**3GPP TSG-SA3 Meeting #111 *S3-233339***

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

|  |
| --- |
| *CR-Form-v12.1* |
|  **Draft CHANGE REQUEST** |
|  |
|  | **33.511** | **CR** | **draftCR** | **rev** | **1** | **Current version:** | **17.3.0** |  |
|  |
| *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:***  | Changes for SCAS gNB for Rel18  |
|  |  |
| ***Source to WG:*** | Keysight Technologies UK |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** | 2023-05-12 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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:*** |  Update the test cases to the new specifications of Rel-17.  |
|  |  |
| ***Summary of change:*** | Update the references and the redaction of the test case for Rel-17 |
|  |  |
| ***Consequences if not approved:*** | The test cases does not follow the correct requirements of Release 17 |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.1.1, 4.2.2.1.2, 4.2.2.1.5, 4.2.2.1.6, 4.2.2.1.7, 4.2.2.1.8, 4.2.2.1.9, 4.2.2.1.11, 4.2.2.1.12, 4.2.2.1.13, 4.2.2.1.14, 4.2.2.1.15, 4.2.2.1.18, 4.2.2.1.19, 4.2.2.1.X (new), 4.2.2.1.Y (new), 4.4 |
|  |  |
|  | **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:*** | draftCR |
|  |  |
| ***This draftCR's revision history:*** | SA3#109: S3-223933SA3#110: S3-230648SA3#111: S3-233261 S3-232434 |

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

# 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] 3GPP TS 33.216: "Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class".

[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".

[Y] 3GPP TS 23.501: "System Architecture for 5G System (5GS)".

[Z] 3GPP TS 38.300: "NR and NG-RAN Overall Description".

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

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

##### 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

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.2 Integrity protection of user data between the UE and the gNB

*Requirement Name:* Integrity protection of user data between the UE and the gNB.

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

*Requirement Description:* The gNB supports integrity protection and replay protection of user data between the UE and the gNB as specified in TS 33.501 [2], clause 5.3.3.

NOTE: This requirement does not apply to the gNB that is used as a secondary node connecting to the EPC.

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

***Test Case****:*

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

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

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

##### 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*:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 4 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 5 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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 UE sends 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 SMC to the UE.

4. The gNB receive AS SMP from the UE.

**Expected Results:**

Control plane packets sent to the UE after the gNB sends AS SMC is ciphered.

**Expected format of evidence:**

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

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 6 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.7 Ciphering of user data between the UE and the gNB

*Requirement Name:* Ciphering of user data between the UE and the gNB

*Requirement Reference:* TS 33.501 [2], clause 5.3.2

*Requirement Description:* The gNB supports ciphering of user data between the UE and the gNB. as specified in TS 33.501 [2], clause 5.3.2.

*Threat References:* TR 33.926 [5], clause D.2.2.3 – User plane data confidentiality protection at gNB

***Test Case****:*

**Test Name:** TC-UP-DATA-CIP\_gNB

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 6 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 7 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.8 Replay protection of user data between the UE and the gNB

*Requirement Name:* Replay protection of user data between the UE and the gNB.

*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.2.2.4 – User plane data integrity protection.

***Test Case****:*

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 7 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 8 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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-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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 8 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 9 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 9 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 10 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.12 AS algorithms selection

*Requirement Name*: AS algorithms selection

*Requirement Reference:* TS 33.501 [2], clause 6.7.3.0 and clause 5.11.2.

*Requirement Description*:The serving network selects the algorithms to use dependent on: the UE security capabilities of the UE, the configured allowed list of security capabilities of the currently serving network entity as specified in TS 33.501 [2], clause 5.11.2.

Each gNB/ng-eNB is configured via network management with lists of algorithms which are allowed for usage. There is one list for integrity algorithms, and one for ciphering algorithms. These lists are ordered according to a priority decided by the operator as specified in TS 33.501 [2], clause 6.7.3.0.

*Threat References*: TR 33.926 [5], D.2.2.5 – AS algorithm selection and use

*Test Case*:

Test Name: TC-AS-alg-select\_gNB

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 11 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 12 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.13 Key refresh at the gNB

*Requirement Name*: Key refresh at the gNB

*Requirement Reference:* TS 33.501 [2], clause 6.9.4.1; TS 38.331 [6], clause 5.3.1.2

*Requirement Description*: Key refresh is possible for KgNB, KRRC-enc, KRRC-int, KUP-enc, and KUP-int (if available) and is to be initiated by the gNB/ng-eNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same KgNB as specified in TS 33.501 [2], clause 6.9.4.1.

