**3GPP TSG-SA3 Meeting #107-e *draft\_S3-220959-r1***

**e-meeting, 16 - 20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.401** | **CR** | **0707** | **rev** |  | **Current version:** | **17.1.0** |  |
|  | | | | | | | | |
| *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 | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | UP IP: mapping of EPS integrity algorithm to NR integrity algorithm | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | SA3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | UPIP\_SEC | | | | |  | ***Date:*** | | | 2022-05-09 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | SA3 has received an LS in S3-220666 / R2-2203663 from RAN2:  *In response to SA3’s request “…****to inform SA3 on their final decision with respect to which algorithm code points are to be used****”, RAN2 would like to provide the following information:*  ***UPIP for the EPC connected architectures uses NR PDCP and is configured in following way:***   * ***(as is done for legacy LTE UE) an LTE algorithm code point is configured in field integrityProtectionAlgorithm in IE SecurityAlgorithmConfig in the TS 36.331 SecurityModeCommand message, and this is used to derive KUPint (and also to derive KUPEnc, as for legacy LTE UE).*** * ***The NR algorithm code point (corresponding to the LTE algorithm code point used in the SecurityModeCommand) indicated by the integrityProtAlgorithm included in the securityConfig in the TS 38.331 RadioBearerConfig is used to configure the UP IP algorithm applied by NR PDCP to perform integrity protection.*** * ***The integrityProtection indicated in pdcp-Config in the DRB-ToAddMod(list) in the TS 38.331 RadioBearerConfig is used to activate the UP IP for a DRB using the configured algorithm, which can be done only at DRB setup. Consequently, UP IP activation/deactivation for a DRB can be changed only by DRB-release-and-add.*** | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | It is proposed to clarify in clause 5.1.4.2 that NR PDCP will be used for user plane integrity protection by adding a new NOTE and reference to TS 36.331:  NOTE: NR PDCP is used for user plane integrity protection in eNB and UE, as specified in TS 36.331~~.~~  It is proposed to add the following requirements in clause 7.2.4.1:   * For normal UE, user plane integrity shall be activated during the RRC Connection Reconfiguration procedure. * The same integrity algorithm shall be used for both RRC integrity protection and UP integrity protection. * The same ciphering algorithm shall be used for both RRC ciphering and UP ciphering.   It is proposed to clarify in clause 7.2.4.2.1 that the following sentence includes integrity protection of user plane traffic between UE and eNB (marked in blue text).  *“The integrity algorithm is used for integrity protection of the RRC traffic, and, if applicable, for the integrity protection of user plane traffic between RN and DeNB and between UE and eNB.”*  It is proposed to add a NOTE in clause 7.2.4.5 that :  NOTE: The selected EPS integrity algorithm indicated in the AS security mode command message is used for both RRC integrity protection and user plane integrity protection, but user plane integrity protection is activated in RRC Connection Reconfiguration procedure.  It is proposed to add the following requirements in clause 7.3.4 that :   * The eNB shall select the NR algorithm (NIA) for the integrity algorithm (which needs to be indicated in the RRC Connection Reconfiguration procedure to the UE), which corresponds to the EPS algorithm (EIA) which the eNB selected and indicated to the UE in the AS Security Mode Command procedure. * When the UE receives the RRC Connection Reconfiguration message then the UE shall map the received NR algorithm to the corresponding EPS algorithm (EIA) and use the EPS algorithm (EIA) for UP integrity protection.   It is proposed to add a new clause 7.3.4.1 which describes the mapping from the selected EPS integrity algorithm in AS SMC to the corresponding NR integrity algorithm indicated in RRC Connection Reconfiguration procedure. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | This specification is not aligned with stage 3. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.1.4.2, 7.2.4.1, 7.2.4.2.1, 7.2.4.5, 7.3.4, 7.3.4.x (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 OF CHANGE \*\*\*\*

### 5.1.4 User data and signalling data integrity

#### 5.1.4.1 Integrity requirements

Synchronization of the input parameters for integrity protection shall be ensured for the protocols involved in the integrity protection.

Integrity protection, and replay protection, shall be provided to NAS and RRC-signalling.

All NAS signaling messages except those explicitly listed in TS 24.301 [9] as exceptions shall be integrity-protected. All RRC signaling messages except those explicitly listed in TS 36.331 [21] as exceptions shall be integrity-protected.

