|  |  |
| --- | --- |
| 3GPP TS 33.523 V0.5.0 (2023-02) | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® 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

4.2.2.1 Security functional requirements on the gNB-CU deriving from 3GPP specifications – TS 33.501 [3] 8

4.2.2.1.1 Security functional requirements inherited from gNB 8

4.2.2.1.2 Control plane data confidentiality protection over N2/Xn/F1 interface 9

4.2.2.1.3 Control plane data integrity protection over N2/Xn/F1 interface 10

4.2.2.1.4 User plane data confidentiality protection over N3/Xn/F1 interface 10

4.2.2.1.5 User plane data integrity protection over N3/Xn/F1 interface 10

4.2.3 Technical Baseline 11

4.2.4 Operating systems 11

4.2.5 Web servers 11

4.2.6 Network devices 11

4.3 Adaptations of hardening requirements and related test cases 11

4.4 Adaptations of basic vulnerability testing requirements and related test cases 11

5 gNB-CU-CP-specific security requirements and related test cases 11

5.1 Introduction 11

5.2 Security functional adaptations of requirements and related test cases 11

5.2.1 Introduction 11

5.2.2 Requirements and test cases deriving from 3GPP specifications 12

5.2.2.1 Security functional requirements on the gNB-CU-CP deriving from 3GPP specifications – TS 33.501 [3] 12

5.2.2.1.1 Security functional requirements inherited from gNB 12

5.2.2.1.2 Control plane data confidentiality protection over N2/Xn/F1/E1 interface 12

5.2.2.1.3 Control plane data integrity protection over N2/Xn/F1/E1 interface 13

5.2.2.1.4 Ciphering of user data based on the security policy sent by the SMF 13

5.2.2.1.5 Integrity of user data based on the security policy sent by the SMF 14

5.2.3 Technical Baseline 15

5.2.4 Operating systems 15

5.2.5 Web servers 15

5.2.6 Network devices 15

5.3 Adaptations of hardening requirements and related test cases 15

5.4 Adaptations of basic vulnerability testing requirements and related test cases 15

6 gNB-CU-UP-specific security requirements and related test cases 16

6.1 Introduction 16

6.2 Security functional adaptations of requirements and related test cases6.2.1 Introduction 16

6.2.2 Requirements and test cases deriving from 3GPP specifications 16

6.2.2.1 Security functional requirements on the gNB-CU-UP deriving from 3GPP specifications – TS 33.501 [3] 16

6.2.2.1.1 Security functional requirements inherited from gNB 16

6.2.2.1.2 Control plane data confidentiality protection over E1 interface 16

6.2.2.1.3 Control plane data integrity protection over E1 interface 16

6.2.2.1.4 User plane data confidentiality protection over N3/Xn/F1 interface 17

6.2.2.1.5 User plane data integrity protection over N3/Xn/F1 interface 17

6.2.2.1.6 Integrity protection of user data between the UE and the gNB-CU-UP 17

6.2.2.1.7 Ciphering of user data between the UE and the gNB-CU-UP 18

6.2.3 Technical Baseline 19

6.2.4 Operating systems 19

6.2.5 Web servers 19

6.2.6 Network devices 19

6.3 Adaptations of hardening requirements and related test cases 19

6.4 Adaptations of basic vulnerability testing requirements and related test cases 19

7 gNB-DU-specific security requirements and related test cases 19

7.1 Introduction 19

7.2 Security functional adaptations of requirements and related test cases 20

7.2.1 Introduction 20

7.2.2 Requirements and test cases deriving from 3GPP specifications 20

7.2.2.1 Security functional requirements on the gNB-DU deriving from 3GPP specifications – TS 33.501 [3] 20

7.2.2.1.1 Control plane data confidentiality protection over F1 interface 20

7.2.2.1.2 Control plane data integrity protection over F1 interface 20

7.2.2.1.3 User plane data confidentiality protection over F1 interface 20

7.2.2.1.4 User plane data integrity protection over F1 interface 21

7.2.3 Technical Baseline 21

7.2.4 Operating systems 21

7.2.5 Web servers 21

7.2.6 Network devices 21

7.3 Adaptations of hardening requirements and related test cases 21

7.4 Adaptations of basic vulnerability testing requirements and related test cases 21

Annex <X> (informative): Change history 22

**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.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 (and are based upon and borrow heavily from the specification for the gNB product class (see TS 33.511 [6])). 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 ‘W’ in the clauses for the references to threats will need to be aligned with the final Annex allocation in TR 33.926.

