**3GPP TSG-SA3 Meeting #123 S3-252950**

Goteborg, Sweden, 25 – 29 August 2025

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.511** | **CR** | **0093** | **rev** | **1** | **Current version:** | **19.2.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Correcting the RRC replay test case to remove the UP packets text | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, MITRE | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Maint | | | | |  | ***Date:*** | | | 2025-08-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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:*** | | Sending an RRC message does not result in a UP packet being sent over the N2 interface so the current text in clause 4.2.2.1.9 is incorrect. Checking the logs is also unnecessary.  Some other clarfications to help make the test description clearer. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify that the messages on the N2 interface could be a NAS message from inside an RCC message for example.  In addition step 4 was re-worded to make it that the gNB needs to detect the replay as processing of the message is necessary to check if is a replay. Also the need to check logs was removed as unnecessary.  Step 5 is almost a repeat of step 4 so is re-worded. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Confusing test case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 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:*** | | Rev 1 deletes the checking of logs as well. | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

4.2.2.1.9 Replay protection of RRC-signalling

*Requirement Name:* Replay protection of RRC-signalling.

*Requirement Reference:* TS 33.501 [2], clause 5.3.3

*Requirement Description:* The gNB supports integrity protection and replay protection of RRC-signallingas specified in TS 33.501 [2], clause 5.3.3.

*Threat References:* TR 33.926 [5], clause D.2.2.2 – Control plane data integrity protection.

*Test Case:*

**Test Name:** TC-UP-DATA-RRC-REPLAY\_gNB

**Purpose:**

Toverify the replay protection of RRC-signalling between UE and gNB over the NG RAN air interface.

**Pre-Condition:**

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

- Tester shall have knowledge of the integrity algorithm and the corresponding protection keys.

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

- The tester shall have access to the N2 interface.

- The tester shall activate the integrity protection of RRC-signalling.

**Execution Steps:**

1. The tester shall capture the data sent between UE and the gNB using any network analyser over the NG RAN air interface.

2. Tester shall filter RRC signalling packets.

3. Tester shall check for the PDCP COUNT of the filtered RRC signalling packets and shall use any packet crafting tool to create RRC signalling packets similar to the captured packets or the tester shall replay the captured RRC uplink packet to the gNB to perform the replay attack over gNB.

4. Tester shall check whether the replayed RRC signalling packets were detected by the gNB or not, by capturing over NG RAN air interface to see if any corresponding response message is received from the gNB or by capturing the N2 interface to see if any of the replayed RRC signalling packets have resulted in a message sent by the gNB (e.g. a NAS messages from inside an RRC message).

5. Tester shall verify from the result that if the replayed RRC signalling packets are not accepted by the gNB, the RRC signalling on the NG RAN air interface is replay protected. .

**Expected Results:**

The RRC signalling over the NG RAN air interface is replay protected.

**Expected format of evidence:**

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

- Log files, e.g., containing corresponding log events.

**\*\*\*\* END OF CHANGES \*\*\*\***