When authentication of the credentials on the UICC during Emergency Calling in Limited Service Mode, as defined in the TS 23.401 [2], can not be successfully performed, the integrity and replay protection of the RRC and NAS signaling shall be omitted (see clause 15). This shall be accomplished by the network by selecting EIA0 for integrity protection of NAS and RRC. EIA0 shall only be used for unauthenticated emergency calls.

User plane packets between the eNB and the UE may be integrity protected on the Uu interface. User plane packets between the RN and the UE may be integrity protected. All user plane packets carrying S1 and X2 messages between RN and DeNB shall be integrity-protected. Integrity protection for all other user plane packets between RN and DeNB may be supported.

All user data packets sent via the MME shall be integrity protected.

#### 5.1.4.2 Algorithm Identifier Values

All algorithms specified in this subclause are algorithms with a 128-bit input key.

NOTE: Deviations from the above requirement have to be indicated explicitly in the algorithm identifier list below.

Each EPS Integrity Algorithm (EIA) will be assigned a 4-bit identifier. Currently, the following values have been defined:

"00002" EIA0 Null Integrity Protection algorithm

"00012" 128-EIA1 SNOW 3G based algorithm

"00102" 128-EIA2 AES based algorithm

"00112" 128-EIA3 ZUC based algorithm

The remaining values have been reserved for future use.

UEs and eNBs shall implement 128-EIA1 and 128-EIA2 for RRC signalling integrity protection. UEs and eNBs may implement 128-EIA3 for RRC signalling integrity protection.

UEs shall and eNBs may implement 128-EIA1 and 128-EIA2 for the user plane integrity protection. UEs and eNBs may implement 128-EIA3 for the user plane integrity protection.

NOTE: NR PDCP is used for user plane integrity protection in eNB and UE, as specified in TS 36.331 [21].

UEs and MMEs shall implement 128-EIA1 and 128-EIA2 for NAS signalling integrity protection. UEs and MMEs may implement 128-EIA3 for NAS signalling integrity protection.

UEs shall implement EIA0 for integrity protection of NAS and RRC signalling. As specified in clause 5.1.4.1 of this specification, EIA0 is only allowed for unauthenticated emergency calls. EIA0 shall not be used for integrity protection between RN and DeNB.

Implementation of EIA0 in MMEs, RNs and eNBs is optional, EIA0, if implemented, shall be disabled in MMEs, RNs and eNBs in the deployments where support of unauthenticated emergency calling is not a regulatory requirement.

\*\*\*\* NEXT CHANGE \*\*\*\*

### 7.2.4 Security mode command procedure and algorithm negotiation

#### 7.2.4.1 Requirements for algorithm selection

1. An active UE and a serving network shall agree upon algorithms for

- RRC ciphering and RRC integrity protection (to be used between UE and eNB)

- UP ciphering and integrity protection (to be used between UE and eNB)

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

An active RN and a network serving the RN shall additionally agree upon algorithms for UP integrity.

1. 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

1. The same set of ciphering and integrity algorithms shall be supported by the UE both for AS and NAS level.
2. Each selected algorithm shall be acknowledged to the UE in an integrity protected way such that the UE is ensured that the algorithm selection was not manipulated, i.e. that the UE security capabilities were not bidden down.
3. The UE security capabilities the ME sent to the network shall be repeated in an integrity protected NAS level message to the ME such that "bidding down attacks" against the UE's security capabilities can be detected by the ME. The UE security capabilities apply to both AS and NAS level security.
4. Separate AS and NAS level security mode command procedures are required. AS level security mode command procedure shall configure AS security (RRC and UP) and NAS level security mode command procedure shall configure NAS security.

a) Both integrity protection and ciphering for RRC shall be activated within the same AS SMC procedure, but not necessarily within the same message.

b) User plane ciphering shall be activated at the same time as RRC ciphering.

c) For Relay Node (RN), user plane integrity shall be activated at the same time as RRC ciphering. For normal UE, user plane integrity shall be activated during the RRC Connection Reconfiguration procedure. User plane integrity shall be applied to a data radio bearer if integrity protection is configured for that data radio bearer at the time of data radio bearer set-up.

1. It shall be possible that the selected AS and NAS algorithms are different at a given point of time.
2. The same integrity algorithm shall be used for both RRC integrity protection and UP integrity protection.
3. The same ciphering algorithm shall be used for both RRC ciphering and UP ciphering.

