**3GPP TSG-SA3 Meeting #99-e *S3-201031***

**Online, , 11th May 2020 - 15th May 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **0785** | **rev** | 4 | **Current version:** | **16.2.0** |  |
|  |
| *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:***  | CR to 33.501 - Update to User Plane Integrity Protection |
|  |  |
| ***Source to WG:*** | Deutsche Telekom AG, NTT DOCOMO INC.  |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | UPIP\_SEC |  | ***Date:*** | 2020-05-12 |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***Release:*** | Rel-16 |
|  | *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:*** | Updates to the User Plane Integrity Protetion requirements following new advice from the GSMA regarding attacks based on the lack of User Plane Integrity Protetion in 5G and the adverse impacts that these attacks may have. |
|  |  |
| ***Summary of change:*** | In Section 5.2.3 - Update the text to explicitly include the UE’s maximum supported data rate.In Section 5.3.3 - Update the text to explicitly include all data rates and add a note to recommend that UPIP is only turned off by exception. |
|  |  |
| ***Consequences if not approved:*** | Security of user plane data may be compromised |
|  |  |
| ***Clauses affected:*** | 5.2.3, 5.3.3 |
|  |  |
|  | **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:*** |  |

[…]

\*\*\*\*\*\*\*\*\*\* BEGIN MODIFIED SECTION \*\*\*\*\*\*\*\*\*\*

### 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 at the UE’s maximum supported data rate.

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.

\*\*\*\*\*\*\*\*\*\* END OF MODIFIED SECTION\*\*\*\*\*\*\*\*\*\*

[…]

\*\*\*\*\*\*\*\*\*\* BEGIN MODIFIED SECTION \*\*\*\*\*\*\*\*\*\*

### 5.3.3 User data and signalling data integrity

The gNB shall support integrity protection and replay protection of user data between the UE and the gNB.

The gNB shall activate integrity protection of user data based on the security policy sent by the SMF.

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

The gNB shall support the following integrity protection algorithms:

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

The gNB may support the following integrity protection algorithm:

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

Integrity protection of the user data between the UE and the gNB is optional to use and shall not use NIA0.

NOTE1: Integrity protection of user plane adds the overhead of the packet size and increases the processing load both in the UE and the gNB. NIA0 will add an unnecessary overhead of 32-bits MAC with no security benefits.

NOTE2: It is recommended to activate user plane integrity protection by default for all data rates and disable it only by exception.

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.

NIA0 shall be disabled in gNB in the deployments where support of unauthenticated emergency session is not a regulatory requirement.

\*\*\*\*\*\*\*\*\*\* END OF MODIFIED SECTION\*\*\*\*\*\*\*\*\*\*