ETSI TS 133 511 V17.3.1 (2023-02)

5G;
Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (3GPP TS 33.511 version 17.3.1 Release 17)

Reference
RTS/TSGS-0333511vh31

Keywords
5G,SECURITY

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document contains objectives, requirements and test cases that are specific to the gNB network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases given there, as well as specifying requirements and test cases unique to the gNB network product class.

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 (Release 15): "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".

3 Definitions of terms and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC	5G Core Network
AMF	Access and Mobility Management Function
gNB	NR Node B
NG	Next Generation
NG-RAN	5G Radio Access Network
SMF	Session Management Function

4 gNodeB-specific security requirements and related test cases

4.1 Introduction

gNB specific security requirements include both requirements derived from gNB-specific security functional requirements as well as security requirements derived from threats specific to gNB as described in TR 33.926 [5]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [3] and are not repeated in the present document.

4.2 gNodeB-specific security functional adaptations of requirements and related test cases

4.2.1 Introduction

Present clause contains gNB-specific security functional adaptations of requirements and related test cases.

4.2.2 Security functional requirements on the gNodeB deriving from 3GPP specifications and related test cases

4.2.2.1 Security functional requirements on the gNodeB deriving from 3GPP specifications – TS 33.501 [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 shall support integrity protection of RRC-signalling over the NG RAN air interface" 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: To verify 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.

Execution Steps:

1. The NIA0 is disabled at UE and gNB.
2. gNB sends AS SMC message to the UE, and UE responses AS SMP.
3. Check any RRC message sent by gNB after sending AS SMC 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 SMC.

Expected format of evidence:

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

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 shall support integrity protection of user data packets over the NG RAN air interface" 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

Purpose: To verify that the user data packets are integrity protected over the NG RAN air interface.

Pre-Condition:

- The gNB network product shall be connected in emulated/real network environments. UE may be simulated.
- Tester shall enable the user plane integrity protection and ensure NIA0 is not used.
- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the NG RAN air interface, or can capture the message at the UE.

Execution Steps:

1. The NIA0 is disabled at UE and gNB.
2. gNB sends RRCConnectionReconfiguration with integrity protection indication "on".
3. Check any User data sent by gNB after sending RRCConnectionReconfiguration and before UE enters CM-Idle state is Integrity protected.

Expected Results:

Any user plane packets sent between UE and gNB over the NG RAN air interface after gNB sending RRCConnectionReconfiguration is integrity protected.

Expected format of evidence:

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

4.2.2.1.3 VOID

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 [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.

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 [5], clause D.2.2.4, User plane data integrity protection

Test Case:

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.

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 shall support ciphering of RRC-signalling over the NG RAN air interface" 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: To verify 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.

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 shall provide ciphering of user data packets between the UE and the gNB on NG RAN air interface" 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

Purpose: To verify that the user data packets are confidentiality protected over the NG RAN air interface.

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 PDU session establishment Request to the SMF.
2. The SMF sends a UP security policy with UP ciphering required or preferred to the gNB.

3. The gNB sends RRCConnectionReconfiguration with ciphering protection indication "on".

4. Check any user data sent by the gNB after sending RRCConnectionReconfiguration and before the UE enters into CM-Idle state.

Expected Results:

The user plane packets sent to the UE after the gNB sends RRCConnectionReconfiguration is confidentiality protected.

Expected format of evidence:

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

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 shall support 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.

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

Purpose: To verify that the user data packets are replay protected over the NG RAN air interface.

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.
- The tester shall active the user plane integrity protection of the RRC-signalling packets.

Execution Steps:

1. The tester shall capture the user plane data sent between UE and gNB using any network analyser over the NG RAN air interface.
2. Tester shall filter user plane data packets sent between UE and gNB.
3. Tester shall replay the captured user plane packets or shall use any packet crafting tool to create a user plane packet similar to the captured user plane packet and replay to the gNB.
4. Tester shall check whether the replayed user plane packets were processed by the gNB 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 received from the gNB to the replayed packet.
6. Tester shall verify from the result that if the replayed user plane packets are not accepted by gNB, the NG RAN air interface is replay protected.

