**3GPP TSG- WG3 Meeting #**

**21st February – 3rd March 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  **0676** | **rev** | **2** | **Current version:** | **16.8.0** |  |
|  |
| *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 |  | Radio Access Network | **x** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Support for mapping complete security capabilities from NAS [UE\_Sec\_Caps] |
|  |  |
| ***Source to WG:*** | , Ericsson, Huawei, Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** |  |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** |  |
|  |  |  |  |  |
| ***Category:*** | **C** |  | ***Release:*** |  |
|  | *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:*** | SA3 has requested RAN3 (in S3-213272) “to modify their specifications to ensure that all of MME, eNB, AMF and NG-RAN node copy on the complete UE security capabilities” from release 17 onwards, to prevent the network not selecting what would be the preferred security algorithm if the full UE security capabilities were available at the eNB or NG-RAN node. |
|  |  |
| ***Summary of change:*** | All currently defined bits in the NAS security capability IEs (both 4G and 5G) are mapped to bits in the corresponding RAN IEs, irrespective of whether they are currently assigned to represent support for a security algorithm. A statement is also added that the “NG-RAN nodes store and send the complete bitmaps without modification or truncation as specified in TS 38.300”. |
|  |  |
| ***Consequences if not approved:*** | No support for the requested functionality in S3-213272. RAN may not be aware of UE’s support for new security algorithms.  |
|  |  |
| ***Clauses affected:*** | 9.2.3.49 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TS36.413 CR1835, TS 36.423 CR1624, TS 38.413 CR0669 |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

#### 9.2.3.49 UE Security Capabilities

The *UE Security Capabilities* IE defines the supported algorithms for encryption and integrity protection in the UE. The NG-RAN nodes store and send the complete bitmaps without modification or truncation as specified in TS 38.300 [9].

Note: There is a 1-bit circular shift between the bitmaps of the IE in this specification and the corresponding bitmaps in TS 38.413.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IE/Group Name | Presence | Range | IE Type and Reference | Semantics Description |
| NR Encryption Algorithms | M |  | BIT STRING {nea1-128(1), nea2-128(2), nea3-128(3)} (SIZE(16, …)) | Each position in the bitmap represents an encryption algorithm:"all bits equal to 0" – UE supports no other NR algorithm than NEA0,"second bit" – 128-NEA1,"third bit" – 128-NEA2,"fourth bit" – 128-NEA3,“fifth to eighth bit” correspond to bit 4 to bit 1 of octet 3 in the *UE Security Capability* IE defined in TS 24.501 [30],other bits reserved for future use. Value ‘1’ indicates support and value ‘0’ indicates no support of the algorithm.Algorithms are defined in TS 33.501 [28]. |
| NR Integrity Protection Algorithms | M |  | BIT STRING {nia1-128(1), nia2-128(2), nia3-128(3)} (SIZE(16, …)) | Each position in the bitmap represents an integrity protection algorithm:"all bits equal to 0" – UE supports no other NR algorithm than NIA0,"second bit" – 128-NIA1,"third bit" – 128-NIA2,"fourth bit" – 128-NIA3,“fifth to eighth bit” correspond to bit 4 to bit 1 of octet 4 in the *UE Security Capability* IE defined in TS 24.501 [30],other bits reserved for future use.Value ‘1’ indicates support and value ‘0’ indicates no support of the algorithm.Algorithms are defined in TS 33.501 [28]. |
| E-UTRA Encryption Algorithms | M |  | BIT STRING {eea1-128(1), eea2-128(2), eea3-128(3)} (SIZE(16, …)) | Each position in the bitmap represents an encryption algorithm:"all bits equal to 0" – UE supports no other algorithm than EEA0,"second bit" – 128-EEA1,"third bit" – 128-EEA2,"fourth bit" – 128-EEA3,“fifth to eighth bit” correspond to bit 4 to bit 1 of octet 5 in the *UE Security Capability* IE defined in TS 24.501 [30],other bits reserved for future use. Value ‘1’ indicates support and value ‘0’ indicates no support of the algorithm.Algorithms are defined in TS 33.401 [29]. |
| E-UTRA Integrity Protection Algorithms | M |  | BIT STRING {eia1-128(1), eia2-128(2), eia3-128(3)} (SIZE(16, …)) | Each position in the bitmap represents an integrity protection algorithm:"all bits equal to 0" – UE supports no other algorithm than EIA0,"second bit" – 128-EIA1,"third bit" – 128-EIA2,"fourth bit" – 128-EIA3,“fifth to eighth bit” correspond to bit 4 to bit 1 of octet 6 in the *UE Security Capability* IE defined in TS 24.501 [30],other bits reserved for future use.Value ‘1’ indicates support and value ‘0’ indicates no support of the algorithm.Algorithms are defined in TS 33.401 [29]. |