##### 4.2.2.1.1 Security functional requirements inherited from gNB

The following security functional requirements in clause 4.2.2.1 of TS 33.511 [6] apply to the gNB-CU by changing the gNB to gNB-CU for the entity under test in the test cases and with the below change to threat references:

4.2.2.1.1 Integrity protection of RRC-signalling

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

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

*Threat References*: TR 33.926 [4], clause W.2.2.4 – User plane data integrity protection.

4.2.2.1.4 RRC integrity check failure

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

4.2.2.1.5 UP integrity check failure

*Threat References*: TR 33.926 [4], clause W.2.2.4 – User plane data integrity protection.

4.2.2.1.6 Ciphering of RRC-signalling

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

4.2.2.1.7 Ciphering of user data between the UE and the gNB

*Threat References:* TR 33.926 [4], clause W.2.2.3 – User plane data confidentiality protection at gNB.

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

*Threat References:* TR 33.926 [4], clause W.2.2.4 – User plane data integrity protection.

4.2.2.1.9 Replay protection of RRC-signalling

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

4.2.2.1.10 Ciphering of user data based on the security policy sent by the SMF

*Threat References:* TR 33.926 [4], clause W.2.2.8 – Security Policy Enforcement.

4.2.2.1.11 Integrity of user data based on the security policy sent by the SMF

*Threat References:* TR 33.926 [4], clause W.2.2.8 – Security Policy Enforcement.

4.2.2.1.12 AS algorithms selection

*Threat References*: TR 33.926 [4], clause W.2.2.5 – AS algorithm selection and use.

4.2.2.1.13 Key refresh at the gNB

*Threat References*: TR 33.926 [4], clause W.2.2.7 – Key Reuse.

4.2.2.1.14 Bidding down prevention in Xn-handovers

*Threat References*: TR 33.926 [4], clause W.2.2.6 – Bidding Down on Xn-Handover.

4.2.2.1.15 AS protection algorithm selection in gNB change

*Threat References*: TR 33.926 [4], clause W.2.2.5 – AS algorithm selection and use.

4.2.2.1.18 Key update at the gNB on dual connectivity

*Threat References*: TR 33.926 [4], clause W.2.2.7 – Key Reuse.

4.2.2.1.19 UP security activation in Inactive scenario

*Threat Reference*: TR 33.926 [4], clause W.2.2.9 – State transition from inactive state to connected state.

##### 4.2.2.1.2 Control plane data confidentiality protection over N2/Xn/F1 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 supports the 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 W.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

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 supports the 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 W.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].

##### 4.2.2.1.4 User plane data confidentiality protection over N3/Xn/F1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.R of TS 33.511 [6] but modified as the gNB-CU supports the F1 interface.

Editor’s Note: The ‘R’ in the clause in the Note referring to TS 33.511 needs correction once the CR to include this test case in TS 33.511 is approved.

*Requirement Name:* User plane data confidentiality protection over N3/Xn/F1 interface.

*Requirement Reference:* TS 33.501 [2], clauses 5.3.9, 9.3 and 9.4.

*Requirement Description:* "*The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane"*, *"The transport of user data over N3 shall be integrity, confidentiality and replay-protected."*, and *"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 5.3.9, 9.3 and 9.4.

*Threat References:* TR 33.926 [4], clause W.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].

