3GPP TS 33.523 V19.2.0 (2025-07)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 5G Security Assurance Specification (SCAS); split gNB product classes (Release 19)

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

Contents

Foreword

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

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

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 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]). The present document contains objectives, requirements and test cases that are specific to the various split gNB network product classes. Test cases for such deployments are provided, are based upon and borrow heavily from the specification for the gNB product class (see TS 33.511 [6]). The main differences are the inclusion of cases for the F1 signalling and user plane connection and the E1 signalling connection on the top of the gNB cases as well as some revised cases to account for the split functionality. The present document also 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: "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".

[7] 3GPP TS 23.501: "System Architecture for 5G System (5GS)".

[8] 3GPP TS 38.300: "NR and NG-RAN Overall Description".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 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]

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 and in some cases small changes specific to the gNB-CU:

4.2.2.1.1 Integrity protection of RRC-signalling

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

4.2.2.1.4 RRC integrity check failure

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

4.2.2.1.5 UP integrity check failure

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

4.2.2.1.6 Ciphering of RRC-signalling

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

4.2.2.1.12 AS algorithms selection

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

4.2.2.1.14 Bidding down prevention in Xn-handovers

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

4.2.2.1.19 UP security activation in Inactive scenario

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

4.2.2.1.22 Checking expiry certificate

Threat Reference: TR 33.926 [4], clause R.2.2.. 11 – Certificate expiry checking.

4.2.2.1.23 Peer certificate checking

Threat Reference: TR 33.926 [4], clause R.2.2. 10 – Peer certificate validity checking.

Possible peers and interfaces for the gNB-CU are AMF, SEG/UPF, gNB and gNB-DU, and N2, N3, Xn and F1 interfaces respectively.

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

NOTE: This is based on the security functional requirement on the gNB given in clause 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 supports confidentiality, integrity and replay protection, the transport of control plane data over N2 is integrity, confidentiality and replay-protected and the transport of control plane data and user data over Xn is 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 R.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: This is based on the security functional requirement on the gNB given in clause 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 supports confidentiality, integrity and replay protection, the transport of control plane data over N2 is 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, 9.2 and 9.4.

Threat References: TR 33.926 [4], clause R.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: This is based on the security functional requirement on the gNB given in clause 4.2.2.1.20 of TS 33.511 [6] but modified as the gNB-CU supports the F1 interface.

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

Requirement Reference: TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

Requirement Description: The gNB supports confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane, the transport of user data over N3 is integrity, confidentiality and replay-protected, and the transport of control plane data and user data over Xn is integrity, confidentiality and replay-protected as specified in TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

Threat References: TR 33.926 [4], clause R.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 [2].

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

NOTE: This is based on the security functional requirement on the gNB given in clause 4.2.2.1.21 of TS 33.511 [6] but modified as the gNB-CU supports the F1 interface.

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

Requirement Reference: TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

Requirement Description: The gNB supports confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane, the transport of user data over N3 is 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, 9.3 and 9.4.

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

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

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

4.4.1 Introduction

There are no gNB-CU specific additions to clause 4.4.1 of TS 33.117 [2].

4.4.2 Port Scanning

There are no gNB-CU specific additions to clause 4.4.2 of TS 33.117 [2].

4.4.3 Vulnerability scanning

There are no gNB-CU specific additions to clause 4.4.3 of TS 33.117 [2].

4.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [2] are applicable to gNB-CU.

The interface defined for the gNB-CU are in clause 4.2.3 of TS 23.501 [7] and in clause 4.1 of TS 38.300 [8].

According to clause 4.4.4 of TS 33.117 [2], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for gNB-CU, the following interfaces and protocols are in the scope of the testing:

For N2: the SCTP and NGAP protocols.

For N3: the UDP and GTP-U protocols.

For Xn-C: the SCTP and XnAP protocols.

For Xn-U: the UDP and GTP-U protocols.

For F1-C: the SCTP and F1AP protocols.

