**3GPP TSG-SA3 Meeting #102-e *S3-210090r1***

**e-meeting, 18 - 29 January 2021, Online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.511** | **CR** | **0019** | **rev** | **1** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | gNB Cipher Security Policy Verification | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | S3 | | | | | | | | | |
| ***Source to TSG:*** | FutureWei | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | ***Date:*** | | | 2021-07-01 |
|  |  | | | |  | |  | | |  |
| ***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 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:*** | | Test case in 4.2.2.1.10 is to verify the received cipher security policy sent by SMF is applied. Verification of the test case should involve capturing the user plane data to see if the data is ciphered according to the cipher security policy. Additionally, since the test case is a positive test case to test a UP security policy of "required", it is incorrect to check whether "UP is disabled according to the UP security policy" in Step 7. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. Add a step to capture user plane data to verify the policy is implemented.  2. Remove checking "UP is disabled" part in Step 7. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incorrect specifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.1.10 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.10 Ciphering of user data based on the security policy sent by the SMF

*Requirement Name:* Ciphering of user data based on the security policy sent by the SMF

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

*Requirement Description: "The gNB shall activate ciphering of user data based on the security policy sent by the SMF"* as specified in TS 33.501 [2], clause 5.3.2.

*Threat References:* TR 33.926 [5], clause D.2.2.8 – Security Policy Enforcement.

***Test Case****:*

**Test Name:** TC-UP-DATA-CIP-SMF

**Purpose:** Toverify that the user data packets are confidentiality protected based on the security policy sent by the SMF via AMF

**Pre-Condition:**

- The gNB network product shall be connected in emulated/real network environments. The UE and the 5GC may be simulated.

- The tester shall have access to the NG RAN air interface.

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

- RRC ciphering is already activated at the gNB.

**Execution Steps:**

1. The tester triggers PDU session establishment procedure by sending PDU session establishment request message.

2. Tester shall trigger the SMF to send the UP security policy with ciphering protection "required", “preferred”, or “not needed” to the gNB.

3. The tester shall capture the RRC connection reconfiguration procedure between gNB to UE over NG RAN air interface. And filter the RRC connection reconfiguration message sent by gNB to UE.

4. The tester shall decrypt the RRC connection Reconfiguration message and retrieve the UP ciphering protection indication presenting in the decrypted message.

5. The tester shall verify if the UP security policy received at gNB is same as the UP ciphering protection indication notified by the gNB to the UE in the RRC connection Reconfiguration message.

6. Tester shall capture the RRC connection Reconfiguration complete message sent between UE and gNB.

6a. Tester shall capture the user plane data sent between UE and gNB using any network analyser.

7. Tester shall check that the captured UP data according to the UP security policy.

**Expected Results:**

In case the UP cipher is enabled when the received UP cipher protection indication is set to “required” or “preferred”, the captured user plane data appear to be garbled (i.e. no longer plaintext) and tThe user plane packets are confidentiality protected based on the UP security policy sent by the SMF.

In case the UP cipher is disabled when the received UP cipher protection indication is set to “preferred” or “not needed”, the captured user plane data appear to be plaintext and the user plane packets are not confidentiality protected based on the UP security policy sent by the SMF.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*