Expected Results:

The user plane packets sent between the UE and gNB over the NG air interface is replay protected.

Expected format of evidence:

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

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: To verify 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.

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 shall 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: To verify 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.

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 5.3.2

Requirement Description: "The gNB shall provide integrity protection 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-INT-SMF

Purpose: To verify that the user data packets are integrity protected 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 and cipher are 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 integrity protection is "required" or "not needed" to the gNB.
3. The tester shall capture the RRC connection reconfiguration message sent by gNB to UE over NG RAN air interface.
4. The tester shall decrypt the RRC connection 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 connection reconfiguration message.
6. Tester shall capture the user plane data sent between UE and gNB using any network analyser.
7. The tester shall check whether the user plane data packet contains a message authentication code.

Expected Results:
When the received UP integrity protection is set to "required", the user plane data packet contains a message authentication code and the user plane packets are integrity protected based on the security policy sent by the SMF.

When the received UP interity protection is set to "not needed", the user plane data packet message authentication code is not present and 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.

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 shall select 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 shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be 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

Purpose:

Verify that the gNB selects the algorithms with the highest priority in its configured list.

Pre-Conditions:

Test environment with the gNB has been pre-configured with allowed security algorithms with priority.

Execution Steps

1) The UE sends registration request message to the gNB.
2) The gNB receives UE context setup request message.
3) The gNB sends the AS SECURITY MODE COMMAND message.
4) The UE replies with the AS SECURITY MODE COMPLETE message.

Expected Results:

The gNB initiates the SECURITY MODE COMMAND message that includes the chosen algorithm with the highest priority according to the ordered lists and is contained in the UE NR security capabilities.

The MAC in the AS SECURITY MODE COMPLETE message is verified, and the AS protection algorithms are selected and applied correctly.

Expected format of evidence:

Sample copies of the log files.

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 shall be possible for K_{gNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-int}, and K_{UP-enc} and shall be initiated by the gNB when a PDCP COUNTs are about to be re-used with the same Radio Bearer identity and with the same K_{gNB}."* 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. In order to avoid such re-use, the network may e.g. use 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

Purpose:

Verify that the gNB performs K_{gNB} refresh when DRB-IDs are about to be reused under the following conditions:

- the successive Radio Bearer establishment uses the same RB identity while the PDCP COUNT is reset to 0, or
- the PDCP COUNT is reset to 0 but the RB identity is increased after multiple calls and wraps around.

Pre-Conditions:

The UE, AMF and SMF may be simulated.

Execution Steps

1) The gNB sends the AS Security Mode Command message to the UE.

2) The UE responds with the AS Security Mode Complete message.

3) A DRB is set up.

4) DRB is set up and torn down for multiple times within one active radio connection without the UE going to idle (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 ID is reused.

Expected Results:

Before DRB ID reuse, the gNB takes a new K_{gNB} 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 all the DRB identities 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.

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 g_{NB} shall send the UE's 5G security capabilities, UP security policy with corresponding PDU session ID received from the source gNB 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

Purpose:

Verify that bidding down is prevented in Xn-handovers.

Pre-Conditions:

Test environment with source gNB and target gNB, and the source gNB may be simulated.

Execution Steps:

The target gNB sends the path-switch message to the AMF.

Expected Results:

The UE NR security capabilities are in the path-switch message.

Expected format of evidence:

Snapshots containing the result.

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 shall select the algorithm with highest priority from the UE's 5G security capabilities according to the locally configured prioritized list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the Handover Command message if the target gNB selects different algorithms compared to the source gNB "* 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

Purpose:

Verify that AS protection algorithm is selected correctly.

Pre-Conditions:

Test environment with source gNB, target gNB and AMF. Source gNB and AMF may be simulated.

Execution Steps:

Test Case 1:

Source gNB transfers the ciphering and integrity algorithms used in the source cell to the target gNB in the handover request message.

Target gNB verifies the algorithms and selects AS algorithms which have the highest priority according to the ordered lists. Target gNB includes the algorithm in the handover command.

