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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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