##### 4.2.2.1.5 User plane data integrity protection over N3/Xn/F1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.S of TS 33.511 [6] but modified as the gNB-CU supports the F1 interface.

Editor’s Note: The ‘S’ in the clause in the Note referring to TS 33.511 needs correction once the CR to include this test case in TS 33.511 is approved.

*Requirement Name:* User plane data integrity protection over N3/Xn/F1 interface.

*Requirement Reference*: TS 33.501[2], clauses 5.3.9, 9.3 and 9.4.

*Requirement Description:* "*The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane"*, *"The transport of user data over N3 shall be integrity, confidentiality and replay-protected."*, and *"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 5.3.9, 9.3 and 9.4.

*Threat References:* TR 33.926 [4], clause W.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].

### 4.2.3 Technical Baseline

The baseline technical requirements are identical to the ones for the gNB product class given in clause 4.2.3 of TS 33.511 [6].

### 4.2.4 Operating systems

There are no gNB-CU-specific additions to clause 4.2.4 of TS 33.117 [2].

NOTE: The ICMP changes applied for a gNB only apply for a DU. In a split deployment where the CU(-CP/UP) is deployed in a data center, the CU(-CP/UP) should be treated as any other IP nodes (e.g., UPF) as the data center nodes are assumed to have connectivity to IP networks whereas DU can be considered like a gNB from ICMP threat perspective.

### 4.2.5 Web servers

There are no gNB-CU-specific additions to clause 4.2.5 of TS 33.117 [2].

### 4.2.6 Network devices

These requirements are identical to the ones for the gNB product class given in clause 4.2.6 of TS 33.511 [6].

## 4.3 Adaptations of hardening requirements and related test cases

These requirements are identical to the ones for the gNB product class given in clause 4.3 of TS 33.511 [6].

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

There are no gNB-CU-specific additions to clause 4.4 of TS 33.117 [2].

# 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 ‘X’ in the clauses for the references to threats will need to be aligned with the final Annex allocation in TR 33.926.

##### 5.2.2.1.1 Security functional requirements inherited from gNB

The following security functional requirements from clause 4.2.2.1 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 and with the below changes of threat reference:

4.2.2.1.1 Integrity protection of RRC-signalling

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

4.2.2.1.4 RRC integrity check failure

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

4.2.2.1.6 Ciphering of RRC-signalling

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

4.2.2.1.9 Replay protection of RRC-signalling

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

4.2.2.1.12 AS algorithms selection

*Threat References*: TR 33.926 [4], clause X.2.2.3 – AS algorithm selection and use.

4.2.2.1.13 Key refresh at the gNB

*Threat References*: TR 33.926 [4], clause X.2.2.5 – Key Reuse.

4.2.2.1.14 Bidding down prevention in Xn-handovers

*Threat References*: TR 33.926 [4], clause X.2.2.4 – Bidding Down on Xn-Handover.

4.2.2.1.15 AS protection algorithm selection in gNB change

*Threat References*: TR 33.926 [4], clause X.2.2.3 – AS algorithm selection and use.

4.2.2.1.18 Key update at the gNB on dual connectivity

*Threat References*: TR 33.926 [4], clause X.2.2.5 – Key Reuse.

4.2.2.1.19 UP security activation in Inactive scenario

*Threat Reference*: TR 33.926 [4], clause X.2.2.7 – State transition from inactive state to connected state.

##### 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 interfaces.

*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." and "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 X.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, 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 X.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].

##### 5.2.2.1.4 Ciphering of user data based on the security policy sent by the SMF

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.10 of TS 33.511 [6] but modified as the gNB-CU-CP informs both the gNB-CU-UP and UE whether to use a non-NULL ciphering algorithm or not.

*Requirement Name:* Ciphering of user data based on the security policy sent by the SMF.

*Requirement Reference:* TS 33.501 [3], 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 [3], clause 5.3.2.

*Threat References:* TR 33.926 [4], clause X.2.2.6 – Security Policy Enforcement.

