**3GPP TSG-SA3 Meeting #113 *S3-234415***

**Chicago, USA, 6 - 10 November 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** | **-** | **Current version:** |  |  |
|  |
| *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 |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | To replace RRC connection reconfiguration by RRC reconfiguration |
|  |  |
| ***Source to WG:*** | ISSDU, III |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G |  | ***Date:*** | 2023-06-22 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | The message name, RRC connection reconfiguration, is incorrect.  |
|  |  |
| ***Summary of change:*** | To replace RRC connection reconfiguration in TS 33.511 by RRC reconfiguration defined by TS 38.331 |
|  |  |
| ***Consequences if not approved:*** | There is an inconsistency between between TS 33.511 and TS 38.331. |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.10 and 4.2.2.1.11 |
|  |  |
|  | **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 CHANGES \*\*\*\***

##### 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" or "not needed" to the gNB.

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

4. The tester shall decrypt the RRC 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 Reconfiguration message.

6. Tester shall capture the RRC 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 is activated/de-activated according to the UP security policy.

**Expected Results:**

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

When the received UP cipher protection indication is set to "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.

##### 4.2.2.1.11 Integrity of user data based on the security policy sent by the SMF

*Requirement Name:* Integrity 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 provide integrity protection 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-INT-SMF

**Purpose:** Toverify that the user data packets are integrity protected based on the security policy sent by the SMF.

**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 integrity algorithm and protection keys.

- RRC integrity and cipher are 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 integrity protection is "required" or "not needed" to the gNB.

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

4. The tester shall decrypt the RRC reconfiguration message and retrieve the UP integrity protection indication presenting in the decrypted message.

5. Tester shall check whether UP integrity is enabled /disabled to verify if the UP security policy received at gNB is same as the UP integrity protection indication notified by the gNB to the UE in the RRC reconfiguration message.

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

7. The tester shall check whether the user plane data packet contains a message authentication code.

**Expected Results:**

When the received UP integrity protection is set to "required", the user plane data packet contains a message authentication code and the user plane packets are integrity protected based on the security policy sent by the SMF.

When the received UP interity protection is set to "not needed", the user plane data packet message authentication code is not present and the user plane packets are not integrity protected based on the 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 \*\*\*\***