ETSI TS 133 116 V16.1.0 (2022-01)

LTE;
Security Assurance Specification (SCAS)
for the MME network product class
(3GPP TS 33.116 version 16.1.0 Release 16)

Reference
RTS/TSGS-0333116vg10

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 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 MME 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 MME 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 41.001: "GSM Specification set".

[3] 3GPP TR 33.117: "Catalogue of General Security Assurance Requirements".

[4] 3GPP TR 33.916: "Security assurance scheme for 3GPP network products for 3GPP network product classes".

[5] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[6] void.

[7] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[8] 3GPP TS 33.102: "3G security; Security architecture".

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].

MME Application: The running processes (typically more than one) executing the software package for the MME functions and OAM functions of the MME network product model.

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 MME-specific security requirements and related test cases

4.1 Introduction

The structure of the present TS 33.116 is aligned with TS 33.117 such that the MME-specific adaptation of a generic requirement in 33.sas, clause 4.a.b.c.d, can be always found in TS 33.116, clause 4.a.b.c.d. The text on pre-requisites for testing in clause 4.1.2 of TS 33.117 [3] applies also to the present document.

4.2 MME-specific adaptations of security functional requirements and related test cases

4.2.1 Introduction

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

4.2.2.1 Security functional requirements on the MME deriving from 3GPP specifications – general approach

In addition to the requirements and test cases in TS 33.117, clause 4.2.2, an MME shall satisfy the following:

It is assumed for the purpose of the present SCAS that an MME conforms to all mandatory security-related provisions pertaining to an MME in:

- 3GPP TS 33.401: "EPS security architecture";
- other 3GPP specifications that make reference to TS 33.401 or are referred to from TS 33.401 (e.g. TS 23.401 [7]).

Security procedures pertaining to an MME are typically embedded in mobility management procedures and are hence assumed to be tested together with them. Examples include:

- AKA authentication is embedded in an Attach procedure or a TAU procedure.
- Security Mode Control is embedded in an Attach procedure or a TAU procedure.
- The derivation of a mapped security context is embedded in inter-RAT mobility procedures.

4.2.2.2 Authentication and key agreement procedure

4.2.2.2.1 Access with 2G SIM forbidden

Requirement Name: 2G SIM access forbidden

Requirement Reference: TBA

Requirement Description: "Access to E-UTRAN with a 2G SIM or a SIM application on a UICC shall not be granted." as specified in TS 33.401, clause 6.1.1.

Threat References: TBA

Security Objective References: TBA

Test Case:

Purpose:

Verify that access to EPS with a 2G SIM is not possible.

Pre-Conditions:

Test environment with HSS. HSS may be simulated.

Execution Steps

Include 2G authentication vector in *authentication data response* from HSS.

Expected Results:

MME rejects UE authentication when receiving 2G authentication vector from HSS.

NOTE: When both MME and HSS function correctly 2G authentication vector are never included in authentication data response from HSS to MME.

4.2.2.2.2 Re-synchronization

Requirement Name: Inclusion of RAND, AUTS

Requirement Reference: TBA

Requirement Description: "In the case of a synchronization failure, the MME shall also include RAND and AUTS." as specified in TS 33.401, clause 6.1.2.

Threat References: TBA

Security Objective References: TBA

Test Case: **Purpose:**

Verify that Re-synchronization procedure works correctly.

Pre-Conditions:

Test environment with UE and HSS. UE and HSS may be simulated.

Execution Steps

The MME receives an AUTHENTICATION FAILURE message, with the EMM cause #21 "synch failure" and a re-synchronization token AUTS.

Expected Results:

The MME includes the stored RAND and the received AUTS in the *authentication data request* to the HSS.

NOTE: When RAND and AUTS are not included in the authentication data request to the HSS then the HSS will return a new authentication vector (AV) based on its current value of the sequence number SQN_{HE} (cf. TS 33.102, clause 6.3.5) A new authentication procedure between MME and UE using this new AV will be successful just the same if the cause of the synchronisation failure was the sending of a "stale" challenge, i.e. one that the UE had seen before or deemed to be too old. But if the cause of the synchronisation failure was a problem with the sequence number SQN_{HE} in the HSS (which should be very rare), and the RAND and AUTS are not included in the authentication data request to the HSS, then an update of SQN_{HE} based on AUTS will not occur in the HSS, and the new authentication procedure between MME and UE using the new AV will fail again. This can be considered a security-relevant failure case as it may lead to a subscriber being shut out from the system permanently.

4.2.2.2.3 Integrity check of Attach message

Requirement Name: Integrity check of Attach message

Requirement Reference: TBA

Requirement Description: "If the user cannot be identified or the integrity check fails, then the MME shall send a response indicating that the user identity cannot be retrieved." as specified in TS 33.401, clause 6.1.4.

Threat References: TBA

Security Objective References: TBA

Test Case:

Purpose:

Verify that secure user identification by means of integrity check of Attach request works correctly.

Pre-Conditions:

Test environment with new and old MME. New MME may be simulated.

Execution Steps

The old MME receives an Identification Request message from the new MME with incorrect integrity protection.

Expected Results:

The old MME sends a response indicating that the user identity cannot be retrieved.

4.2.2.2.4 Not forwarding EPS authentication data to SGSN

Requirement Name: Not forwarding EPS authentication data to SGSN

Requirement Reference: TBA

Requirement Description: "EPS authentication data shall not be forwarded from an MME towards an SGSN." as specified in TS 33.401, clause 6.1.4.

Threat References: TBA

Security Objective References: TBA

Test Case:

Purpose:

Verify that EPS authentication data remains in the EPC.

Pre-Conditions:

Test environment with MME and SGSN. SGSN may be simulated.