**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 - 26 May 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **17.3.1** |  |
|  |
| *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:***  | SCAS release reference corrections |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** | 2023-05-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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:*** | SA3 has been adding the release numbers explicitly to any of the references pertaining to the network function targeted by the SCAS work, for example reference 2 in TS 33.511. This is because the SCAS work has always been one "release late" since it is challenging to develop the SCAS requirements and tests in parallel to targeted new features within the same release timeline. The references have not been regularly updated and some SCAS specifications include more than one reference to the same specification, for example references 2 and 7 in TS 33.512. This practice is neither future proof nor it is documented anywhere. Furthermore, for SCAS evaluation of network products, this dependency on previous releases in SCAS documents turned out to be not very useful anyway. This issue has been discussed several times in previous SA3 meetings and the proposed resolution is documented in [S3-231050](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_110_Athens/docs/S3-231050.zip). |
|  |  |
| ***Summary of change:*** | Removal of the release number from the relevant references and minor reformulations to avoid verbatim content copies from other specifications |
|  |  |
| ***Consequences if not approved:*** | Unnecessary dependencies on previous releases and risk for confusion on scope of SCAS specifications |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.1.4, 4.2.2.1.10, 4.2.2.1.16, 4.2.2.1.17, 4.2.2.1.18, 4.2.2.1.19 |
|  |  |
|  | **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\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[4] Void

[5] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[6] 3GPP TS 38.331: "NR; Radio Resource Control (RRC) protocol specification".

\*\*\*\* Next 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 are expected to 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 is expected to 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 [5], 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.

\*\*\*\* Next 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 is expected to 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 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 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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.1.16 Control plane data confidentiality protection over N2/Xn interface

*Requirement Name:* Control plane data confidentiality protection over N2/Xn interface

*Requirement Reference:* TS 33.501 [2], clauses 9.2 and 9.4

*Requirement Description:* The transport of control plane data over N2 is expected to be integrity, confidentiality and replay-protected. The transport of control plane data and user data over Xn is expected to be integrity, confidentiality and replay-protected; as specified in TS 33.501 [2], clauses 9.2 and 9.4.

*Threat References:* TR 33.926 [5], clause D.2.2.1 – Control plane data confidentiality protection.

*Test Case:* the test case in clause 4.2.3.2.4 of TS 33.117 [3]

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.1.17 Control plane data integrity protection over N2/Xn interface

*Requirement Name:* Control plane data integrity protection over N2/Xn interface

Requirement Reference: TS 33.501[2], clauses 9.2 and 9.4

*Requirement Description:* The transport of control plane data over N2 is expected to be integrity, confidentiality and replay-protected. The transport of control plane data and user data over Xn is expected to be integrity, confidentiality and replay-protected*;* as specified in TS 33.501 [2], clauses 9.2 and 9.4.

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

*Test Case:* the test case in clause 4.2.3.2.4 of TS 33.117 [3].

\*\*\*\* Next Changes\*\*\*\*

##### 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 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 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.

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.1.19 UP security activation in Inactive scenario

*Requirement Name*: UP security activation in Inactive scenario

*Requirement Reference:* TS 33.501 [2], clause 6.8.2.1.3.

*Requirement Description*: If the UP security activation status can be supported in the target gNB/ng-eNB, the target gNB/ng-eNB is expected to use the UP security activations that the UE used at the last source cell. Otherwise, the target gNB/ng-eNB is expected to respond with an RRC Setup message to establish a new RRC connection with the UE as specified in TS 33.501 [2], clause 6.8.2.1.3.

*Threat Reference*: TR 33.926 [5], clause D.2.2.9 State transition from inactive state to connected state.

**Test Name:** TC\_GNB\_INACTIVE\_TO\_ACTIVE

 **Purpose:**

Verify that the target gNB/ng-eNB uses the UP security activation status to activate the UP security.

**Pre-Conditions:**

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

- The UE may be simulated.

**Execution Steps**

1. The tester shall complete a Registration Procedure and PDU Session establishment procedure to make sure the gNB configure the UP security, and get the UP security activation status.

2. The gNB sends RRC Release message with a suspend config to the UE.

3. The tester deletes the UP security activation status of the UE.

4. The tester triggers the UE to send RRC Resume message.

**Expected Results:**

The gNB sends RRC Setup message to the UE.

**Expected format of evidence:**

Screenshot containing the operational results.

\*\*\*\* End of Changes\*\*\*\*