**3GPP TSG-SA3 Meeting #108-e *S3-221826r1***

**e-meeting, 22 - 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | **0028** | **rev** | **1** | **Current version:** | **17.1.0** |  |
|  |
| *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:***  | Corrections for gNB test cases |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G |  | ***Date:*** | 2022-08-10 |
|  |  |  |  |  |
| ***Category:*** | **A** |  | ***Release:*** | Rel-17 |
|  | *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:*** | There are several place in the gNB test that requirement correction or clarification, e.g. missing test name that is mandatory according to TR 33.916 (clause 5.2.3.4.4) or ‘user plane’ when ‘RRC signalling’ is meant.In clause 4.2.2.18, the text case on PDCP wrap was removed (see CR 0023 to TS 33.511) but the requirement was left. Hence it is proposed that this is removed. |
|  |  |
| ***Summary of change:*** | Changes to make the needed corrections/clarifications |
|  |  |
| ***Consequences if not approved:*** | Specification is incomplete or could be read inaccurately leading to test problems. |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.4, 4.2.2.1.5, 4.2.2.1.9, 4.2.2.1.18 |
|  |  |
|  | **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:*** | Rev1 changes the WID code and CR type as it was agreed to take the changes back one release |

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

4.2.2.1.4 RRC integrity check failure

*Requirement Name*: RRC integrity check failure

*Requirement Reference:* TS 33.501 [2], clause 6.5.1

*Requirement Description*: *"The RRC integrity checks shall be performed both in the ME and the gNB. In case failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. This can happen on the gNB side or on the ME side."* as specified in TS 33.501 [2], clause 6.5.1.

*Threat References*: TR 33.926 [4], clause D.2.2.2, Control plane data integrity protection

*Test Case*:

**Test Name:** TC-CP-DATA-RRC-INT-CHECK\_gNB

**Purpose:**

Verify that RRC integrity check failure is handled correctly by the gNB.

**Pre-Conditions:**

Test environment with a UE. The UE may be simulated. RRC integrity protection is activated at the gNB.

**Execution Steps**

1a) The UE sends a RRC message to the gNB without MAC-I; or

1b) The UE sends a RRC message to the gNB with a wrong MAC-I.

2b) The gNB verifies the integrity of the RRC message from the UE.

**Expected Results:**

The RRC message is discarded by the gNB after step 1a) or after step 2b).

**Expected format of evidence:**

Sample copies of the log files.

4.2.2.1.5 UP integrity check failure

*Requirement Name*: UP integrity check failure

*Requirement Reference:* TS 33.501 [2], clause 6.6.4

*Requirement Description: "If the gNB or the UE receives a PDCP PDU which fails integrity check with faulty or missing MAC-I after the start of integrity protection, the PDU shall be discarded."* as specified in TS 33.501 [2], clause 6.6.4.

*Threat References*: TR 33.926 [4], clause D.2.2.4, User plane data integrity protection

*Test Case*:

**Test Name:** TC-UP-DATA-RRC-INT-CHECK\_gNB

**Purpose:**

Verify that UP integrity check failure is handled correctly by the gNB.

**Pre-Conditions:**

Test environment with a UE. The UE may be simulated. UP integrity protection is activated at the gNB.

**Execution Steps**

1a) The UE sends a PDCP PDU to the gNB without MAC-I; or

1b) The UE sends a PDCP PDU to the gNB with a wrong MAC-I.

2b) The gNB verifies the integrity of the PDCP PDU from the UE.

**Expected Results:**

The PDCP PDU is discarded by the gNB after step 1a) or after step 2b).

**Expected format of evidence:**

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

**\*\*\*\* NEXT CHANGE \*\*\*\***

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 shall support integrity protection and replay protection of RRC-signalling "* as 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 active 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 RRC SQN 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 processed by the gNB or not, by capturing over NG RAN air interface to see if any corresponding response message is received from the gNB.

5. Tester shall confirm that gNB provides replay protection by dropping/ignoring the replayed packet if no corresponding response is sent by the gNB to the replayed packet.