#### 

\*\*\*\* NEXT CHANGE \*\*\*\*

#### 7.2.4.2 Procedures for AS algorithm selection

##### 7.2.4.2.1 Initial AS security context establishment

Each eNB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator. When AS security context is established in the eNB, the MME shall send the UE EPS security capabilities to the eNB. The eNB shall choose the ciphering algorithm which has the highest priority from its configured list and is also present in the UE EPS security capabilities. The eNB shall choose the integrity algorithm which has the highest priority from its configured list and is also present in the UE EPS security capabilities. The chosen algorithms shall be indicated to the UE in the AS SMC. The ciphering algorithm is used for ciphering of the user plane and RRC traffic. The integrity algorithm is used for integrity protection of the RRC traffic, and, if applicable, for the integrity protection of user plane traffic between RN and DeNB and between UE and eNB.

\*\*\*\* NEXT CHANGE \*\*\*\*

#### 7.2.4.5 AS security mode command procedure

The AS SMC procedure consists of a roundtrip of messages between eNB and UE. The eNB sends the AS security mode command to the UE and the UE replies with the AS security mode complete message. See figure 7.2.4.5-1.

The AS security mode command message from eNB to UE shall contain the selected AS algorithms. This message shall be integrity protected with RRC integrity key based on the current KASME.

NOTE: The selected EPS integrity algorithm indicated in the AS security mode command message is used for both RRC integrity protection and user plane integrity protection, but user plane integrity protection is activated in RRC Connection Reconfiguration procedure.

The AS security mode complete message from UE to eNB shall be integrity protected with the selected RRC algorithm indicated in the AS security mode command message and RRC integrity key based on the current KASME.

RRC and UP downlink ciphering (encryption) at the eNB shall start after sending the AS security mode command message. RRC and UP uplink deciphering (decryption) at the eNB shall start after receiving and successful verification of the AS security mode complete message.

RRC and UP uplink ciphering (encryption) at the UE shall start after sending the AS security mode complete message. RRC and UP downlink deciphering (decryption) at the UE shall start after receiving and successful verification of the AS security mode command message

If any control of the AS security mode command is not successful in the ME, the ME shall reply with an unprotected security mode failure message (see TS 36.331[21]).

AS security mode command always changes the AS keys.



Figure 7.2.4.5-1: AS security setup

\*\*\*\* NEXT CHANGE \*\*\*\*

### 7.3.4 UP integrity protection activation mechanism

AS UP integrity protection activation shall be done as part of the DRB addition procedure using RRC Connection Reconfiguration procedure as described in this clause, see Figure 7.3.4 -1.

As defined in Clause 7.3.3, the MME may send the UP integrity protection policy to the eNB. If the MME does not send the UP integrity protection policy, the eNB may use locally configured UP integrity protection policy.



Figure 7.3.4-1: User plane (UP) integrity protection activation mechanism

1a. This RRC Connection Reconfiguration procedure which is used to add DRBs shall be performed only after RRC security and UP ciphering have been activated as part of the AS security mode command procedure defined in Clause 7.2.4.5 and the UE indicates that it supports use of user plane integrity protection with EPC.

1b. The eNB shall send the RRC Connection Reconfiguration message to the UE for UP security activation containing indication for the activation of UP integrity protection for each DRB according to the security policy.

The eNB shall select the NR integrity algorithm and indicate it in the RRC Connection Reconfiguration procedure to the UE. The selected NR integrity algorithm corresponds to the EPS integrity algorithm which the eNB selected and indicated to the UE in the AS Security Mode Command procedure.

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

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

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 eNB.

When the UE receives the RRC Connection Reconfiguration message then the UE shall use the EPS algorithm which corresponds to the NR algorithm indicated in the RRC Connection Reconfiguration message for UP integrity protection.

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

\*\*\*\* NEXT CHANGE \*\*\*\*

#### 7.3.4.x Mapping from E-UTRA security algorithm to the corresponding NR security algorithm for user plane integrity protection

When the eNB needs to activate user plane integrity protection as part of the DRB addition procedure using RRC Connection Reconfiguration procedure then the eNB shall select the NR algorithm (NIA) for the integrity algorithm which corresponds to the EPS algorithm (EIA) which the eNB selected and indicated to the UE in the AS Security Mode Command procedure.

The eNB shall map the EPS security algorithm to the corresponding NR security algorithm in the following way:

"00012" 128-EIA1 -> "00012" 128-NIA1

"00102" 128-EIA2 -> "00102" 128-NIA2

"00112" 128-EIA3 -> "00112" 128-NIA3

\*\*\*\* END OF CHANGE \*\*\*\*