**3GPP TSG-SA3 Meeting #104-e *S3-213026***

**e-meeting, 16 - 27 August 2021**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.401** | **CR** | **draftCR** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *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:***  | Addition of User Plane Integrity Protection to LTE |
|  |  |
| ***Source to WG:*** | Vodafone |
| ***Source to TSG:*** | SA3 |
|  |  |
| ***Work item code:*** | UPIP\_SEC\_LTE |  | ***Date:*** | 2021-05-08 |
|  |  |  |  |  |
| ***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:*** | Several Attacks on LTE networks have been published recently that rely on the lack of User Plane integrity Protection (UPIP) which may allow user data tampering. UPIP is added to LTE to overcome these security issues. |
|  |  |
| ***Summary of change:*** | Clause 5.1.4.1 - change UPIP support from "shall not" to "may"Clause 5.1.4.2 - Add details of UPIP algorithms to be supportedClause 7.2.4.1 - (a) Add UPIP to algorithm negotiation;(c ) indicate that EIA-x need not be used for UPIP;(h) indicate that (as in R15, option 3x architecture) the AS algorithm choice is configured by RRC signalling indepenently pre radio bearer;(i) indicate that the PGW(s) may send UPIP policy to the MME/eNB on a per EPS bearer basis, and, that without policy the default is “upip=preferred”. |
|  |  |
| ***Consequences if not approved:*** | Users may be redirected to sites that they have not requested or find their data has been corrupted. |
|  |  |
| ***Clauses affected:*** |  |
|  |  |
|  | **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:*** | Creates Release 17 specification |
|  |  |
| ***This CR's revision history:*** |  |

### 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 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 and eNBs shall implement 128-EIA1 and 128-EIA2 to integrity protect the user plane packets between the eNB and the UE and the user plane packets between the RN and the UE. UEs and eNBs may implement 128-EIA3 to integrity protect the user plane packets between the eNB and the UE and the user plane packets between the RN and the UE.

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.

[…]

### 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) User plane integrity shall be activated at the same time as RRC ciphering. 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. It shall be possible to use different AS algorithms for AS Signalling Radio Bearers (e.g. 128-EIA/EEA-x) and AS Data Radio Bearers (e.g. 128-EIAEEA-y).
3. The PGW may provide the MME (and the MME provide the eNB) with User Plane integrity protection policy information on a per EPS bearer basis. In the absence of any policy information, the eNB shall assume that the policy is “UPIP preferred”.