**3GPP TSG-SA3 Meeting #99e *S3-201225***

**e-meeting, 11 -15 May 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | **0014** | **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 |  | Radio Access Network | **X** | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  |  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G |  | ***Date:*** | 01-05-2020 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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:*** | The threat references in sub-clauses 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.4, 4.2.2.1.5, 4.2.2.1.6, 4.2.2.1.7, 4.2.2.1.8 and 4.2.2.1.9 need to be removed for the following reasons:* The requirements and test cases in sub-clauses 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.4, 4.2.2.1.5, 4.2.2.1.6, 4.2.2.1.7, 4.2.2.1.8 and 4.2.2.1.9 are all about testing of integrity, confidentiality and replay protection over air interface between the UE and the gNB, while the corresponding threats in TR 33.926 that are expected to be addressed by these test cases are all about integrity and confidentiality over N2/Xn reference points. Hence the test cases failed to address the referenced threats.

The execution steps in sub-clauses 4.2.2.1.6 and 4.2.2.1.7 need to be removed for the following reasons:* The execution steps of test cases in sub-clauses 4.2.2.1.6, and 4.2.2.1.7 all refer to the sub-clause 4.2.3.2.4 in TS 33.117, which is however about the compliance test of 3GPP profiles for IPSec/TLS and not applicable to air interface between the UE and the gNB. Hence the the execution steps do not meet the purpose of the tests.
 |
|  |  |
| ***Summary of change:*** | * Replaced the threat references in sub-clauses 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.4, 4.2.2.1.5, 4.2.2.1.6, 4.2.2.1.7, 4.2.2.1.8 and 4.2.2.1.9 with TBA.
* Replaced the execution steps in sub-clauses 4.2.2.1.6 and 4.2.2.1.7 with TBA
 |
|  |  |
| ***Consequences if not approved:*** | mismatch between test cases and reference threats, mismatched test steps |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.4, 4.2.2.1.5, 4.2.2.1.6, 4.2.2.1.7, 4.2.2.1.8, 4.2.2.1.9 |
|  |  |
|  | **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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.6 Ciphering of RRC-signalling

*Requirement Name:* Ciphering of RRC-signalling

*Requirement Reference:* TS 33.501 [2], clause 5.3.2

*Requirement Description:* *"The gNB shall support ciphering of RRC-signalling over the NG RAN air interface"* as specified in TS 33.501 [2], clause 5.3.2.

*Threat References:* TR 33.926 [5], clause D.2.2.1 – Control plane data confidentiality protection.

***Test Case****:*

**Test Name:** TC-CP-DATA-CIP-RRC-SIGN\_gNB

**Purpose:** Toverify that the RRC-signalling data sent between UE and gNB over the NG RAN air interface are confidentiality protected.

**Pre-Condition:**

- The gNB network product shall be connected in emulated/real network environments.

- Tester shall have access to the ciphering algorithm and confidentiality protection keys.

- The tester shall have access to the NG RAN air interface or can capture the message at the UE.

**Execution Steps:**

1. The UE sends an Registraton Request to the AMF.

2. The AMF sends a KgNB and the UE security capability to the gNB.

3. gNB selects an algorithm and sends AS SMC to the UE,

4. gNB receive AS SMP from the UE.**Expected Results:**

Control plane packets sent by the gNB after eNB sending AS SMC is ciphered.

**Expected format of evidence:**

Evidence suitable for the interface, e.g. Screenshot containing the operational results.

##### 4.2.2.1.7 Ciphering of user data between the UE and the gNB

*Requirement Name:* Ciphering of user data between the UE and the gNB

*Requirement Reference:* TS 33.501 [2], clause 5.3.2

*Requirement Description:* *"The gNB shall provide ciphering of user data packets between the UE and the gNB on NG RAN air interface"* as specified in TS 33.501 [2], clause 5.3.2.

*Threat References:* TR 33.926 [5], clause D.2.2.3 – User plane data confidentiality protection at gNB

***Test Case****:*

**Test Name:** TC-UP-DATA-CIP\_gNB

**Purpose:** Toverify that the user data packets are confidentiality protected over the NG RAN air interface.

**Pre-Condition:**

- The gNB network product shall be connected in emulated/real network environments. UE may be simulated.

- The tester shall have knowledge of the ciphering algorithm and the confidentiality protection keys.

- The tester shall have access to the NG RAN air interface or can capture the message at the UE.

- Tester shall enable the user plane ciphering protection and ensure NIA0 is not used.

**Execution Steps:**

1. UE sends PDU session establishment Request to the SMF.

2. SMF sends a UP security policy with UP ciphering required or preferred to the gNB.

3. The gNB sends RRCConnectionReconfiguration with integrity protection indication "on".

4. Check any User data sent by gNB after sending RRCConnectionReconfiguration and before UE enters CM-Idle state is Integrity protected.

**Expected Results:**

The user plane packets sent between the UE and gNB after sending RRCConnectionReconfiguration is confidentiality protected.

**Expected format of evidence:**

Evidence suitable for the interface e.g. Screenshot containing the operational results.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*