For F1-U: the UDP and GTP-U protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 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]

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 and in some cases small changes specific to the gNB-CU-CP:

4.2.2.1.1 Integrity protection of RRC-signalling

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

4.2.2.1.4 RRC integrity check failure

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

4.2.2.1.6 Ciphering of RRC-signalling

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

4.2.2.1.12 AS algorithms selection

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

4.2.2.1.14 Bidding down prevention in Xn-handovers

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

4.2.2.1.19 UP security activation in Inactive scenario

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

4.2.2.1.22 Checking expiry certificate

Threat Reference: TR 33.926 [4], clause S.2.2. 9 – Certificate expiry checking.

4.2.2.1.23 Peer certificate checking

Threat Reference: TR 33.926 [4], clause S.2.2. 8 – Peer certificate validity checking.

Possible peers and interfaces for the gNB-CU-CP are AMF, gNB, gNB-CU-UP and gNB-DU, and N2, Xn, E1 and F1 interfaces respectively.

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

NOTE: This is based on the security functional requirement on the gNB given in clause 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 supports confidentiality, integrity and replay protection, the E1 interface between CU-CP and CU-UP is confidentiality, integrity and replay protected, the transport of control plane data over N2 is integrity, confidentiality and replay-protected and the transport of control plane data and user data over Xn is 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 S.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: This is based on the security functional requirement on the gNB given in clause 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 supports confidentiality, integrity and replay protection, the E1 interface between CU-CP and CU-UP is confidentiality, integrity and replay protected, the transport of control plane data over N2 is integrity, confidentiality and replay-protected and the transport of control plane data and user data over Xn is 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 S.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: This is based on the security functional requirement on the gNB given in clause 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 activates 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 S.2.2.6 – Security Policy Enforcement.

***Test Case**:*

Test Name: TC-UP-DATA-CIP-SMF_gNB-CU-CP

Purpose: To verify that activation of confidentiality protectionfor user data at the gNB is 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-CU-CP.

Execution Steps:

All execution steps are to be performed two times. Once with the UP security policies' ciphering protection in step 2 set to "required" and the second time set to "not needed".

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 capture the RRC Reconfiguration message sent by gNB-CU-CP to UE over NG RAN air interface.
5. The tester shall retrieve the UP ciphering protection indication present in the captured messages.
6. 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 Reconfiguration message and the gNB-CU-UP in the Bearer Context Setup Request message.

Expected Results:

Both the RRC connection Reconfiguration message and Bearer Context Setup Request message indicate that ciphering is to be used in line with the policy received from the SMF.

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: This is based on the security functional requirement on the gNB given in clause 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 activates 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 S.2.2.6 – Security Policy Enforcement.

Test Case*:*

Test Name: TC-UP-DATA-INT-SMF_gNB-CU-CP

Purpose: To verify that activation of integrity protection for user data packets is 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 is activated at the gNB-CU-CP.

Execution Steps:

All execution steps are to be performed two times. Once with the UP security policies' ciphering protection in step 2 set to "required" and the second time set to "not needed".

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 capture the RRC Reconfiguration message sent by gNB-CU-CP to UE over NG RAN air interface.
5. The tester shall retrieve the UP integrity protection indication present in the captured messages.
6. Tester shall check whether UP integrity policy received at gNB-CU-CP is same as the UP integrity protection indication notified by the gNB-CU-CP to the UE in the RRC Reconfiguration message and the gNB-CU-UP in the Bearer Context Setup Request message.

Expected Results:

Both the the RRC Reconfiguration message and Bearer Context Setup Request message indicate that integrity is to be used inline with the policy received from the SMF.

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-CP 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

5.4.1 Introduction

There are no gNB-CU-CP specific additions to clause 4.4.1 of TS 33.117 [2].

5.4.2 Port Scanning

There are no gNB-CU-CP specific additions to clause 4.4.2 of TS 33.117 [2].

5.4.3 Vulnerability scanning

There are no gNB-CU-CP specific additions to clause 4.4.3 of TS 33.117 [2].

5.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [2] are applicable to gNB-CU-CP.

The interface defined for the gNB-CU-CP are in clause 4.2.3 of TS 23.501 [7] and in clause 4.1 of TS 38.300 [8].

According to clause 4.4.4 of TS 33.117 [2], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for gNB-CU-CP, the following interfaces and protocols are in the scope of the testing:

For N2: the SCTP and NGAP protocols.

For Xn-C: the SCTP and XnAP protocols.

For F1-C: the SCTP and F1AP protocols.