***Test Case****:*

**Test Name:** TC-UP-DATA-CIP-SMF\_gNB-CU-CP

**Purpose:** Toverify that the user data packets are confidentiality protected based on the security policy sent by the SMF via AMF

**Pre-Condition:**

- The gNB-CU-CP 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 and of the security keys etc needed to decrypt the messages on the E1 interface.

- 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-CU-CP.

3. The tester shall capture the Bearer Context Setup Request message sent to the gNB-CU-UP over the E1 interface.

4. The tester shall decrypt the Bearer Context Setup Request message.

5. The tester shall capture the RRC connection reconfiguration procedure between gNB-CU-CP to UE over NG RAN air interface. And filter the RRC connection reconfiguration message sent by gNB-CU-CP to UE.

6. The tester shall decrypt the RRC connection Reconfiguration message and retrieve the UP ciphering protection indication presenting in the decrypted message.

7. The tester shall verify if the UP ciphering policy received at gNB-CU-CP is same as the UP ciphering protection indication notified by the gNB-CU-CP to the UE in the RRC connection Reconfiguration message and the gNB-CU-UP in the Bearer Context Setup Request message.

**Expected Results:**

Both the messages indicate that ciphering is to be used inline with the received policy.

**Expected format of evidence:**

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

##### 5.2.2.1.5 Integrity of user data based on the security policy sent by the SMF

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.11 of TS 33.511 [6] but modified as the gNB-CU-CP informs both the gNB-CU-UP and UE whether to use a non-NULL integrity algorithm or not.

*Requirement Name:* Integrity of user data based on the security policy sent by the SMF.

*Requirement Reference:* TS 33.501 [3], 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 [3], clause 5.3.2.

*Threat References:* TR 33.926 [4], clause X.2.2.6 – Security Policy Enforcement.

***Test Case****:*

**Test Name:** TC-UP-DATA-INT-SMF\_gNB-CU-CP

**Purpose:** Toverify that the user data packets are integrity protected based on the security policy sent by the SMF.

**Pre-Condition:**

- The gNB-CU-CP 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 and of the security keys etc needed to decrypt the messages on the E1 interface.

- 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 Bearer Context Setup Request message sent to the gNB-CU-UP over the E1 interface.

4. The tester shall decrypt the Bearer Context Setup Request message.

5. The tester shall capture the RRC connection reconfiguration message sent by gNB to UE over NG RAN air interface.

6. The tester shall decrypt the RRC connection reconfiguration message and retrieve the UP integrity protection indication presenting in the decrypted message.

7. Tester shall check whether UP integrity policy received at gNB-CU-UP is same as the UP integrity protection indication notified by the gNB-CU-CP to the UE in the RRC connection reconfiguration message and the gNB-CU-UP in the Bearer Context Setup Request message.

**Expected Results:**

Both the messages indicate that integrity is to be used inline with the received policy.

**Expected format of evidence:**

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

### 5.2.3 Technical Baseline

The baseline technical requirements are identical to the ones for the gNB product class given in clause 4.2.3 of TS 33.511 [6].

### 5.2.4 Operating systems

There are no gNB-CU specific additions to clause 4.2.4 of TS 33.117 [2].

### 5.2.5 Web servers

There are no gNB-CU-CP specific additions to clause 4.2.5 of TS 33.117 [2].

### 5.2.6 Network devices

These requirements are identical to the ones for the gNB product class given in clause 4.2.6 of TS 33.511 [6] except the GTP-U Filtering case in clause 4.2.6.2.4 of TS 33.117 [2] as the gNB-CU-CP does not support user plane interfaces.

## 5.3 Adaptations of hardening requirements and related test cases

These requirements are identical to the ones for the gNB product class given in clause 4.3 of TS 33.511 [6].

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

There are no gNB-CU-CP specific additions to clause 4.4 of TS 33.117 [2].

# 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 ‘Y’ in the clauses for the references to threats will need to be aligned with the final Annex allocation in TR 33.926.

