|  |
| --- |
| 3GPP TS 33.742 V0.2.0 (2022-09) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;5G Security Assurance Specification (SCAS); Split gNB product classes (Release 18) |
|   |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2022, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 gNB-CU-specific security requirements and related test cases 8

4.1 Introduction 8

4.2 Security functional adaptations of requirements and related test cases 8

4.2.1 Introduction 8

4.2.2 Requirements and test cases deriving from 3GPP specifications 8

4.2.3 Technical Baseline 9

4.2.4 Operating systems 9

4.2.5 Web servers 9

4.2.6 Network devices 9

4.3 Adaptations of hardening requirements and related test cases 9

4.3.1 Introduction 9

4.3.2 Technical Baseline 9

4.3.3 Operating Systems 9

4.3.4 Web Servers 9

4.3.5 Network Devices 9

4.3.6 Network Functions in service-based architecture 9

4.4 Adaptations of basic vulnerability testing requirements and related test cases 10

5 gNB-CU-CP-specific security requirements and related test cases 10

5.1 Introduction 10

5.2 Security functional adaptations of requirements and related test cases 10

5.2.1 Introduction 10

5.2.2 Requirements and test cases deriving from 3GPP specifications 10

5.2.3 Technical Baseline 12

5.2.4 Operating systems 12

5.2.5 Web servers 12

5.2.6 Network devices 12

5.3 Adaptations of hardening requirements and related test cases 12

5.3.1 Introduction 12

5.3.2 Technical Baseline 12

5.3.3 Operating Systems 12

5.3.4 Web Servers 12

5.3.5 Network Devices 12

5.3.6 Network Functions in service-based architecture 12

5.4 Adaptations of basic vulnerability testing requirements and related test cases 12

6 gNB-CU-UP-specific security requirements and related test cases 12

6.1 Introduction 12

6.2 Security functional adaptations of requirements and related test cases 12

6.2.1 Introduction 12

6.2.2 Requirements and test cases deriving from 3GPP specifications 13

6.2.3 Technical Baseline 14

6.2.4 Operating systems 14

6.2.5 Web servers 14

6.2.6 Network devices 14

6.3 Adaptations of hardening requirements and related test cases 14

6.3.1 Introduction 14

6.3.2 Technical Baseline 14

6.3.3 Operating Systems 14

6.3.4 Web Servers 14

6.3.5 Network Devices 14

6.3.6 Network Functions in service-based architecture 14

6.4 Adaptations of basic vulnerability testing requirements and related test cases 14

7 gNB-DU-specific security requirements and related test cases 14

7.1 Introduction 14

7.2 Security functional adaptations of requirements and related test cases 14

7.2.1 Introduction 14

7.2.2 Requirements and test cases deriving from 3GPP specifications 15

7.2.3 Technical Baseline 16

7.2.4 Operating systems 16

7.2.5 Web servers 16

7.2.6 Network devices 16

7.3 Adaptations of hardening requirements and related test cases 16

7.3.1 Introduction 16

7.3.2 Technical Baseline 16

7.3.3 Operating Systems 16

7.3.4 Web Servers 16

7.3.5 Network Devices 16

7.3.6 Network Functions in service-based architecture 16

7.4 Adaptations of basic vulnerability testing requirements and related test cases 16

Annex <A> (normative): <Normative annex for a Technical Specification> 17

Annex <B> (informative): <Informative annex for a Technical Specification> 18

B.1 Heading levels in an annex 18

Annex <X> (informative): Change history 19

**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.**Error! Bookmark not defined.

# 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.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# 1 Scope

The present document contains objectives, requirements and test cases that are specific to the various split gNB network product classes. The gNB can be deployed as more than one entity by splitting the gNB into gNB-CU and gNB-DU(s) and possibly further splitting the gNB-CU into gNB-CU-CP and gNB-CU-UP(s) (see TS 38.401 [5]). Test cases for such deployments are provided. The present document refers to the Catalogue of General Security Assurance Requirements (see TS 33.117 [2]) and formulates specific adaptions of the requirements and test cases given there, as well as specifying requirements and test cases unique to the various split 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 33.117: "Catalogue of general security assurance requirements".

[3] 3GPP TS 33.501 (Release 15): "Security architecture and procedures for 5G system".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] 3GPP TS 38.401: "NG-RAN; Architecture description".

[6] 3GPP TS 33.511: "Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class".

