ETSI TS 133 216 V15.2.0 (2020-01)

LTE;
Security Assurance Specification (SCAS)
for the evolved Node B (eNB) network product class
(3GPP TS 33.216 version 15.2.0 Release 15)

Reference
RTS/TSGS-0333216vf20

Keywords
LTE,SECURITY

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Legal Notice

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

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

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

Modal verbs terminology

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

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

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

The present document contains objectives, requirements and test cases that are specific to the eNB network product class. It refers to the Catalogue of General Security Assurance Requirements and formulates specific adaptions of the requirements and test cases given there, as well as specifying requirements and test cases unique to the eNB 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 TR 33.117 (Release 15): "Catalogue of general security assurance requirements".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

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

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

4 eNodeB-specific security requirements and related test cases

4.1 Introduction

eNodeB specific security requirements include both requirements derived from eNodeB-specific security functional requirements as well as security requirements derived from threats specific to eNB 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 eNodeB-specific security functional adaptations of requirements and related test cases

4.2.1 Introduction

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

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

4.2.2.1 Security functional requirements on the eNodeB deriving from 3GPP specifications – TS 33.401 [3]

4.2.2.1.1 Control plane data confidentiality protection

Requirement Name: Control plane data confidentiality protection

Requirement Reference: TS 33.401 [3], clause 5.3.4a

Requirement Description: "The eNB shall provide confidentiality protection for control plane packets on the S1/X2 reference points." as specified in TS 33.401 [3], clause 5.3.4a.

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

Test Case:

The requirement mentioned in this clause is tested in accordance to the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [2].

4.2.2.1.2 Control plane data integrity protection

Requirement Name: Control plane data integrity protection

Requirement Reference: TS 33.401 [3], clause 5.3.4a

Requirement Description: "The eNB shall provide integrity protection for control plane packets on the S1/X2 reference points." as specified in TS 33.401 [3], clause 5.3.4a.

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

Test Case:

The requirement mentioned in this clause is tested in accordance to the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [2].

4.2.2.1.3 User plane data ciphering and deciphering at the eNB

Requirement Name: User plane data ciphering and deciphering at the eNB

Requirement Reference: TS 33.401 [3], clause 5.3.4

Requirement Description: "The eNB shall cipher and decipher user plane packets between the Uu reference point and the S1/X2 reference points." as specified in TS 33.401 [3], clause 5.3.4.

Threat References: TR 33.926 [4], clause C.2.2.3 – User plane data ciphering and deciphering at the eNB.

Test Case:

The requirement mentioned in this clause is tested in accordance to the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [2].

4.2.2.1.4 User plane data integrity protection

Requirement Name: User plane data integrity protection

Requirement Reference: TS 33.401 [3], clause 5.3.4

Requirement Description: "The eNB shall handle integrity protection for user plane packets for the S1/X2 reference points." as specified in TS 33.401 [3], clause 5.3.4.

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

Test Case:

The requirement mentioned in this clause is tested in accordance to the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [2].

4.2.2.1.5 AS algorithms selection

Requirement Name: AS algorithms selection

Requirement Reference: TS 33.401 [3], clause 7.2.4.1; TS 33.401 [3], clause 7.2.4.2.1

Requirement Description: " The serving network shall select the algorithms to use dependent on: the UE security capabilities of the UE, and the configured allowed list of security capabilities of the currently serving network entity." as specified in TS 33.401 [3], clause 7.2.4.1".

"Each eNB shall be configured via network management with lists of algorithms which are allowed for usage. There shall be one list for integrity algorithms, and one for ciphering algorithms. These lists shall be ordered according to a priority decided by the operator." as specified in TS 33.401 [3], clause 7.2.4.2.1.

Threat References: TBA

Test Case:

Purpose:

Verify that the eNB select the algorithm with the highest priority in its configured list.

Pre-Conditions:

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

Execution Steps

1) The UE sends attach request message to the eNB.
2) The eNB receives S1 context setup request message.
3) The eNB sends the SECURITY MODE COMMAND message.
4) The UE replies with the AS SECURITY MODE COMPLETE message.