##### 6.2.2.1.1 Security functional requirements inherited from gNB

The following security functional requirements from clause 4.2.2.1 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 and with the below changes of threat reference:

4.2.2.1.5 UP integrity check failure

*Threat References*: TR 33.926 [4], clause Y.2.2.4 – User plane data integrity protection.

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

*Threat References:* TR 33.926 [4], clause Y.2.2.4 – User plane data integrity protection.

##### 6.2.2.1.2 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 5.3.10.

*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 Y.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].

##### 6.2.2.1.3 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 5.3.10.

*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 Y.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].

##### 6.2.2.1.4 User plane data confidentiality protection over N3/Xn/F1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.R of TS 33.511 [6] but modified as the gNB-CU-UP supports the F1 interface.

Editor’s Note: The ‘R’ in the clause in the Note referring to TS 33.511 needs correction once the CR to include this test case in TS 33.511 is approved.

*Requirement Name:* User plane data confidentiality protection over N3/Xn/F1 interface.

*Requirement Reference:* TS 33.501 [2], clauses 5.3.9, 9.3 and 9.4.

*Requirement Description:* "*The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane"*, *"The transport of user data over N3 shall be integrity, confidentiality and replay-protected."*, and *"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 5.3.9, 9.3 and 9.4.

*Threat References:* TR 33.926 [4], clause Y.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].

##### 6.2.2.1.5 User plane data integrity protection over N3/Xn/F1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.S of TS 33.511 [6] but modified as the gNB-CU-UP supports the F1 interface.

Editor’s Note: The ‘S’ in the clause in the Note referring to TS 33.511 needs correction once the CR to include this test case in TS 33.511 is approved.

*Requirement Name:* User plane data integrity protection over N3/Xn/F1 interface.

*Requirement Reference*: TS 33.501[2], clauses 5.3.9, 9.3 and 9.4.

*Requirement Description:* "*The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane"*, *"The transport of user data over N3 shall be integrity, confidentiality and replay-protected."*, and *"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 5.3.9, 9.3 and 9.4.

*Threat References:* TR 33.926 [4], clause Y.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].

##### 6.2.2.1.6 Integrity protection of user data between the UE and the gNB-CU-UP

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.2 of TS 33.511 [6] but modified as the gNB-CU-CP informs the gNB-CU-UP to use a non-NULL integrity algorithm.

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

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

*Threat References:* TR 33.926 [4], clause Y.2.2.4 – User plane data integrity protection.

***Test Case****:*

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

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

**Pre-Condition:**

- The gNB-CU-UP 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-CU-UP.

2. The gNB-CU-UP is sent by the gNB-CU-CP a Bearer Context Setup Request message with integrity protection indication "on".

3. Check any User data sent by gNB-CU-UP after receiving the Bearer Context Setup Request message and before UE enters CM-Idle state is integrity protected.

**Expected Results:**

Any user plane packets sent between UE and gNB-CU-UP over the NG RAN air interface after gNB-CU-UP receives the Bearer Context Setup Request is integrity protected.

**Expected format of evidence:**

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

##### 6.2.2.1.7 Ciphering of user data between the UE and the gNB-CU-UP

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.7 of TS 33.511 [6] but modified as the gNB-CU-CP informs the gNB-CU-UP to use a non-NULL confidentiality algorithm.

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

*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 [4], clause Y.2.2.3 – User plane data confidentiality protection at gNB

*Test Case:*

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

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

**Pre-Condition:**

- The gNB-CU-UP 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 gNB-CU-UP is sent by the gNB-CU-CP a Bearer Context Setup Request message with ciphering protection indication "on".

2. Check any user data sent by the gNB-CU-UP after receiving the Bearer Context Setup Request message and before the UE enters into CM-Idle state.

**Expected Results:**

The user plane packets sent to the UE after the gNB-CU-UP receives the Bearer Context Setup Request is confidentiality protected.

