ETSI TS 133 216 V18.1.0 (2024-05)

LTE;
Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class (3GPP TS 33.216 version 18.1.0 Release 18)

Reference
RTS/TSGS-0333216vi10

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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 https://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".

[5] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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 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].

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 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 eNB.

Test Case:

Test Name: TC-DATA-CIP-eNB-Uu

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

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE and the MME may be simulated,
- The tester can capture the messages via the air interface.
- The tester shall enable the user plane ciphering protection and ensure EEA0 is not used.

Execution Steps:

1. The UE sends an attach request to the MME.
2. The MME sends a KeNB and the UE security capability to the eNB.
3. eNB selects an algorithm and sends AS SMC to the UE,
4. eNB receive AS SMP from the UE.

Expected Results:

User plane packets sent by the eNB after eNB sending AS SMC is ciphered.

Expected format of evidence:

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

Test Name: TC-DATA-CIP-eNB-S1/X2

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 selects the algorithms 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.

Security Objective 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; TS 36.331 [5], clause 5.3.1.2.

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_{eNB}. " as specified in TS 33.401 [3], clause 7.2.9.1.

Moreover, "The eNB is responsible for avoiding reuse of the COUNT with the same RB identity and with the same K_{eNB}, e.g. due to the transfer of large volumes of data, release and establishment of new RBs. In order to avoid such re-use, the eNB may e.g. use different RB identities for successive RB establishments, trigger an intra cell handover or by triggering a transition from RRC_CONNECTED to RRC_IDLE or RRC_INACTIVE and then back to RRC_CONNECTED." as specified in TS 36.331 [x], clause 5.3.1.2.

Threat References: TR 33.926[4], clause C.2.3.1 – Key reuse for eavesdropping

Test Case 1:

Test Name: TC_ENB_KEY_REFRESH_ PDCP_COUNT

Purpose:

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

Pre-Conditions:

The UE may be simulated.

Execution Steps

1) The eNB sends AS Security Mode Command message to the UE, and the UE respondswith the AS ecurity Sode Momplete messageC.
2) The UE sends RRC messages or UP messages to the eNB with an increasing PDCP COUNT until the value wraps around.

Expected Results:

The eNB triggers an intra-cell handover and takes a new K_{eNB} into use.

Expected format of evidence:

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

Test Case 2:

Test Name: TC_ENB_KEY_REFRESH_DRB_ID

Purpose:

Verify that the eNB performs K_{eNB} refresh when DRB-IDs are about to be reused under the following conditions:

- the successive Radio Bearer establishment uses the same RB identity while the PDCP COUNT is reset to 0, or
- the PDCP COUNT is reset to 0 but the RB identity is increased after multiple calls and wraps around.

Pre-Conditions:

The UE and MME may be simulated.

Execution Steps

1) The eNB sends the AS Security Mode Command message to the UE.
2) the UE responds with the AS Security Mode Complete message.
3) A DRB is set up.
4) DRB is set up and torn down for multiple times within one active radio connection without the UE going to idle (e.g. by the UE making multiple IMS calls, or by the MME requesting bearer setup and bearer deactivation), until the DRB ID is reused.

Expected Results:

Before DRB ID reuse, the eNB takes a new K_{eNB} into use by e.g. triggering an intra-cell handover or triggering a transition from RRC_CONNECTED to RRC_IDLE or RRC_INACTIVE and then back to RRC_CONNECTED.

Expected format of evidence:

Part of log that shows all the DRB identities and the intra-cell handover or the transition from RRC_CONNECTED to RRC_IDLE or RRC_INACTIVE and then back to RRC_CONNECTED. 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: TS 33.401 [3], clause 7.2.4.2.2

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 has 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.

4.2.2.1.13 Map a UE NR security capability

Requirement Name: Map a UE NR security capability

Requirement Reference: TS 33.401 [3], clause E.3.10.2

Requirement Description: " The MeNB that does not have the UE NR security capabilities shall create them as follow:

- Set the support of NEA0, 128-NEA1, 128-NEA2, 128-NEA3, NIA0, 128-NIA1, 128-NIA2, 128-NIA3 to the same as EEA0, 128-EEA1, 128-EEA2, 128-EEA3, EIA0, 128-EIA1, 128-EIA2, 128-EIA3 respectively; and

- Set the rest of the bits to 0." as specified in TS 33.401 [3], clause E.3.10.2.

Threat References: TBA

Test Case:

Test Name: TC_MAP_NR_SEC_CAP

Purpose: To verify that the eNB creates mapped UE NR security capabilities.