Expected Results:

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

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

Expected format of evidence:

Sample copies of the log files.

4.2.2.1.6 Verify RRC integrity protection

Requirement Name: The check of RRC integrity

Requirement Reference: TS 33.401 [3], clause 7.4.1

Requirement Description: " The supervision of failed RRC integrity checks shall be performed both in the ME and the eNB. In case of failed integrity check (i.e. faulty or missing MAC-I) is detected after the start of integrity protection, the concerned message shall be discarded. " as specified in TS 33.401 [3], clause 7.4.1.

Threat References: TBA

Test Case:

Purpose:

Verify that the message is discarded in case of failed integrity check (i.e. faulty or missing MAC-I).

Pre-Conditions:

Test environment with RRC Protection is activated at the eNB.

Execution Steps

Positive:

The eNB receives a RRC message with a right MAC-I.

Negative:

The eNB receives a RRC message with a wrong MAC-I or missing MAC-I.

Expected Results:

The RRC message is discarded in the negative test.

Expected format of evidence:

Sample copies of the log files.

4.2.2.1.7 The selection of EIA0

Requirement Name: The selection of EIA0

Requirement Reference: TS 33.401 [3], clause 5.1.4.2

Requirement Description: " EIA0 is only allowed for unauthenticated emergency calls " as specified in TS 33.401 [3], clause 5.1.4.2.

Threat References: TBA

Test Case:

Purpose:

Verify that AS NULL integrity algorithm is used correctly.

Pre-Conditions:

Test environment with a UE. The UE may be simulated.

The vendor shall provide documentation describing how EIA0 is disabled or enabled.

Execution Steps

Positive:

1) The eNB receives a UE security capability only containing EIA0 from S1 context setup message.

2) The eNB sends AS SMC to the UE.

Negative:

1) The eNB receives a UE security capability that contains EIA0 and other integrity algorithm(s).

2) The eNB sends AS SMC to the UE.

Expected Results:

EIA0 is only selected in the Positive test.

Expected format of evidence:

Sample copies of the log files.

4.2.2.1.8 Key refresh at the eNB

Requirement Name: Key refresh at the eNB

Requirement Reference: TS 33.401 [3], clause 7.2.9.1

Requirement Description: "Key refresh shall be possible for K_{eNB}, $K_{RRC-enc}$, $K_{RRC-int}$, K_{UP-int}, and K_{UP-enc} and shall be initiated by the eNB when a PDCP COUNTs is about to be re-used with the same Radio Bearer identity and with the same K_{eN}. " as specified in TS 33.401 [3], clause 7.2.9.1.

Threat References: TBA

Test Case:

Purpose:

Verify that the eNB performs K_{eNB} refresh when PDCP COUNTs are about to wrap around.

Pre-Conditions:

UE may be simulated.

Execution Steps

1) The eNB sends AS SMC to the UE, and the UE response AS SMC.

2) UE sends RRC messages or UP messages to the eNB with a PDCP COUNT that is about to wrap around. UE continue sending RRC messages or UP messages with an increasing PDCP COUNT until step 3 occurs or PDCP COUNT wraps around.

3) The eNB triggers intra-cell handover.

Expected Results:

The eNB triggers intra-cell handover to get a new KeNB.

Expected format of evidence:

Part of log that shows the PDCP COUNT wrap around and the intra-cell handover. This part can be presented for example as a screenshot.

4.2.2.1.9 AS Security Mode Command Procedure

Requirement Name: AS integrity algorithm selection

Requirement Reference: TS 33.401 [3], clause 7.4.2

Requirement Description: The eNB shall protect the SECURITY MODE COMMAND message with the integrity algorithm, which has the highest priority according to the ordered lists.

Threat References: TBA

Test Case:

Purpose:

Verify that AS integrity protection algorithm is selected and applied correctly.

