ETSI TS 133 511 V17.6.0 (2024-04)

5G;
Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (3GPP TS 33.511 version 17.6.0 Release 17)

Reference
RTS/TSGS-0333511vh60

Keywords
5G

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 https://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

Intellectual Property Rights 2
Legal Notice 2
Modal verbs terminology 2
Foreword 5
1 Scope 6
2 References 6
3 Definitions of terms and abbreviations 6
3.1 Terms 6
3.2 Abbreviations 6
4 gNodeB-specific security requirements and related test cases 7
4.1 Introduction 7
4.2 gNodeB-specific security functional adaptations of requirements and related test cases 7
4.2.1 Introduction 7
4.2.2 Security functional requirements on the gNodeB deriving from 3GPP specifications and related test cases 7
4.2.2.1 Security functional requirements on the gNodeB deriving from 3GPP specifications – TS 33.501 [2] 7
4.2.2.1.1 Integrity protection of RRC-signalling 7
4.2.2.1.2 Integrity protection of user data between the UE and the gNB 8
4.2.2.1.3 VOID 8
4.2.2.1.4 RRC integrity check failure 8
4.2.2.1.5 UP integrity check failure 9
4.2.2.1.6 Ciphering of RRC-signalling 10
4.2.2.1.7 Ciphering of user data between the UE and the gNB 10
4.2.2.1.8 Replay protection of user data between the UE and the gNB 11
4.2.2.1.9 Replay protection of RRC-signalling 12
4.2.2.1.10 Ciphering of user data based on the security policy sent by the SMF 12
4.2.2.1.11 Integrity of user data based on the security policy sent by the SMF 13
4.2.2.1.12 AS algorithms selection 14
4.2.2.1.13 Key refresh at the gNB 15
4.2.2.1.14 Bidding down prevention in Xn-handovers 16
4.2.2.1.15 AS protection algorithm selection in gNB change 16
4.2.2.1.16 Control plane data confidentiality protection over N2/Xn interface 17
4.2.2.1.17 Control plane data integrity protection over N2/Xn interface 17
4.2.2.1.18 Key update at the gNB on dual connectivity 18
4.2.2.1.19 UP security activation in Inactive scenario 19
4.2.3 Technical Baseline 20
4.2.3.1 Introduction 20
4.2.3.2 Protecting data and information 20
4.2.3.2.1 Protecting data and information – general 20
4.2.3.2.2 Protecting data and information – unauthorized viewing 20
4.2.3.2.3 Protecting data and information in storage 20
4.2.3.2.4 Protecting data and information in transfer 20
4.2.3.2.5 Logging access to personal data 20
4.2.3.3 Protecting availability and integrity 20
4.2.3.4 Authentication and authorization 20
4.2.3.4.1 Authentication attributes 20
4.2.3.5 Protecting sessions 21
4.2.3.6 Logging 21
4.2.4 Operating systems 21
4.2.5 Web servers 21
4.2.6 Network devices 21
4.2.6.1 Protection of data and information 21
4.2.6.2 Protecting availability and integrity 21

4.2.6.2.1 Packet filtering....21
4.2.6.2.2 Interface robustness requirements....21
4.2.6.2.3 GTP-C Filtering....21
4.2.6.2.4 GTP-U Filtering....21
4.2.7 Void....21
4.3 gNodeB-specific adaptations of hardening requirements and related test cases....21
4.3.1 Introduction....22
4.3.2 Technical Baseline....22
4.3.3 Operating Systems....22
4.3.4 Web Servers....22
4.3.5 Network Devices....22
4.3.6 Network Functions in service-based architecture....22
4.4 gNodeB-specific adaptations of basic vulnerability testing requirements and related test cases....22

Annex A (informative): Change history....23

History....24

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.