 128-NIA1, 128-NIA2 as defined in Annex D of the present document.

The UE may implement the following integrity protection algorithm:

128-NIA3 as defined in Annex D of the present document.

The UE shall implement the integrity algorithms as specified in TS 33.401 [10] if it supports E-UTRA connected to 5GC.

Integrity protection of the user data between the UE and the gNB is optional to use.

NOTE: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB.

Integrity protection of the RRC-signalling, and NAS-signalling is mandatory to use, except in the following cases:

All NAS signalling messages except those explicitly listed in TS 24.501 [35] as exceptions shall be integrity-protected.

All RRC signalling messages except those explicitly listed in TS 38.331 [22] as exceptions shall be integrity-protected with an integrity protection algorithm different from NIA0, except for unauthenticated emergency calls.

The UE shall implement NIA0 for integrity protection of NAS and RRC signalling. NIA0 is only allowed for unauthenticated emergency session as specified in clause 10.2.2.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.4 Requirements on the ng-eNB

The security requirements for ng-eNB are as specified for eNB in TS 33.401 [10] with the following additional requirement:

* ng-eNB shall support the use of integrity protection with the UE over the Uu interface.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.6.2 UP security activation mechanism

AS UP integrity protection and ciphering activation shall be done as part of the DRB addition procedure using RRC Connection Reconfiguration procedure as described in this clause, see Figure 6.6.2-1.

The SMF shall send the UP security policy to the gNB/ng-eNB as defined in Clause 6.6.1.



Figure 6.6.2-1: User plane (UP) security activation mechanism

1a. This RRC Connection Reconfiguration procedure which is used to add DRBs shall be performed only after RRC security has been activated as part of the AS security mode command procedure defined in Clause 6.7.4.

1b. The gNB/ng-eNB shall send the RRC Connection Reconfiguration message to the UE for UP security activation containing indications for the activation of UP integrity protection and ciphering for each DRB according to the security policy.

1c. If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB/ng-eNB does not have KUPint, the gNB/ng-eNB shall generate KUPint and UP integrity protection for such DRBs shall start at the gNB/ng-eNB. Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the gNB/ng-eNB does not have KUPenc, the gNB/ng-eNB shall generate KUPenc and UP ciphering for such DRBs shall start at the gNB/ng-eNB.

2a. UE shall verify the RRC Connection Reconfiguration message. If successful:

2a.1 If UP integrity protection is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have KUPint, the UE shall generate KUPint and UP integrity protection for such DRBs shall start at the UE.

2a.2 Similarly, if UP ciphering is activated for DRBs as indicated in the RRC Connection Reconfiguration message, and if the UE does not have KUPenc, the UE shall generate KUPenc and UP ciphering for such DRBs shall start at the UE

2b. If the UE successfully verifies integrity of the RRC Connection Reconfiguration message, the UE shall send the RRC Connection Reconfiguration Complete message to the gNB/ng-eNB.

If UP integrity protection is not activated for DRBs, the gNB/ng-eNB and the UE shall not integrity protect the traffic of such DRB and shall not put MAC-I into PDCP packet.

If UP ciphering is not activated for DRBs, the gNB/ng-eNB and the UE shall not cipher the traffic of such DRBs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 6.6.4 UP integrity mechanisms

#### 6.6.4.1 General

The PDCP protocol, as specified in TS 38.323 [23] between the UE and the NG-RAN, shall be responsible for user plane data integrity protection.

#### 6.6.4.2 UP integrity mechanisms between the UE and the gNB

The use and mode of operation of the 128-bit NIA algorithms are specified in Annex D.

The input parameters to the 128-bit NIA algorithms as described in Annex D are, the message packet, a 128-bit integrity key KUPint as KEY, a 5-bit bearer identity BEARER value of which is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, and a bearer specific, and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

#### 6.6.4.3 UP integrity mechanisms between the UE and the ng-eNB

If the UE supports E-UTRA connected to 5GC, the UE shall indicate support of integrity protection by setting the EIA7 algorithm bit in 5G UE Security Capability IE (see clause 9.11.3.54 of TS 24.501 [35]) to indicate that the UE supports user plane integrity protection with an ng-eNB.

Editor’s Note: The setting of the EIA7 bit to 1 needs to be specified by CT1 in TS 24.501. This Editor’s note can be removed once this is done by CT1.

When the UE and the ng-eNB use 128-NIA algorithms, clause 6.6.4.2 applies.

When the UE and the ng-eNB use 128-EIA algorithms, the following applies:

* The use and mode of operation of the 128-EIA algorithms are specified in Annex B of TS 33.401 [10].
* The input parameters to the 128-bit EIA algorithms as described in Annex B of TS 33.401 [10] are, the message packet, a 128-bit integrity key KUPint as KEY, a 5-bit bearer identity BEARER value of which is assigned as specified by TS 38.323 [23], the 1-bit direction of transmission DIRECTION, and a bearer specific, time and direction dependent 32-bit input COUNT which corresponds to the 32-bit PDCP COUNT.

If the ng-eNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded.