# 3 Definitions of terms, symbols 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].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 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].

gNB-CU as defined in TS 38.401 [5]

gNB-CU-CP as defined in TS 38.401 [5]

gNB-CU-UP as defined in TS 38.401 [5]

gNB-DU as defined in TS 38.401 [5]

# 4 gNB-CU-specific security requirements and related test cases

## 4.1 Introduction

gNB-CU specific security requirements include both requirements derived from gNB-CU-specific security functional requirements as well as security requirements derived from threats specific to gNB-CU as described in TR 33.926 [4]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [2] and are not repeated in the present document.

## 4.2 Security functional adaptations of requirements and related test cases

### 4.2.1 Introduction

The present clause contains gNB-CU-specific security functional adaptations of requirements and related test cases. Many of the security functional requirements are directly inherited from the gNB product class.

### 4.2.2 Requirements and test cases deriving from 3GPP specifications

4.2.2.1 Security functional requirements on the gNB-CU deriving from 3GPP specifications – TS 33.501 [3]

Editor’s note: The threat references for all security functional need to refer to a gNB-CU one once they are defined

4.2.2.1.1 Security functional requirements inherited from gNB

The security functional requirements in clause 4.2.2.1 of TS 33.511 [6] cases except the ones in clauses 4.2.2.1.16 and 4.2.2.1.17 apply to the gNB-CU by changing the gNB to gNB-CU for the entity under test in the test cases.

NOTE 1: The security functional requirements in clauses 4.2.2.1.16 and 4.2.2.1.17 of TS 33.511 [6] do not apply directly as the gNB-CU supports more interfaces compared to the gNB.

4.2.2.1.2 Control plane data confidentiality protection over N2/Xn/F1 interface

*Requirement Name:* Control plane data confidentiality protection over N2/Xn/F1 interface

*Requirement Reference:* TS 33.501 [3], clauses 5.3.9, 9.2 and 9.4

*Requirement Description:* *"F1-C interface shall support confidentiality, integrity and replay protection."*, *"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 [3], clauses 5.3.9, 9.2 and 9.4.

*Threat References:* TR 33.926 [4], clause D.2.2.1 – Control plane data confidentiality protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2]

4.2.2.1.3 Control plane data integrity protection over N2/Xn/F1 interface

*Requirement Name:* Control plane data integrity protection over N2/Xn/F1 interface

*Requirement Reference*: TS 33.501 [3], clauses 5.3.9, 9.2 and 9.4

*Requirement Description:* *"F1-C interface shall support confidentiality, integrity and replay protection.",* *"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 [3], clauses 5.3.9, 9.2 and 9.4.

*Threat References:* TR 33.926 [4], clause D.2.2.2 – Control plane data integrity protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2].

Editor’s note: The user plane over network interface cases need to be added.

### 4.2.3 Technical Baseline

### 4.2.4 Operating systems

### 4.2.5 Web servers

### 4.2.6 Network devices

## 4.3 Adaptations of hardening requirements and related test cases

### 4.3.1 Introduction

### 4.3.2 Technical Baseline

### 4.3.3 Operating Systems

### 4.3.4 Web Servers

### 4.3.5 Network Devices

### 4.3.6 Network Functions in service-based architecture

The requirements and test cases in clause 4.3.6 of TS 33.117 [2] are not applicable to the gNB-CU network products.

## 4.4 Adaptations of basic vulnerability testing requirements and related test cases

# 5 gNB-CU-CP-specific security requirements and related test cases

## 5.1 Introduction

gNB-CU-CP specific security requirements include both requirements derived from gNB-CU-CP-specific security functional requirements as well as security requirements derived from threats specific to gNB-CU-CP as described in TR 33.926 [4]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [2] and are not repeated in the present document.

## 5.2 Security functional adaptations of requirements and related test cases

### 5.2.1 Introduction

The present clause contains gNB-CU-CP-specific security functional adaptations of requirements and related test cases. Many of the security functional requirements are directly inherited from the gNB product class.