For E1: the SCTP and E1AP protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 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 cases

6.2.1 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]

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 and in some cases small changes specific to the gNB-CU-UP:

4.2.2.1.5 UP integrity check failure

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

4.2.2.1.22 Checking expiry certificate

Threat Reference: TR 33.926 [4], clause T.2.2. 6 – Certificate expiry checking.

4.2.2.1.23 Peer certificate checking

Threat Reference: TR 33.926 [4], clause T.2.2. 5 – Peer certificate validity checking.

Possible peers and interfaces for the gNB-CU-UP are SEG/UPF, gNB, gNB-CU-CP and gNB-DU, and N3, Xn, E1 and F1 interfaces respectively.

6.2.2.1.2 Control plane data confidentiality protection over E1 interface

NOTE: This is based on the security functional requirement on the gNB given in clause 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 is confidentiality, integrity and replay protected as specified in TS 33.501 [3], clauses 5.3.10.

Threat References: TR 33.926 [4], clause T.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: This is based on the security functional requirement on the gNB given in clause 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 is confidentiality, integrity and replay protected as specified in TS 33.501 [3], clauses 5.3.10.

Threat References: TR 33.926 [4], clause T.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: This is based on the security functional requirement on the gNB given in clause 4.2.2.1.20 of TS 33.511 [6] but modified as the gNB-CU-UP supports the F1 interface.

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

Requirement Reference: TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

Requirement Description: The gNB supports confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane, the transport of user data over N3 is integrity, confidentiality and replay-protected, and the transport of control plane data and user data over Xn is integrity, confidentiality and replay-protected as specified in TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

Threat References: TR 33.926 [4], clause T.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 [2].

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

NOTE: This is based on the security functional requirement on the gNB given in clause 4.2.2.1.21 of TS 33.511 [6] but modified as the gNB-CU-UP supports the F1 interface.

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

Requirement Reference: TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

Requirement Description: The gNB supports confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane, the transport of user data over N3 is integrity, confidentiality and replay-protected, and the transport of control plane data and user data over Xn is integrity, confidentiality and replay-protected as specified in TS 33.501 [3], clauses 5.3.9, 9.3 and 9.4.

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

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

6.2.2.1.6 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 clause 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 [3], clause 5.3.3

Requirement Description: The gNB supports integrity protection and replay protection of user data between the UE and the gNB as specified in TS 33.501 [3], 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 T.2.2.4 – User plane data integrity protection.

***Test Case**:*

Test Name: TC-UP-DATA-INT_gNB-CU-UP

Purpose: To verify 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.
- The tester shall enable user plane integrity protection and ensure NIA0 is not used at the gNB-CU-UP network product.
- The 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 tester triggers the gNB-CU-CP to send a Bearer Context Setup Request message with integrity protection indication "on" to the gNB-CU-UP.
2. The tester checks that 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: This is based on the security functional requirement on the gNB given in clause 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 [3], clause 5.3.2

Requirement Description: The gNB supports ciphering of user data between the UE and the gNB as specified in TS 33.501 [3], clause 5.3.2.

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

Test Case:

Test Name: TC-UP-DATA-CIP_gNB

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

Pre-Condition:

- The gNB-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.
- The tester shall enable user plane confidentiality protection and ensure NEA0 is not used at the gNB-CU-UP network product.

Execution Steps:

1. The tester triggers the gNB-CU-CP to send a Bearer Context Setup Request message with ciphering protection indication "on" to the gNB-CU-UP.
2. The tester checks that 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 is confidentiality protected.

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-UP 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

6.4.1 Introduction

There are no gNB-CU-UP specific additions to clause 4.4.1 of TS 33.117 [2].

6.4.2 Port Scanning

There are no gNB-CU-UP specific additions to clause 4.4.2 of TS 33.117 [2].

6.4.3 Vulnerability scanning

There are no gNB-CU-UP specific additions to clause 4.4.3 of TS 33.117 [2].

6.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [2] are applicable to gNB-CU-UP.

The interface defined for the gNB-CU-UP are in clause 4.2.3 of TS 23.501 [7] and in clause 4.1 of TS 38.300 [8].

According to clause 4.4.4 of TS 33.117 [2], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for gNB-CU-UP, the following interfaces and protocols are in the scope of the testing:

For N3: the UDP and GTP-U protocols.