UE and the ng-eNB (or the ng-eNB acting as the MN) shall derive UP integrity key as specified in Annex A.7 of TS 33.401 [10], with the KeNB set to KgNB.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.10.3.2 Derivation of keys

The UE and MN shall derive the security key KSN of the SN as defined in Annex A.16 of the present document.

The SN RRC and UP keys shall be derived from the KSN both at the SN and the UE using the function given in Annex A.7 of TS 33.401 [10] if the SN is a ng-eNB or using the function given in Annex A.8 of the present specification if the SN is a gNB.

Once all the SN RRC and UP keys have been derived from the KSN, the SN and UE may delete the KSN.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.10.4 Protection of traffic between UE and SN

This subclause provides the details of the needed SN RRC and UP keys and the algorithms used to protect the traffic whose PDCP terminates on the SN. The UE and SN may either calculate all the SN RRC and UP keys at once or as there are required to be used. The RRC and UP keys are KRRCenc and KRRCint for the SRB whose PDCP terminates on the SN and KUPenc for the DRBs whose PDCP terminate on the SN.

When the SN is a gNB, the RRC traffic protection directly between the UE and SN is done using the mechanism described in subclause 6.5 of the present document with the algorithms specified in Annex D of the present document.

When the SN is a gNB, the UP traffic protection and activation is done using the mechanism described in subclauses 6.6 of the present document using the algorithms specified in Annex D of the present document. The UP security activation procedure for MR-DC (meaning NR-DC, NE-DC and NGEN-DC) scenarios use the mechanism described in sublcause 6.10.2.1 with the following additional procedures:

In the case of split PDU session where some of the DRB(s) is terminated at the MN and some DRB(s) is terminated at the SN, the MN shall ensure that all DRBs which belong to the same PDU session have the same UP integrity protection and ciphering activation. To achieve this, the MN shall inform the SN with its UP integrity protection and ciphering activation decision of any DRB that is offloaded and to be terminated at the SN. The SN shall activate the UP integrity protection and ciphering based on the MN decision.

For UP Integrity Protection, if the UE does not indicate that it supports the use of integrity protection with ng-eNB:

Case 1: UP security policy indicates UP Integrity Protection "required":

In NGEN-DC scenario, the MN shall reject the PDU session.

In NE-DC scenario, if the MN decides to activate the UP integrity protection for this PDU session, the MN shall not offload any DRB of the PDU session to the SN.

In NR-DC scenario, the MN makes the decision for PDU sessions that are terminated at the MN while the SN makes the decision for PDU sessions that are terminated at the SN.

Case 2: UP security policy indicates UP Integrity Protection "preferred":

In NGEN-DC scenario, the MN shall always deactivate UP integrity protection. In this case, the SN shall always deactivate the UP integrity protection of any PDU session terminated at the SN.

In NE-DC scenario, if the MN has activated any of this PDU session DRBs with UP integrity protection "on", the MN shall not offload any DRB of this PDU session to the SN. However, if the MN has activated all DRBs of this PDU session with integrity protection "off", the MN may offload DRBs of this PDU session to the SN. In this case, the SN shall not activate the UP integrity protection and shall always set the UP integrity protection indication to "off".

In NR-DC scenario, the MN makes the decision for PDU sessions that are terminated at the MN while the SN makes the decision for PDU sessions that are terminated at the SN.

Case 3: UP security policy indicates UP Integrity Protection "not needed":

In all MR-DC scenarios, the MN and SN shall always deactivate UP integrity protection.

For UP integrity protection, if the UE indicates that it supports use of integrity protection with ng-eNB, in all 5GC-based MR-DC scenarios, the MN and SN shall make a decision on UP integrity protection according to the UP security policy for PDU sessions which terminate at the MN and SN, respectively, where all DRBs belonging to the same PDU session shall have the integrity protection either "on" or "off".

For UP Ciphering Protection:

In all MR-DC scenario, the MN and SN shall make a decision on UP ciphering protection according to the UP security policy for PDU sessions which terminate at the MN and SN, respectively, where all DRBs belonging to the same PDU session shall have the ciphering protection either "on" or "off".

NOTE 1: A UE that is Rel-16 or prior does not support UP integrity protection with ng-eNB. Therefore, explicit indication, as specified in clause 6.6.4.3, that the UE supports use of UP integrity protection with ng-eNB is required.

In all scenarios of MR-DC, the SN shall send the UP integrity protection and encryption indications to the MN in the SN Addition/Modification Request Acknowledgement message. The MN shall forward the UP integrity protection and encryption indications to the UE in RRC Connection Reconfiguration message. The UE activate the UP security protection with the SN based on the UP integrity protection and encryption indications using the scheme described in subclause 6.6.2. If the MN has not activated the RRC security before sending the RRC Connection Reconfiguration message, the MN shall perform AS SMC procedure first.

When the SN is a ng-eNB, the RRC and UP traffic is protected using the mechanism described in subclauses 7.4 and 7.3 respectively of TS 33.401 [10] with the algorithms specified in Annex C of TS 33.401 [10]. Additionally, the UP traffic is integrity protected based on the UP security policy and the indication that the UE supports the use of UP integrity protection with ng-eNB.

NOTE: Void.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*