### 5.2.2 Requirements and test cases deriving from 3GPP specifications

5.2.2.1 Security functional requirements on the gNB-CU-CP deriving from 3GPP specifications – TS 33.501 [3]

Editor’s note: The threat references for all security functional need to refer to a gNB-CU-CP one once they are defined

5.2.2.1.1 Security functional requirements inherited from gNB

The security functional requirements in the following clauses of TS 33.511 [6] apply to the gNB-CU-CP by changing the gNB to gNB-CU-CP for the entity under test in the test cases:

* 4.2.2.1.1 Integrity protection of RRC-signalling;
* 4.2.2.1.4 RRC integrity check failure;
* 4.2.2.1.6 Ciphering of RRC-signalling;
* 4.2.2.1.9 Replay protection of RRC-signalling;
* 4.2.2.1.12 AS algorithms selection;
* 4.2.2.1.13 Key refresh at the gNB;
* 4.2.2.1.14 Bidding down prevention in Xn-handovers;
* 4.2.2.1.15 AS protection algorithm selection in gNB change;
* 4.2.2.1.18 Key update at the gNB on dual connectivity; and
* 4.2.2.1.19 UP security activation in Inactive scenario.

5.2.2.1.2 Control plane data confidentiality protection over N2/Xn/F1/E1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.16 of TS 33.511 [6] but modified as the gNB-CU-CP supports the F1 and E1 interface.

*Requirement Name:* Control plane data confidentiality protection over N2/Xn/F1/E1 interface

*Requirement Reference:* TS 33.501 [3], clauses 5.3.9, 5.3.10, 9.2 and 9.4

*Requirement Description:* *"F1-C interface shall support confidentiality, integrity and replay protection."*, *"The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected.", "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 [3], clauses 5.3.9, 5.3.10, 9.2 and 9.4.*

*Threat References:* TR 33.926 [4], clause D.2.2.1 – Control plane data confidentiality protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2]

5.2.2.1.3 Control plane data integrity protection over N2/Xn/F1/E1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.17 of TS 33.511 [6] but modified as the CU-CP supports the F1 and E1 interfaces.

*Requirement Name:* Control plane data integrity protection over N2/Xn/F1/E1 interface

Requirement Reference: TS 33.501 [3], clauses 5.3.9, 9.2 and 9.4

*Requirement Description:* *"F1-C interface shall support confidentiality, integrity and replay protection.",* *"The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected."*, *"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 [3], clauses 5.3.9, 5.3.10, 9.2 and 9.4.

*Threat References:* TR 33.926 [4], clause D.2.2.2 – Control plane data integrity protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2].

### 5.2.3 Technical Baseline

### 5.2.4 Operating systems

### 5.2.5 Web servers

### 5.2.6 Network devices

## 5.3 Adaptations of hardening requirements and related test cases

### 5.3.1 Introduction

### 5.3.2 Technical Baseline

### 5.3.3 Operating Systems

### 5.3.4 Web Servers

### 5.3.5 Network Devices

### 5.3.6 Network Functions in service-based architecture

The requirements and test cases in clause 4.3.6 of TS 33.117 [2] are not applicable to the gNB-CU-CP network products.

## 5.4 Adaptations of basic vulnerability testing requirements and related test cases

# 6 gNB-CU-UP-specific security requirements and related test cases

## 6.1 Introduction

gNB-CU-UP specific security requirements include both requirements derived from gNB-CU-UP-specific security functional requirements as well as security requirements derived from threats specific to gNB-CU-UP as described in TR 33.926 [4]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [2] and are not repeated in the present document.

### 6.2 Security functional adaptations of requirements and related test cases6.2.1 Introduction

The present clause contains gNB-CU-UP-specific security functional adaptations of requirements and related test cases. Many of the security functional requirements are directly inherited from the gNB product class.

### 6.2.2 Requirements and test cases deriving from 3GPP specifications

6.2.2.1 Security functional requirements on the gNB-CU-UP deriving from 3GPP specifications – TS 33.501 [3]

Editor’s note: The threat references for all security functional need to refer to a gNB-CU-UP one once they are defined

6.2.2.1.1 Security functional requirements inherited from gNB

The security functional requirements in the following clauses of TS 33.511 [6] apply to the gNB-CU-UP by changing the gNB to gNB-CU-UP for the entity under test in the test cases:

* 4.2.2.1.5 UP integrity check failure; and
* 4.2.2.1.8 Replay protection of user data between the UE and the gNB.

6.2.2.1.4 Control plane data confidentiality protection over E1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.16 of TS 33.511 [6] but modified as the gNB-CU-UP only supports the E1 interface.

*Requirement Name:* Control plane data confidentiality protection over E1 interface

*Requirement Reference:* TS 33.501 [3], clauses 5.3.9

*Requirement Description:* *"* *The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected."* as specified in TS 33.501 [3], clauses 5.3.10.

*Threat References:* TR 33.926 [4], clause D.2.2.1 – Control plane data confidentiality protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2].