For Xn-U: the UDP and GTP-U protocols.

For F1-U: the UDP and GTP-U protocols.

For E1: the SCTP and E1AP protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 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]

7.2.2.1.1 Control plane data confidentiality protection over F1 interface

NOTE: This is based on the security functional requirement on the gNB given in clause 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 supports confidentiality, integrity and replay protection as specified in TS 33.501 [3], clauses 5.3.9.

Threat References: TR 33.926 [4], clause U.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: This is based on the security functional requirement on the gNB given in clause 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 supports confidentiality, integrity and replay protection as specified in TS 33.501 [3], clauses 5.3.9.

Threat References: TR 33.926 [4], clause U.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: This is based on the security functional requirement on the gNB given in clause 4.2.2.1.20 of TS 33.511 [6] but modified as the gNB-DU only supports the F1 interface.

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

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

Requirement Description: The gNB supports confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane as specified in TS 33.501 [3], clauses 5.3.9.

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

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

7.2.2.1.4 User plane data integrity protection over F1 interface

NOTE: This is based on the security functional requirement on the gNB given in clause 4.2.2.1.21 of TS 33.511 [6] but modified as the gNB-DU only supports the F1 interface.

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

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

Requirement Description: The gNB supports confidentiality, integrity and replay protection on the gNB DU-CU F1-U interface for user plane as specified in TS 33.501 [3], clauses 5.3.9.

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

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

7.2.2.1.5 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-DU by changing the gNB to gNB-DU for the entity under test in the test cases and with the below changes of threat reference and in some cases small changes specific to the gNB-DU:

4.2.2.1.22 Checking expiry certificate

Threat Reference: TR 33.926 [4], clause U.2.2. 6 – Certificate expiry checking.

4.2.2.1.23 Peer certificate checking

Threat Reference: TR 33.926 [4], clause U.2.2. 5 – Peer certificate validity checking.

Possible peers and interfaces for the gNB-DU are gNB-CU, gNB-CU-CP and gNB-CU-UP, and E1 and F1 interfaces respectively.

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

7.4.1 Introduction

There are no gNB-DU specific additions to clause 4.4.1 of TS 33.117 [2].

7.4.2 Port Scanning

There are no gNB-DU specific additions to clause 4.4.2 of TS 33.117 [2].

7.4.3 Vulnerability scanning

There are no gNB-DU specific additions to clause 4.4.3 of TS 33.117 [2].

7.4.4 Robustness and fuzz testing

The test cases under clause 4.4.4 of TS 33.117 [2] are applicable to gNB-DU.

The interface defined for the gNB-DU are in clause 4.1 of TS 38.300 [7].

According to clause 4.4.4 of TS 33.117 [2], the transport protocols available on the interfaces providing IP-based protocols need to be robustness tested. Following TCP/IP layer model and considering all the protocols over transport layer, for gNB-DU, the following interfaces and protocols are in the scope of the testing:

For F1-U: the UDP and GTP-U protocols.

For F1-C: the SCTP and F1AP protocols.

NOTE: There could be other interfaces and/or protocols requiring testing under clause 4.4.4 of TS 33.117 [2].

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2023-06	SA#100	SP-230573				Presented for approval	2.0.0
2023-06	SA#100					Upgrade to change control version	18.0.0
2023-06	SA#100					EditHelp review	18.0.1
2023-09	SA#101		0001	-	F	Adding the clause references to TS 33.523	18.1.0
2024-03	SA#103	SP-240364	0005	1	F	Clarification and simplification of test cases regarding UP CP and IP activation at split-gNB	18.2.0
2024-03	SA#103	SP-240364	0006	-	F	Clarification of test cases on user data IP and CP in split-gNB	18.2.0
2024-03	SA#103	SP-240368	0007	-	F	Correct clause references to TS 33.511	18.2.0
2024-03	SA#103	SP-240368	0008	-	F	Adding the missing Xn-U interface	18.2.0
2025-01	SA#106	SP-241798	0009	2	B	Adding certificate handling tests to SCAS for split gNB	19.0.0
2025-03	SA#107	SP-250098	0010	1	F	Finalising the certificate test for split gNBs	19.1.0
2025-07	SA#108	SP-250657	0012	-	F	Clean up of 33.523	19.2.0