Pre-Conditions:

Test environment with UE. UE may be simulated.

Execution Steps:

The eNB sends the SECURITY MODE COMMAND message. The UE replies with the SECURITY MODE COMPLETE message.

Expected Results:

1. The eNB has selected the integrity algorithm which has the highest priority according to the ordered lists and is contained in the UE EPS security capabilities. The eNB checks the message authentication code on the SECURITY MODE COMPLETE message.
2. The MAC in the SECURITY MODE COMPLETE is verified, and the AS integrity protection algorithm is selected and applied correctly.

Expected format of evidence:

Snapshots containing the result.

4.2.2.1.10 Bidding down prevention in X2-handovers

Requirement Reference: TBA

Requirement Description: "In the path-switch message, the target eNB shall send the UE EPS security capabilities received from the source eNB to the MME." as specified in TS 33.401 [3], clause 7.2.4.2.2."

Threat References: TBA

Test Case:

Purpose:

Verify that bidding down is prevented in X2-handovers.

Pre-Conditions:

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

Execution Steps:

The target eNB sends the path-switch message to the MME.

Expected Results:

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

Expected format of evidence:

Snapshots containing the result

4.2.2.1.11 AS protection algorithm selection in eNB change

Requirement Name: AS protection algorithm selection in eNB change.

Requirement Reference: TS 33.401 [3], clause 7.2.4.2.2, and clause 7.2.4.2.3

Requirement Description: "The target eNB shall select the algorithm with highest priority from the UE EPS security capabilities according to the prioritized locally configured list of algorithms (this applies for both integrity and ciphering algorithms). The chosen algorithms shall be indicated to the UE in the handover command if the target eNB selects different algorithms compared to the source eNB" as specified in TS 33.401 [3], clause 7.2.4.2.2, and clause 7.2.4.2.3.

Threat References: TBA

Test Case:

Purpose:

Verify that AS protection algorithm is selected correctly.

Pre-Conditions:

Test environment with source eNB, target eNB and MME. Source eNB and MME may be simulated.

Execution Steps:

Test Case 1:

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

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

Test Case 2:

MME sends the UE EPS security capability to the Target eNB.

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

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

Expected Results:

For both test cases:

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

Expected format of evidence:

Snapshots containing the result.

4.2.2.1.12 RRC and UP downlink ciphering at the eNB

Requirement Name: RRC and UP downlink ciphering at the eNB.

Requirement Reference: TS 33.401 [3], clause 7.2.4.5

Requirement Description: "The eNB shall start RRC and UP downlink ciphering after sending the AS security mode command message" .

Threat References: TBA

Test Case:

Test Name: TC_eNB_DL_Cipher

Purpose: To verify that the eNB performs RRC and UP downlink ciphering after sending the AS security mode command message.

Pre-Condition:

- The UE and eNB network products are connected in the test environment. UE may be simulated.

- The tester shall have access to the AS security context and the corresponding cryptographic keys (e.g. RRC and UP cipher keys).
- The tester have access to Uu interface and ability to capture the Uu interface messages with the debug port enabled in the UE.

Execution Steps:

1) The tester shall POWER ON the UE to trigger the registration procedures (Attach and SMC).
2) The tester performs packet capturing over the Uu interface using any packet analyser.
3) The tester filters the AS SMC command message and the following RRC and UP downlink packets from eNB to UE.
4) The tester proceeds the testing based on the parameters (algorithm identifier and algorithm distinguisher) present in the AS SMC command message.

   Case 1: If the parameters refer to null ciphering algorithm, the tester verifies that the downlink packets filtered in step 3 are unciphered.

   Case 2: If the parameters refer to algorithms such as SNOW, AES, ZUC, the tester verifies that the downlink packets filtered in step 3 are ciphered.

   The tester also checks if the packets are ciphered in accordance with the selected algorithm stated in the AS SMC command message.

NOTE: The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.3.2.4 of TS 33.117 [2].