Test Case 2:

AMF sends the UE NR security capability to the Target gNB.

The target gNB selects the AS algorithms which have the highest priority according to the ordered lists in the HANDOVER COMMAND.

The above test cases assume that the algorithms selected by the target gNB are different from the ones received from the source gNB.

Expected Results:

For both test cases:

1. The UE checks the message authentication code on the handover command message.
2. The MAC in the handover complete message is verified, and the AS integrity protection algorithm is selected and applied correctly.

Expected format of evidence:

Snapshots containing the result.

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 shall be integrity, confidentiality and replay-protected." "The transport of control plane data and user data over Xn shall 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]

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 shall be integrity, confidentiality and replay-protected." "The transport of control plane data and user data over Xn shall 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].

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 K_{SN} 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 K_{SN}, and then shall perform a SN Modification procedure to update the K_{SN}" 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 K_{SN} 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 K_{SN} 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 K_{SN} 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 K_{NG-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 K_{SN} 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 K_{SN} to SN, until the SN Counter value wraps around.

Expected Results:

- Before SN Counter wraps around, the gNB under test takes a new K_{NG-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.

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 shall use the UP security activations that the UE used at the last source cell. Otherwise, the target gNB/ng-eNB shall 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.

4.2.3 Technical Baseline

4.2.3.1 Introduction

The present clause provides baseline technical requirements.

4.2.3.2 Protecting data and information

4.2.3.2.1 Protecting data and information – general

There are no gNB-specific additions to clause 4.2.3.2.1 of TS 33.117 [3].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no gNB-specific additions to clause 4.2.3.2.2 of TS 33.117 [3].

4.2.3.2.3 Protecting data and information in storage

There are no gNB-specific additions to clause 4.2.3.2.3 of TS 33.117 [3].

4.2.3.2.4 Protecting data and information in transfer

There are no gNB-specific additions to clause 4.2.3.2.4 of TS 33.117 [3].

4.2.3.2.5 Logging access to personal data

The requirement and testcase in clause 4.2.3.2.5 of TS 33.117 [3] are not applicable to the gNB network products.

4.2.3.3 Protecting availability and integrity

There are no gNB-specific additions to clause 4.2.3.3 of TS 33.117 [3].

4.2.3.4 Authentication and authorization

4.2.3.4.1 Authentication attributes

gNB-specific adaptation to clause 4.2.3.4.2.1 of TS 33.117 [2] is:

Dual-factor authentication by combining several authentication options as noted in clause 4.2.3.4.2.1 of TS 33.117 [2] for higher level of security is not applicable to the gNB.

Apart from the above exception, there are no other gNB-specific adaptations to clause 4.2.3.4.2 of TS 33.117 [3].

4.2.3.5 Protecting sessions

There are no gNB-specific additions to clause 4.2.3.5 of TS 33.117 [3].

4.2.3.6 Logging

There are no gNB-specific additions to clause 4.2.3.6 of TS 33.117 [3].

4.2.4 Operating systems

The gNB-specific additions to clause 4.2.4 of TS 33.117 [3] are:

For the requirement defined in clause 4.2.4.1.1.2 Handling of ICMP of TS 33.117[3]:

- Echo Reply can be sent by default.
- In case of remote base station auto deployment, Router Advertisement can be processed. Apart from the above exceptions, there are no gNB-specific additions to clause 4.2.4 of TS 33.117 [3].

4.2.5 Web servers

There are no gNB-specific additions to clause 4.2.5 of TS 33.117 [3].

4.2.6 Network devices

4.2.6.1 Protection of data and information

There are no gNB-specific additions to clause 4.2.6 of TS 33.117 [3].

4.2.6.2 Protecting availability and integrity

4.2.6.2.1 Packet filtering

There are no gNB-specific additions to clause 4.2.6.2.1 of TS 33.117 [3].

4.2.6.2.2 Interface robustness requirements

There are no gNB-specific additions to clause 4.2.6.2.2 of TS 33.117 [3].