**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.

**\*\*\*\* NEXT CHANGE \*\*\*\***

4.2.2.1.18 Key update at the gNB on dual connectivity

*Requirement Name*: Key update at the gNB on dual connectivity

*Requirement Reference:* TS 33.501 [2], clause 6.10.2.1; clause 6.10.2.2.1;clause 6.10.3.1.

*Requirement Description*: "When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN shall, for each new radio bearer, assign a radio bearer identity that has not previously been used since the last KSN change. If the MN cannot allocate an unused radio bearer identity for a new radio bearer in the SN, due to radio bearer identity space exhaustion, the MN shall increment the SN Counter and compute a fresh KSN, and then shall perform a SN Modification procedure to update the KSN" as specified in TS 33.501 [2], clause 6.10.2.1.

"The MN shall refresh the root key of the 5G AS security context associated with the SN Counter before the SN Counter wraps around. Refreshing the root key is done using intra cell handover as described in subclause 6.7.3.3 of the present document. When the root key is refreshed, the SN Counter is reset to '0' as defined above." as specified in TS 33.501 [2], clause 6.10.3.1.

NOTE: The following testcases are only tested when the NR-NR DC, NE-DC and EN-DC scenarios are deployed.

*Threat References*: TR 33.926 [5], clause D.2.2.7 Key Reuse

*Test Case 1:*

**Test Name:** TC\_GNB\_DC\_KEY\_UPDATE\_DRB\_ID

**Purpose:**

Verify that the gNB under test acting as a Master Node (MN) performs KSN update when DRB-IDs are about to be reused.

**Pre-Conditions:**

- Test environment with a gNB or ng-eNB acting as the Secondary Node (SN), which may be simulated

- Test environment with a UE, SMF and AMF, which may be simulated

**Execution Steps**

1. The gNB under test establishes RRC connection and AS security context with the UE.

2. The gNB under test establishes security context between the UE and the SN for the given AS security context shared between the gNB under test and the UE; and generates a KSN sent to the SN.

3. A SCG bearer is set up between the UE and the SN.

4. The gNB under test is triggered to execute the SN Modification procedure to provide additional available DRB IDs to be used for SN terminated bearers (e.g. by the UE making multiple IMS calls, or by the SMF requesting PDU session modification and deactivation via the AMF), until the DRB IDs are reused.

**Expected Results:**

- Before DRB ID reuse, the gNB under test generates a new KSN and sends it via the SN Modification Request message to the SN.

**Expected format of evidence:**

Evidence suitable for the interface, e.g. text representation of the captured SN Modification Request message.

*Test Case 2*:

**Test Name: TC\_GNB\_DC\_KEY\_UPDATE\_SN\_COUNTER**

**Purpose:**

Verify that the gNB under test acting as a Master Node (MN) performs KNG-RAN( AS root key) update when SN COUNTER is about to wrap around.

**Pre-Conditions:**

- Test environment with a gNB or ng-eNB acting as the Secondary Node (SN), which may be simulated

- Test environment with a UE, SMF and AMF, which may be simulated.

**Execution Steps**

1. The gNB under test establishes RRC connection and AS security context with the UE.

2. The gNB under test establishes security context between the UE and the SN for the given AS security context shared between the gNB under test and the UE; and generates a KSN sent to the SN and increases the value of SN Counter.

3. A SCG bearer is set up between the UE and the SN.

4. The gNB under test is triggered to execute the SN Modification procedure to provide updated KSN to SN, until the SN Counter value wraps around.

**Expected Results:**

- Before SN Counter wraps around, the gNB under test takes a new KNG-RAN into use by e.g. triggering an intra-cell handover or triggering a transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED.

**Expected format of evidence:**

Part of log that shows the SN Counter values before and after wrapping around and the intra-cell handover or the transition from RRC\_CONNECTED to RRC\_IDLE or RRC\_INACTIVE and then back to RRC\_CONNECTED. This part can be presented, for example, as a screenshot.

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