Pre-Condition:

- The eNB and gNB network products are connected in the test environment. The gNB may be simulated.
- Tester shall have access to trigger dual connection to a gNB.
- The Tester shall have access to the X2 interface.

Execution Steps:

1) The MeNB does not receive UE NR security capabilities from S1 Initial Context Setup Request message.
2) The MeNB sends SN Addition Request Message to the SgNB.
3) The tester checkes if the NR security capabilities are included in SN Addition Request Message.

Expected Results:

The SN Addition Request Message contains UE NR security capabilities, i.e. NEA0, 128-NEA1, 128-NEA2, 128-NEA3, NIA0, 128-NIA1, 128-NIA2, 128-NIA3

Expected format of evidence:

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

4.2.2.1.14 UE NR security capability is only sent to a SgNB

Requirement Name: UE NR security capability is only sent to a SgNB

Requirement Reference: TS 33.401 [3], clause E.3.4.3

Requirement Description: "When adding SgNB while establishing an EN-DC connection, the MeNB shall send these created UE NR security capabilities to the SgNB. Other than for adding an SgNB, the created UE NR security capabilities shall not be sent from the MeNB." as specified in TS 33.401 [3], clause E.3.4.3.

Threat References: TBA

Test Case:

Test Name: TC_NR_SEC_CAP_SENT

Purpose: To verify that the UE NR security capabilities are only sent to a SgNB.

Pre-Condition:

- The UE, gNB and eNB network products are connected in the test environment. UE and gNB may be simulated.
- The tester shall have access to the X2 interface.

Execution Steps:

1) The tester triggers MeNB to send SN addition Request message to a SgNB.
2) The tester triggers UE HO from MeNB to another eNB.
3) The tester checks if the UE NR security capabilities were sent in the X2 interface in both step 1 and step 2.

Expected Results:

The UE NR security capabilities are only sent to the SgNB.

Expected format of evidence:

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

4.2.2.1.15 Bidding down prevention in X2-handovers when target eNB receives a NR security capability

Requirement Reference: TS 33.401 [3], clause E.3.4.3

Requirement Description: " A target eNB that has received the UE NR security capabilities during handover shall include the UE NR security capabilities in the S1-PATH SWITCH-REQUEST message." as specified in TS 33.401 [3], clause E.3.4.3."

Threat References: TBA

Test Case:

Test Name: TC_BID_DOWN_X2

Purpose:

Verify that bidding down is prevented in X2-handovers when target eNB receives a NR security capability.

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 NR security capability is in the path-switch message.

Expected format of evidence:

Snapshots containing the result.

4.2.2.1.16 Integrity protection of user data between the UE and the eNB

Requirement Name: Integrity protection of user data between the UE and the eNB.

Requirement Reference: TS 33.401 [3], clause 5.1.4.

*Requirement Description: "*User plane packets between the eNB and the UE may be integrity protected on the Uu interface. *" in clause 5.1.4*

Threat References: TBD

Test Case*:*

Test Name: TC-UP-DATA-INT_eNB

Purpose: To verify that the user data packets are integrity protected over the Uu interface.

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE may be simulated.
- The tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.
- The tester shall enable user plane integrity protection and ensure that EIA0 is disabled at the eNB.

Execution Steps:

1. The tester triggers the eNB to send a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.
2. The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and while the UE is in active state is integrity protected.

Expected Results:

Any user plane packets sent between UE and eNB over the Uu interface after eNB sending RRCConnectionReconfiguration is integrity protected.

Expected format of evidence:

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

4.2.2.1.17 Local UP integrity protection configuration

Requirement Name: Select the right UP integrity protection policy.

Requirement Reference: TS 33.401 [2] clause 7.3.3

Requirement Description: " The eNB shall be locally configured with UP integrity protection policy. " in clause 7.3.3

Threat References: TBD

Test Case*:*

Test Name: TC_LOCAL_UP_INTEGRITY_PROTECTION_CONFIGURATION

Purpose: To verify that the eNB is locally configured with a UP integrity protection policy

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE and MME may be simulated.
- The eNB is locally configured to activate UP integrity protection by default if no UP integrity protection policy is received from MME.
- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.
- The tester shall disable EIA0 at the eNB.

Execution Steps:

1. The tester triggers the MME to send an EPS security capability message with EIA7 indicating the UP integrity protection is supported by the UE to the eNB. But the tester also configures the MME to not send a UP integrity protection policy to the eNB.
2. The eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.
3. The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and while the UE is in active state is integrity protected.

Expected Results:

Any user plane packets sent between UE and eNB over the Uu interface after eNB sending the RRCConnectionReconfiguration message is integrity protected.