4.2.6.2.3 GTP-C Filtering

The requirement and testcase in clause 4.2.6.2.3 of TS 33.117 [3] is not applicable to gNB network products.

4.2.6.2.4 GTP-U Filtering

There are no gNB-specific additions to clause 4.2.6.2.4 of TS 33.117 [3].

4.2.7 Void

4.3 gNodeB-specific adaptations of hardening requirements and related test cases.

4.3.1 Introduction

The present clause contains gNB-specific adaptations of hardening requirements and related test cases.

4.3.2 Technical Baseline

There are no gNB-specific additions to clause 4.3.2 of TS 33.117 [3].

4.3.3 Operating Systems

There are no gNB-specific additions to clause 4.3.3 of TS 33.117 [3].

4.3.4 Web Servers

There are no gNB-specific additions to clause 4.3.4 of TS 33.117 [3].

4.3.5 Network Devices

There are no gNB-specific additions to clause 4.3.5 of TS 33.117 [3].

4.3.6 Network Functions in service-based architecture

The requirements and test cases in clause 4.3.6 of TS 33.117 [3] are not applicable to the gNB network products.

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

There are no gNB-specific additions to clause 4.4 of TS 33.117 [3].

Annex A (informative): Change history

Change history							
Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2019-06	SA#84					Upgrade to change control version	16.0.0
2019-09	SA#85	SP-190688	0001	-	F	Add abbreviation and correct references	16.1.0
2019-09	SA#85	SP-190688	0002	1	F	Editorial corrections on the threat references of some test cases	16.1.0
2019-09	SA#85	SP-190688	0003	1	F	Update requirements and test cases for gNB SCAS	16.1.0
2019-09	SA#85	SP-190688	0005	-	F	Correction to test case requirement reference	16.1.0
2019-12	SA#86	SP-191138	0006	-	F	Adding the expected evidence	16.2.0
2019-12	SA#86	SP-191138	0007	1	F	Update testcases for gNB SCAS	16.2.0
2019-12	SA#86	SP-191138	0008	-	F	Fix the reference numbers	16.2.0
2019-12	SA#86	SP-191138	0010	1	F	Corrections for clean-up and alignment	16.2.0
2020-03	SA#87E	SP-200136	0011	1	B	Complete the test cases of key refresh at the gNB	16.3.0
2020-03	SA#87E	SP-200136	0012	-	B	A new test case for key update at the gNB on dual connectivity	16.3.0
2020-07	SA#88E	SP-200358	0013	1	F	Update testcase in gNB SCAS	16.4.0
2020-07	SA#88E	SP-200358	0014	1	F	Remove mismatched threat references and test steps	16.4.0
2020-09	SA#89E	SP-200703	0015	-	F	gNB-specific adaptation to account protection by authentication attribute	16.5.0
2021-03	SA#91e	SP-210117	0019	1	F	gNB Cipher Security Policy Verification	16.6.0
2021-03	SA#91e	SP-210117	0020	1	F	gNB Integrity Security Policy Verification	16.6.0
2021-06	SA#92e	SP-210446	0021	-	F	Editorial correction in clause 4.2.2.1.5	16.7.0
2021-06	SA#92e	SP-210446	0023	1	F	Update conditions of testcases	16.7.0
2021-06	SA#92e	SP-210440	0024	-	B	CR to include R-16 feature of gNB to 33.511	17.0.0
2021-12	SA#94e	SP-211371	0026	1	F	Update testcases to clause 4.2.2.1.18 and 4.2.2.1.19	17.1.0
2022-09	SA#97e	SP-220887	0032	-	A	Corrections for gNB test cases	17.2.0
2022-12	SA#98e	SP-221148	0035	-	A	Corrections to the test cases in TS 33.511	17.3.0
2022-12	SA#98e	SP-221148	0037	-	A	Corrections to the threat references in TS 33.511	17.3.0
2023-02						Refreshing table of contents	17.3.1

History

Document history		
V17.1.0	May 2022	Publication
V17.2.0	September 2022	Publication
V17.3.0	January 2023	Publication (withdrawn)
V17.3.1	February 2023	Publication