**3GPP TSG-SA3 Meeting #102-e *S3-210703***

**e-meeting, 18 - 29 January 2021, Online** revision of S3-210701

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1073** | **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:***  | 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:*** | 2021-01-31 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Extend UPIP support in 5GS for all 5GC connected RAN architecture (NG-RAN) options |
|  |  |
| ***Summary of change:*** | Added requirements to support the use of UP IP with ng-eNB. The security mechanisms and procedures for activating use of UP IP with ng-eNB is also added. |
|  |  |
| ***Consequences if not approved:*** | UPIP not supported in 5GS when the UE is connected over E-UTRA to 4GC |
|  |  |
| ***Clauses affected:*** | 5.2.1, 5.4, 5.11.2, 6.6.1, 6.6.2, 6.6.4, 6.10.4 |
|  |  |
|  | **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 changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.11.2 Requirements for algorithm selection

a) UE in RRC\_Connected and a serving network shall have agreed upon algorithms for

- Ciphering and integrity protection of RRC signalling and user plane (to be used between UE and gNB)

- Ciphering and integrity protection of RRC signalling and user plane (to be used between UE and ng-eNB)

- NAS ciphering and NAS integrity protection (to be used between UE and AMF)

b) The serving network shall select the algorithms to use dependent on

- the UE security capabilities of the UE,

- the configured allowed list of security capabilities of the currently serving network entity

c) The UE security capabilities shall include NR NAS algorithms for NAS level, NR AS algorithms for AS layer and LTE algorithms for AS level if the UE supports E-UTRAN connected to 5GC.

NOTE: If the UE supports both E-UTRAN and NR connected to 5GC, the UE 5G security capabilities include both the LTE and NR algorithms.

d) Each selected algorithm shall be indicated to a UE in a protected manner such that a UE is ensured that the integrity of algorithm selection is protected against manipulation.

e) The UE security capabilities shall be protected against "bidding down attacks".

f) It shall be possible that the selected AS and NAS algorithms are different at a given point of time.

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

### 6.6.1 UP security policy

The SMF shall provide UP security policy for a PDU session to the ng-eNB/gNB during the PDU session establishment procedure as specified in TS 23.502 [8].

The UP security policy shall indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all DRBs belonging to that PDU session. The UP security policy shall be used to activate UP confidentiality and/or UP integrity for all DRBs belonging to the PDU session.

The ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per each DRB, according to the received UP security policy, using RRC signalling as defined in clause 6.6.2. If the user plane security policy indicates "Required" or "Not needed", the ng-eNB/gNB shall not overrule the UP security policy provided by the SMF. If the ng-eNB/gNB cannot activate UP confidentiality and/or UP integrity protection when the received UP security policy is "Required", the ng-eNB/gNB shall reject establishment of UP resources for the PDU Session and indicate reject-cause to the SMF. If the received UP security policy is "Not needed ", then the establishment of the PDU Session shall proceed as described in TS 23.502 [8]. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the ng-eNB can activate UP integrity protection.

NOTE 1: Local SMF can override the confidentiality option in the UP security policy received from the home SMF based on its local policy, roaming agreement and/or regulatory requirements.

At an Xn-handover from the source ng-eNB/gNB to the target ng-eNB/gNB, the source ng-eNB/gNB shall include in the HANDOVER REQUEST message, the UE's UP security policy. If the UP security policy is ‘Required’, the target ng-eNB/gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF. For the accepted PDU sessions, the target ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy and shall indicate that to the UE in the HANDOVER COMMAND by the source ng-eNB/gNB. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

If the UE receives an indication in the HANDOVER COMMAND that UP integrity protection and/or UP encryption for a PDU session is enabled at the target ng-eNB/gNB, the UE shall generate or update the UP encryption key and/or UP integrity protection key and shall activate UP encryption and/or UP integrity protection for the respective PDU session.

NOTE 2: If the security policy is ‘Preferred’, it is possible to have a change in activation or deactivation of UP integrity after the handover.

Further, in the Path-Switch message, the target ng-eNB/gNB shall send the UE's UP security policy and corresponding PDU session ID received from the source ng-eNB/gNB to the SMF. The SMF shall verify that the UE's UP security policy received from the target ng-eNB/gNB is the same as the UE's UP security policy that the SMF has locally stored. If there is a mismatch, the SMF shall send its locally stored UE's UP security policy of the corresponding PDU sessions to the target ng-eNB/gNB. This UP security policy information, if included by the SMF, is delivered to the target ng-eNB/gNB in the Path-Switch Acknowledge message. The SMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm.

If the target ng-eNB/gNB receives UE's UP security policy from the SMF in the Path-Switch Acknowledge message, the target ng-eNB/gNB shall update the UE's UP security policy with the received UE's UP security policy. If UE's current UP confidentiality and/or UP integrity protection activation is different from the received UE's UP security policy, then the target ng-eNB/gNB shall initiate intra-cell handover procedure which includes RRC Connection Reconfiguration procedure to reconfigure the DRBs to activate or de-activate the UP integrity/confidentiality as per the received policy from SMF.

In case of the target ng-eNB/gNB receives both UE security capability and UP security policy, then ng-eNB/gNB initiates the intra-cell handover procedure which contains selected algorithm and an NCC to the UE. New UP keys shall be derived and used at both the UE and the target ng-eNB/gNB.

At an N2-handover the SMF shall send the UE's UP security policy to the target ng-eNB/gNB via the target AMF. The target ng-eNB/gNB shall reject all PDU sessions for which it cannot comply with the corresponding received UP security policy and indicate the reject-cause to the SMF via the target AMF. For all other PDU sessions, the target ng-eNB/gNB shall activate UP confidentiality and/or UP integrity protection per DRB according to the received UE's UP security policy. Only if the UE indicates that it supports use of integrity protection with ng-eNB, the target ng-eNB can activate UP integrity protection.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* 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.

If the 128-NIA algorithm is signalled by the ng-eNB to the UE, clause 6.6.4.2 applies.

If the 128-EIA algorithm is signalled by the ng-eNB to the UE, 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.

NOTE: The ng-eNB decides whether to signal 128-NIA or 128-EIA algorithm (cf. clause 5.3.1.2 of TS 36.331 [69]).

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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

6.10.4 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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*