Expected format of evidence:

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

Text of local configuration of the UP intergrity protection at the eNB.

4.2.2.1.18 UP IP policy selection

Requirement Name: Select the right UP IP policy.

Requirement Reference: TS 33.401 [2] clause 7.3.3

Requirement Description: " If the eNB receives UP integrity protection policy from the MME, the eNB shall use the received UP integrity protection policy, otherwise, the eNB shall use the locally configured UP integrity protection policy if EIA7 in the EPS security capability indicates that the UE supports user plane integrity protection with EPC. " in clause 7.3.3

Threat References: TBD

***Test Case**:*

Test Name: TC_ UP_IP_POLICY_Selection

Purpose: To verify that the UP IP policy sent from the MME is used by the eNB.

Pre-Condition:

- The eNB network product shall be connected in emulated/real network environments. UE and MME may be simulated.
- The eNB locally UP IP is set to NOT NEEDED.
- Tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.
- The tester shall disable EIA0 at the eNB.

Execution Steps:

1. The tester triggers the MME to send a EPS security capability message with EIA7 indicating the UP IP is supported by the UE to the eNB. But the tester also configures the MME to send a UP IP policy with REQUIRED to the eNB.
2. The eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.
3. The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and while the UE is in active state is integrity protected.

Expected Results:

Any user plane packets sent between UE and eNB over the Uu interface after eNB sending the RRCConnectionReconfiguration message is integrity protected according to the UP IP policy sent by the MME.

Expected format of evidence:

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

4.2.2.1.19 UP IP policy selection in S1 Handover

Requirement Name: Select the right UP IP policy in S1 handover.

Requirement Reference: TS 33.401 [2] clause 7.3.3

Requirement Description: " At an S1-handover, the source MME shall send the UE's UP integrity protection policy and the UE EPS security capability to the target eNB via the target MME. Besides, the source eNB shall also send the UE's UP integrity protection policy if received from the source MME to the target eNB in a source-to-target container. The target eNB shall use the UE capability indicating support of UP IP in EPS together with the UP integrity protection policy received from the MME and ignore the UP integrity protection received in the source-to-target container. If the target eNB does not receive the UP integrity protection policy from the MME, the target eNB shall use the UE

capability indicating support of UP IP in EPS together with the UP integrity protection policy received from the source eNB. If both policies from MME and source eNB are absent, but EIA7 in the EPS security capability indicates that the UE supports use of user plane protection with EPC, the eNB shall use locally configured UP integrity protection policy." in clause 7.3.3

Threat References: TR 33.926 [4], clause C.2.2.a, UP integrity protection policy selection

***Test Case**:*

Test Name: TC_ UP_IP_POLICY_Selection_S1_Handover

Purpose: To verify that the eNB has correct selection on UP IP policy in S1 handover

Pre-Condition:

- The target eNB network product shall be connected in emulated/real network environments. UE, source eNB and MME may be simulated.
- The target eNB locally UP IP is set to NOT NEEDED.
- The tester shall have knowledge of integrity algorithm and integrity protection keys.
- The tester can capture the message via the Uu interface, or can capture the message at the UE.

Execution Steps:

Test Case 1:

1) The tester triggers the source MME to send EPS security capability with EIA7 to the target eNB indicating the UP IP is supported by the UE. Furthermore, the tester triggers the source MME to send a UP IP policy with REQUIRED to the target eNB.
2) The source eNB sends UP IP policy with NOT NEEDED in the source-to-target container to the target eNB.
3) The target eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.
4) The tester checks that any user data sent by the target eNB after sending the RRCConnectionReconfiguration message and before UE enters CM-Idle state is integrity protected.

Test Case 2:

1) The tester triggers the source MME to send EPS security capability with EIA7 to the target eNB indicating the UP IP is supported by the UE. Furthermore, the tester prepares the MME to not send a UP IP policy to the target eNB.
2) The source eNB sends UP IP policy with REQUIRED in the source-to-target container to the target eNB.
3) The target eNB sends a RRCConnectionReconfiguration message with integrity protection indication "on" to the UE.
4) The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and before UE enters CM-Idle state is integrity protected.

Test Case 3:

1) The tester configures the target eNB to make sure the local UP IP is set to REQUIRED.
2) The tester triggers the source MME to send EPS security capability with EIA7 to the target eNB indicating the UP IP is supported by the UE. Furthermore, the tester prepares the MME to not send a UP IP policy to the target eNB.
2) The source eNB does not send UP IP policy in the source-to-target container to the target eNB.
3) The target eNB sends a RRCConnectionReconfiguration message with integrity protection indication "off to the UE ".