The network is responsible for avoiding reuse of the COUNT with the same RB identity and with the same key, e.g. due to the transfer of large volumes of data, release and establishment of new RBs, and multiple termination point changes for RLC-UM bearers and multiple termination point changes for RLC-AM bearer with SN terminated PDCP re-establishment (COUNT reset) due to SN only full configuration whilst the key stream inputs (i.e. bearer ID, security key) at MN have not been updated. In order to avoid such re-use, the network e.g. uses different RB identities for RB establishments, change the AS security key, or an RRC\_CONNECTED to RRC\_IDLE/RRC\_INACTIVE and then to RRC\_CONNECTED transition as specified in TS 38.331 [6], clause 5.3.1.2.

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

*Test Case:*

**Test Name:** TC\_GNB\_KEY\_REFRESH\_DRB\_ID

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 12 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 13 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.14 Bidding down prevention in Xn-handovers

*Requirement Name*: Bidding Down Prevention

*Requirement Reference:* TS 33.501 [2], clause 6.7.3.1

*Requirement Description*: In the Path-Switch message, the target gNB/ng-eNB sends the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. as specified in TS 33.501 [2], clause 6.7.3.1

*Threat References*: TR 33.926 [5], clause D.2.2.6 Bidding Down on Xn-Handover

*Test Case*:

Test Name: TC-Xn-handover\_bid\_down\_gNB

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 13 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 14 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.15 AS protection algorithm selection in gNB change

*Requirement Name*: AS protection algorithm selection in gNB change.

*Requirement Reference:* TS 33.501 [2], clauses 6.7.3.1 and 6.7.3.2

*Requirement Description*: The target gNB/ng-eNB selects the algorithm with highest priority from the received 5G security capabilities of the UE according to the prioritized locally configured list of algorithms (this applies for both integrity and ciphering algorithms).The chosen algorithms are indicated to the UE in the Handover Command message if the target gNB/ng-eNB selects different algorithms compared to the source gNB/ng-eNB as specified in TS 33.501 [2], clause 6.7.3.1, and clause 6.7.3.2.

*Threat References*: TR 33.926 [5], D.2.2.5 – AS algorithm selection and use

*Test Case*:

Test Name: Alg\_select\_change\_gNB

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 14 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 15 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.2.1.X User plane data confidentiality protection over N3/Xn interface

*Requirement Name:* User plane data confidentiality protection over N3/Xn interface

*Requirement Reference:* TS 33.501 [2], clauses 9.3 and 9.4

*Requirement Description:* The transport of user data over N3 is integrity, confidentiality and replay-protected.

The transport of control plane data and user data over Xn is integrity, confidentiality and replay-protected as specified in TS 33.501 [2], clauses 9.3 and 9.4.

*Threat References:* TR 33.926 [5], clause D.2.2.3 – User plane data confidentiality protection at gNB.

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

##### 4.2.2.1.Y User plane data integrity protection over N3/Xn interface

*Requirement Name:* User plane data integrity protection over N3/Xn interface

Requirement Reference: TS 33.501[2], clauses 9.3 and 9.4

*Requirement Description:* The transport of user data over N3 is integrity, confidentiality and replay-protected.

The transport of control plane data and user data over Xn is integrity, confidentiality and replay-protected as specified in TS 33.501 [2], clauses 9.3 and 9.4.

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

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 15 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGE 16 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

4.4 gNodeB-specific adaptations of basic vulnerability testing requirements and related test cases

## 4.4.1 Introduction

There are no gNB specific addtions to clause 4.4.1 of TS 33.117 [3].

### 4.4.2 Port Scanning

There are no gNB specific addtions to clause 4.4.2 of TS 33.117 [3].

### 4.4.3 Vulnerability scanning

There are no gNB specific addtions to clause 4.4.3 of TS 33.117 [3].

### 4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [3] are applicable to gNB.

The interfaces defined for the gNB are in clause 4.2.3 of TS 23.501 [Y] and in clause 4.1 of TS 38.300 [Z].

According to clause 4.4.4 of TS 33.117 [3], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for gNB, the following interfaces and protocols are in the scope of the testing:

* For N2: the SCTP and NGAP procotols.
* For N3: the UDP and GTP-U protocols.
* For Xn: the SCTP and XnAP protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 of TS 33.117 [3]

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGE 16 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*