Expected Results:

- The downlink packets following the AS SMC command message are ciphered except NULL ciphering algorithm case.

Expected format of evidence:

Evidence suitable for the interface, e.g. Screenshot contains the operation results.

4.2.3 Technical Baseline

4.2.3.1 Introduction

The present clause provides baseline technical requirements.

4.2.3.2 Protecting data and information

4.2.3.2.1 Protecting data and information – general

There are no eNB-specific additions to clause 4.2.3.2.1 of TS 33.117 [2].

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no eNB-specific additions to clause 4.2.3.2.2 of TS 33.117 [2].

4.2.3.2.3 Protecting data and information in storage

There are no eNB-specific additions to clause 4.2.3.2.3 of TS 33.117 [2].

4.2.3.2.4 Protecting data and information in transfer

There are no eNB-specific additions to clause 4.2.3.2.4 of TS 33.117 [2].

4.2.3.2.5 Logging access to personal data

The requirement and testcases in clause 4.2.3.2.5 of TS 33.117 [2] is not applicable to eNB network product.

4.2.3.3 Protecting availability and integrity

There are no eNB-specific additions to clause 4.2.3.3 of TS 33.117 [2].

4.2.3.4 Authentication and authorization

There are no eNB-specific additions to clause 4.2.3.4 of TS 33.117 [2].

4.2.3.5 Protecting sessions

There are no eNB-specific additions to clause 4.2.3.5 of TS 33.117 [2].

4.2.3.6 Logging

There are no eNB-specific additions to clause 4.2.3.6 of TS 33.117 [2].

4.2.4 Operating Systems

eNB-specific additions to clause 4.2.4 of TS 33.117 [2] are:

For the requirement defined in clause 4.2.4.1.1.2 Handling of ICMP of TS 33.117[2]:

- Echo Reply can be sent by default.
- In case of remote base station auto deployment, Router Advertisement can be processed.

Apart from the above exceptions, there are no eNB-specific addtions to clause 4.2.4 of TS 33.117 [2].

4.2.5 Web Servers

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

4.2.6 Network Devices

4.2.6.1 Protection of Data and Information

There are no eNB-specific additions to clause 4.2.6 of TS 33.117 [2].

4.2.6.2 Protecting availability and integrity

4.2.6.2.1 Packet filtering

There are no eNB-specific additions to clause 4.2.6.2.1 of TS 33.117 [2].

4.2.6.2.2 Interface robustness requirements

There are no eNB-specific additions to clause 4.2.6.2.2 of TS 33.117 [2].

4.2.6.2.3 GTP-C Filtering

The requirement and test case in clause 4.2.6.2.3 of TS 33.117 [2] are not applicable to eNB network products.

4.2.6.2.4 GTP-U Filtering

There are no eNB-specific additions to clause 4.2.6.2.4 of TS 33.117 [2].

4.2.7 Void

4.3 eNodeB-specific adaptations of hardening requirements and related test cases

4.3.1 Introduction

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

4.3.2 Technical Baseline

There are no eNB-specific additions to clause 4.3.2 of TS 33.117 [2].

4.3.3 Operating Systems

There are no eNB-specific additions to clause 4.3.3 of TS 33.117 [2].

4.3.4 Web Servers

There are no eNB-specific additions to clause 4.3.4 of TS 33.117 [2].

4.3.5 Network Devices

There are no eNB-specific additions to clause 4.3.5 of TS 33.117 [2].

4.3.6 Void

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

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

Annex A (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
09-2017	SA#77					Presented for information and approval	1.0.0
09-2017	SA#77					Upgrade to change control version + EditHelp editorial changes added	15.0.0
2019-09	SA#85	SP-190681	0003	1	F	Update requirements and test cases foreNB SCAS	15.1.0
2019-12	SA#86	SP-191139	0005	1	F	Corrections for clean-up and alignment R15	15.2.0

History

Document history		
V15.0.0	September 2018	Publication
V15.1.0	October 2019	Publication
V15.2.0	January 2020	Publication