4) The tester checks that any user data sent by eNB after sending the RRCConnectionReconfiguration message and before UE enters CM-Idle state is not integrity protected.

Expected Results:

For all test cases, any user plane packets sent between UE and eNB over the Uu interface after eNB sending the RRCConnectionReconfiguration message are integrity protected.

Expected format of evidence:

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

For each test case: Configuration of UP IP of target eNB, source eNB and UP IP policy sent by MME.

4.2.2.1.20 Bidding down prevention for UP IP Policy

Requirement Reference: TS 33.401 [3], clause 7.3.3

Requirement Description: "*Further, in the Path-Switch message, the target eNB shall send the UE's UP integrity protection policy and corresponding E-RAB ID to the MME. The sent UP integrity protection policy can either be the one received from source eNB or the locally configured one if the target eNB does not receive it from the source eNB, but the EIA7 in the EPS security capability indicates that the UE supports user plane integrity protection with EPC.* " as specified in TS 33.401 [3], clause 7.3.3.

Threat References: TR 33.926 [4], clause C.2.2.a, bidding down for UP IP Policy

Test Case:

Purpose:

Verify that bidding down for UP IP policy is prevented in X2-handovers.

Pre-Conditions:

- The target eNB network product shall be connected in emulated/real network environments. UE, source eNB and MME may be simulated.

Execution Steps:

Test Case 1:

- The tester configures the target eNB with UP IP set to NOT NEEDED.
- The tester triggers the source eNB to send EPS security capability with EIA7 to the MME indicating the UP IP is supported and UP IP policy with REQUIRED in Handover Request message to the target eNB.
- The target eNB sends path-switch request message with UP IP policy with REQUIRED to the MME.

Test Case 2:

- The tester configures the target eNB with UP IP set to REQUIRED.
- The tester triggers the source eNB to send EPS security capability with EIA7 to the MME indicating the UP IP is supported in Handover Request message to the target eNB. The tester prepares the source eNB to not send UP IP policy in the Handover Request message.
- The target eNB sends path-switch request message with UP IP policy with REQUIRED to the MME.

Expected Results:

For both test casees, the UP IP policy with REQUIRED is in the path-switch request message.

Expected format of evidence:

Snapshots containing the result.

For each test case: Configuration of UP IP of target eNB, source eNB and UP IP policy sent by MME.

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

4.2.3.4.1 Authentication attributes

eNB-specific adaptation to clause 4.2.3.4.2.1 of TS 33.117 [2] is:

- Dual-factor authentication by combining several authentication options as noted in clause 4.2.3.4.2.1 of TS 33.117 [2] for higher level of security is not applicable to the eNB.

Apart from the above exception, there are no other eNB-specific adaptations to clause 4.2.3.4.2 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 testcase in clause 4.2.6.2.3 of TS 33.117 [2] is not applicable to eNB network product.

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**
2017-09	SA#77					Presented for information and approval	1.0.0
2017-09	SA#77					Upgrade to change control version + EditHelp editorial changes added	15.0.0
2018-12	SA#82	SP-181030	0002	1	B	Add EDCE5 related requirements and testcases to 33.216	16.0.0
2019-09	SA#85	SP-190681	0004	-	A	Update requirements and test cases foreNB SCAS	16.1.0
2019-12	SA#86	SP-191139	0006	1	A	Corrections for clean-up and alignment R16	16.2.0
2020-03	SA#87E	SP-200139	0013	1	B	Complete the test cases of key refresh at the eNB	16.3.0
2020-07	SA#88E	SP-200358	0015	-	F	Update eNB SCAS testcase	16.4.0
2020-09	SA#89e	SP-200702	0017	-	A	eNB-specific adaptation to account protection by authentication attribute R16	16.5.0
2021-06	SA#92e	SP-210449	0022	-	F	Address ENs in TS 33.216	16.6.0
2021-09	SA#93e	SP-210849	0023	-	F	An editoral change to TS 33.216	16.7.0
2023-01	SA#98e					Upgrade to Rel-17	17.0.0
2023-06	SA#100	SP-230604	0025	-	B	Updates to eNB SCAS for the support of UP IP	18.0.0
2024-03	SA#103	SP-240369	0026	-	F	Clarification of UP Integrity Protection test cases for eNB	18.1.0
2024-03	SA#103	SP-240369	0027	-	F	Clarification of UP IP selection and bidding down prevention of eNB	18.1.0

History

Document history		
V18.1.0	May 2024	Publication