**3GPP TSG-SA3 Meeting #123 S3-253024**

Goteborg, Sweden, 25 – 29 August 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | **Draft CT** | **rev** | **-** | **Current version:** | **19.2.0** |  |
|  |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at http://www.3gpp.org/Change-Requests.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |
| --- |
|  |
| ***Title:***  | Living document for TS 33.511 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon,BSI (DE), China Telecom, CAICT |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5GA |  | ***Date:*** | 2025-07-29 |
|  | D |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-20 |
|  | *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. | *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:*** | S3-252703Correction of referencesS3-253028The abbreviation "SMP" and "SMC" is not defined in 33.511 and may cause ambiguity. |
|  |  |
| ***Summary of change:*** | S3-252703Correction of referencesS3-253028Change "SMP" to “security mode complete message”, "SMC" to “security mode command message”. |
|  |  |
| ***Consequences if not approved:*** | S3-252703Test case without correct references remains and test automation may be affectedS3-253028There is ambiguity in the understanding of "SMP" and "SMC". |
|  |  |
| ***Clauses affected:*** | 4.2.2.1.1, 4.2.2.1.5, 4.2.2.1.6, 4.2.2.1.11, 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:*** | The merger of S3-252703, S3-253028 |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.1 Integrity protection of RRC-signalling

*Requirement Name:* Integrity 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-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\_CP\_DATA\_INT\_RRC-SIGN\_gNB

**Purpose:**

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

**Pre-Condition:**

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

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

- The tester can capture the message via the NG RAN air interface, or can capture the message at the UE.

- The NIA0 is disabled at UE and gNB.

**Execution Steps:**

1. The tester triggers the gNB to send AS security mode command message to the UE, and UE responses AS security mode complete message.

2. The tester checks any RRC message sent by gNB after sending AS security mode command message and before UE enters CM-Idle state is integrity protected.

**Expected Results:**

Any RRC-signalling over the NG RAN air interface is integrity protected after gNB sending AS security mode command message.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

4.2.2.1.5 UP integrity check failure

*Requirement Name*: UP integrity check failure

*Requirement Reference:* TS 33.501 [2], clause 6.6.4.2

*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 is discarded as specified in TS 33.501 [2], clause 6.6.4.2.

*Threat References*: TR 33.926 [5], clause D.2.2.4, User plane data integrity protection

*Test Case*:

**Test Name:** TC\_GNB\_UP\_INTEGRITY\_CHECK\_FAIL

**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**

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

or

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

NOTE: In a PDCP PDU message without MAC-I, the last 4 Bytes of the PCDP PDU Data will be interpreted as a wrong MAC-I and therefore the integrity check will fail.

**Expected Results:**

The PDCP PDU is discarded by the gNB.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 3rd 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 supports ciphering of RRC-signalling 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. The UE may be simulated.

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

**Execution Steps:**

1. The tester triggers the UE to send a Registraton Request to the AMF.

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

3. The gNB selects an algorithm and sends AS security mode command message to the UE.

4. The gNB receives AS security mode complete message from the UE.

**Expected Results:**

Control plane packets sent to the UE after the gNB sends AS security mode command message is ciphered.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\* END OF 3rd CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 4th CHANGE \*\*\*\*\*\*\*\*\*\*

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 5.3.3

*Requirement Description:* *The gNB activates integrity protection of user data based on the security policy sent by the SMF* as specified in TS 33.501 [2], clause 5.3.3.

*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 activation of integrity protection for user data packets is 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 is activated at the gNB.

**Execution Steps:**

All execution steps are to be performed two times. Once with the UP security policies’ ciphering protection in step 2 set to "required" and the second time set to "not needed".

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.

**Expected Results:**

When the received UP integrity protection is set to "required", the user plane packets are integrity protected based on the security policy sent by the SMF.

When the received UP integrity protection is set to "not needed", 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 4th CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 5th 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 6.10.3.1.

*Requirement Description*: When executing the procedure for adding subsequent radio bearer(s) to the same SN, the MN is expected to, 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 is expected to increment the SN Counter and compute a fresh KSN, and then is expected to perform a SN Modification procedure to update the KSN as specified in TS 33.501 [2], clause 6.10.2.1.

The MN is expected to 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 TS 33.501 [2]. When the root key is refreshed, the SN Counter is reset to '0' as defined above. in that same clause; 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 tester triggers the gNB under test to establish 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 tester triggers the gNB under test to execute the SN Modification procedure to provide additional available DRB IDs to be used for SN terminated bearers (e.g. by triggering the UE to make multiple IMS calls, or by triggering the SMF to request 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 tester triggers the gNB under test to establish 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 tester triggers the gNB under test 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.

NOTE: Random Access Procedure defined in clause 9.2.6 of TS 38.300[8] runs in the above procedures.

**Expected format of evidence:**

Part of log that shows the SN Counter values before and after wrapping around and the corresponding procedure. This part can be presented, for example, as a screenshot.

\*\*\*\*\*\*\*\*\*\* END OF 5th CHANGE \*\*\*\*\*\*\*\*\*\*

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