6.2.2.1.5 Control plane data integrity protection over E1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.17 of TS 33.511 [6] but modified as the gNB-CU-UP only supports the E1 interface.

*Requirement Name:* Control plane data integrity protection over E1 interface

*Requirement Reference*: TS 33.501 [3], clauses 5.3.9

*Requirement Description:* *"* *The E1 interface between CU-CP and CU-UP shall be confidentiality, integrity and replay protected."* as specified in TS 33.501 [3], clauses 5.3.10.

*Threat References:* TR 33.926 [4], clause D.2.2.2 – Control plane data integrity protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2].

Editor’s note: The user plane over network interface cases need to be added.

### 6.2.3 Technical Baseline

### 6.2.4 Operating systems

### 6.2.5 Web servers

### 6.2.6 Network devices

## 6.3 Adaptations of hardening requirements and related test cases

### 6.3.1 Introduction

### 6.3.2 Technical Baseline

### 6.3.3 Operating Systems

### 6.3.4 Web Servers

### 6.3.5 Network Devices

### 6.3.6 Network Functions in service-based architecture

The requirements and test cases in clause 4.3.6 of TS 33.117 [2] are not applicable to the gNB-CU-UP network products.

## 6.4 Adaptations of basic vulnerability testing requirements and related test cases

# 7 gNB-DU-specific security requirements and related test cases

## 7.1 Introduction

gNB-DU specific security requirements include both requirements derived from gNB-DU-specific security functional requirements as well as security requirements derived from threats specific to gNB-DU as described in TR 33.926 [4]. Generic security requirements and test cases common to other network product classes have been captured in TS 33.117 [2] and are not repeated in the present document.

## 7.2 Security functional adaptations of requirements and related test cases

### 7.2.1 Introduction

The present clause contains gNB-DU-specific security functional adaptations of requirements and related test cases.

### 7.2.2 Requirements and test cases deriving from 3GPP specifications

7.2.2.1 Security functional requirements on the gNB-DU deriving from 3GPP specifications – TS 33.501 [3]

Editor’s note: The threat references for all security functional need to refer to a gNB-DU one once they are defined

7.2.2.1.1 Control plane data confidentiality protection over F1 interface

*Requirement Name:* Control plane data confidentiality protection over F1 interface

*Requirement Reference:* TS 33.501 [3], clauses 5.3.9

*Requirement Description:* *"F1-C interface shall support confidentiality, integrity and replay protection."* as specified in TS 33.501 [3], clauses 5.3.9.

*Threat References:* TR 33.926 [4], clause D.2.2.1 – Control plane data confidentiality protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2]

7.2.2.1.2 Control plane data integrity protection over F1 interface

*Requirement Name:* Control plane data integrity protection over F1 interface

*Requirement Reference*: TS 33.501 [3], clauses 5.3.9

*Requirement Description:* *"F1-C interface shall support confidentiality, integrity and replay protection."* as specified in TS 33.501 [3], clauses 5.3.9.

*Threat References:* TR 33.926 [4], clause D.2.2.2 – Control plane data integrity protection.

*Test Case:* the test case in subclause 4.2.3.2.4 of TS 33.117 [2].

Editor’s note: The user plane over network interface cases need to be added.

### 7.2.3 Technical Baseline

### 7.2.4 Operating systems

### 7.2.5 Web servers

### 7.2.6 Network devices

## 7.3 Adaptations of hardening requirements and related test cases

### 7.3.1 Introduction

### 7.3.2 Technical Baseline

### 7.3.3 Operating Systems

### 7.3.4 Web Servers

### 7.3.5 Network Devices

### 7.3.6 Network Functions in service-based architecture

The requirements and test cases in clause 4.3.6 of TS 33.117 [2] are not applicable to the gNB-DU network products.

## 7.4 Adaptations of basic vulnerability testing requirements and related test cases

Annex <A> (normative):
<Normative annex for a Technical Specification>

Annex <B> (informative):
<Informative annex for a Technical Specification>

# B.1 Heading levels in an annex

Heading levels within an annex are used as in the main document, but for Heading level selection, the "A.", "B.", etc. are ignored. e.g. **B.1.2** is formatted using ***Heading 2*** style.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-05 | SA3#107-e | S3-221201 |  |  |  | Skeleton (S3-221196) plus S3-0989 | 0.1.0 |
| 2022-09 | SA3#108-e | S3-222321 |  |  |  | Incorporating S3-221824, S3-222309. S3-221310, S3-222312 and S3-222313 | 0.2.0 |