**Expected format of evidence:**

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

### 6.2.3 Technical Baseline

The baseline technical requirements are identical to the ones for the gNB product class given in clause 4.2.3 of TS 33.511 [6].

### 6.2.4 Operating systems

There are no gNB-CU specific additions to clause 4.2.4 of TS 33.117 [2].

### 6.2.5 Web servers

There are no gNB-CU-UP specific additions to clause 4.2.5 of TS 33.117 [2].

### 6.2.6 Network devices

These requirements are identical to the ones for the gNB product class given in clause 4.2.6 of TS 33.511 [6].

## 6.3 Adaptations of hardening requirements and related test cases

These requirements are identical to the ones for the gNB product class given in clause 4.3 of TS 33.511 [6].

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

There are no gNB-CU-UP specific additions to clause 4.4 of TS 33.117 [2].

# 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 ‘Z’ in the clauses for the references to threats will need to be aligned with the final Annex allocation in TR 33.926.

##### 7.2.2.1.1 Control plane data confidentiality protection over F1 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-DU only supports the 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 Z.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

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-DU only supports the 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 Z.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].

##### 7.2.2.1.3 User plane data confidentiality protection over F1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.R of TS 33.511 [6] but modified as the gNB-DU only supports the F1 interface.

Editor’s Note: The ‘R’ in the clause in the Note referring to TS 33.511 needs correction once the CR to include this test case in TS 33.511 is approved.

*Requirement Name:* User plane data confidentiality protection over F1 interface.

*Requirement Reference:* TS 33.501 [2], clauses 5.3.9.

*Requirement Description:* "*The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane"* as specified in TS 33.501 [2], clauses 5.3.9.

*Threat References:* TR 33.926 [4], clause Z.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].

##### 7.2.2.1.4 User plane data integrity protection over F1 interface

NOTE 1: This is based on the security functional requirement on the gNB given in 4.2.2.1.S of TS 33.511 [6] but modified as the gNB-DU only supports the F1 interface.

Editor’s Note: The ‘S’ in the clause in the Note referring to TS 33.511 needs correction once the CR to include this test case in TS 33.511 is approved.

*Requirement Name:* User plane data integrity protection over F1 interface.

*Requirement Reference*: TS 33.501[2], clauses 5.3.9.

*Requirement Description:* *"The gNB shall support confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface [33] for user plane"* as specified in TS 33.501 [2], clauses 5.3.9.

*Threat References:* TR 33.926 [4], clause Z.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].

### 7.2.3 Technical Baseline

The baseline technical requirements are identical to the ones for the gNB product class given in clause 4.2.3 of TS 33.511 [6].

### 7.2.4 Operating systems

These requirements are identical to the ones for the gNB product class given in clause 4.2.4 of TS 33.511 [6].

### 7.2.5 Web servers

There are no gNB-DU specific additions to clause 4.2.5 of TS 33.117 [2].

### 7.2.6 Network devices

These requirements are identical to the ones for the gNB product class given in clause 4.2.6 of TS 33.511 [6].

## 7.3 Adaptations of hardening requirements and related test cases

These requirements are identical to the ones for the gNB product class given in clause 4.3 of TS 33.511 [6].

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

There are no gNB-DU specific additions to clause 4.4 of TS 33.117 [2].

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 S3-220989. | 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 |
| 2022-11 | SA3#109 | S3-224103 |  |  |  | Incorporating S3-223346, S3-223348, S3-223349, S3-223350, S3-223352, S3-223353 and S3-223354. | 0.3.0 |
| 2023-02 | SA3#110 | S3-230786 |  |  |  | Changing the TS number from TS 33.742 to TS 33.523 due to mis- allocated specification number | 0.4.0 |
| 2023-02 | SA3#110 | S3-231498 |  |  |  | Incorporating S3-230789, S3-230790, S3-230794, S3-231470, S3-231471 and S3-231472. | 0.5.0 |