3GPP TS 33.116 V19.0.0 (2025-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Specification(SCAS) for the MME network product class (Release 19)

Keywords
SCAS, MME, product class, security,LTE
Advanced

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.

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".

[9] 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].

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 GSM SIM forbidden

Requirement Name: GSM SIM access forbidden

Requirement Reference: TS 33.401[5], clause 6.1.1

Requirement Description: "Access to E-UTRAN with a GSM SIM or a SIM application on a UICC shall not be granted." as specified in TS 33.401 [5], clause 6.1.1.

Threat References: TR 33.926 [9], clause A.2.2.1 Access to GSM.

Test Case:

Purpose:

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

Pre-Conditions:

Test environment with HSS. HSS may be simulated.

Execution Steps

Include GSM authentication vector in *authentication data response* from HSS.

Expected Results:

MME rejects UE authentication when receiving GSM authentication vector from HSS.

NOTE: When both MME and HSS function correctly GSM 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: TS 33.401[5], clause 6.1.2

Requirement Description: "In the case of a synchronization failure, the MME shall also include RAND and AUTS." as specified in TS 33.401 [5], clause 6.1.2.

Threat References: TR 33.926 [9], clause A.2.2.2 Resynchronization.

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: TS 33.401[5], clause 6.1.4

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: TR 33.926 [9], clause A.2.2.3 Failed Integrity check of Attach message.

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: TS 33.401[5], clause 6.1.4

Requirement Description: "EPS authentication data shall not be forwarded from an MME towards an SGSN." as specified in TS 33.401[5], clause 6.1.4.

Threat References: TR 33.926 [9], clause A.2.2.4 Forwarding EPS authentication data to SGSN.

Test Case:

Purpose:

Verify that EPS authentication data remains in the EPC.

Pre-Conditions:

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

Execution Steps

The MME receives an Identification Request message from the SGSN.

Expected Results:

The response to the SGSN does not include EPS authentication data.

4.2.2.2.5 Not forwarding unused EPS authentication data between different security domains

Requirement Name: Not forwarding unused EPS authentication between different security domains

Requirement Reference: TS 33.401[5], clause 6.1.5

Requirement Description: "Unused EPS authentication vectors, or non-current EPS security contexts, shall not be distributed between MMEs belonging to different serving domains (PLMNs)." as specified in TS 33.401, clause 6.1.5.

Threat References: TR 33.926 [9], clause A.2.2.5 Forwarding unused EPS authentication data between different security domains.

Test Case:

Purpose:

Verify that unused EPS authentication data remains in the same serving domain.

Pre-Conditions:

Test environment with old and new MME in different serving domains. New MME may be simulated.

Execution Steps

The old MME receives an Identification Request message from the new MME.

Expected Results:

The response to the new MME does not include unused EPS authentication data.

4.2.2.3 Security mode command procedure

4.2.2.3.1 Bidding down prevention

Requirement Name: Bidding down prevention

Requirement Reference: TS 33.401[5], clause 7.2

Requirement Description: "The SECURITY MODE COMMAND shall include the replayed security capabilities of the UE." as specified in TS 33.401[5], clause 7.2.

Threat References: TR 33.926 [9], A.2.3.1 Bidding Down.

Security Objective References: TBA

Test Case:

Purpose:

Verify that bidding down by eliminating certain UE capabilities on the interface from UE to MME is not possible.

Pre-Conditions:

Test environment with UE. UE may be simulated.

Execution Steps

Attach request message includes security capabilities of the UE.

Expected Results:

MME includes the same security capabilities of the UE in the SECURITY MODE COMMAND message.

4.2.2.3.2 NAS integrity algorithm selection and use

Requirement Name: NAS integrity algorithm selection

Requirement Reference: TS 33.401[5], clause 7.2.4.3.1

Requirement Description: "The MME shall protect the SECURITY MODE COMMAND message with the integrity algorithm, which has the highest priority according to the ordered lists." as specified in TS 33.401 [5], clause 7.2.4.3.1."

NOTE: The text in TS 33.401 [5], clause 7.2.4.3.1 is somewhat incomplete. It should properly read: "…which has the highest priority according to the ordered lists and is contained in the UE EPS security capabilities."

Threat References: TR 33.926 [9], A.2.3.2 NAS integrity selection and use

Test Case:

Purpose:

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

Pre-Conditions:

Test environment with UE. UE may be simulated.

Execution Steps

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

Expected Results:

1. The MME 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 MME checks the message authentication code on the SECURITY MODE COMPLETE message.

2. The MAC in the SECURITY MODE COMPLETE is verified, and the NAS integrity protection algorithm is selected and applied correctly.

4.2.2.3.3 NAS NULL integrity protection

Requirement Name: NAS NULL integrity protection

Requirement Reference: TS 33.401[5], clause 5.1.4.1

Requirement Description: "EIA0 shall only be used for unauthenticated emergency calls." as specified in TS 33.401[5], clause 5.1.4.1."

Threat References: TR 33.926 [9], A.2.3.3 NAS NULL integrity protection

Test Case:

Purpose:

Verify that NAS NULL integrity protection algorithm is used correctly.

Pre-Conditions:

Test environment with UE. UE may be simulated.

Execution Steps

The MME sends the SECURITY MODE COMMAND message after successful UE authentication.

Expected Results:

The selected integrity algorithm is different from EIA0.

4.2.2.3.4 NAS confidentiality protection

Requirement Name: NAS confidentiality protection

Requirement Reference: TS 33.401[5], clause 7.2.4.3.1

Requirement Description: "The UE…sends the NAS security mode complete message to MME ciphered and integrity protected." as specified in TS 33.401[5], clause 7.2.4.3.1.

Threat References: TR 33.926 [9], A.2.3.4 NAS confidentiality protection

Test Case:

Purpose:

Verify that NAS confidentiality protection algorithm is applied correctly.

Pre-Conditions:

Test environment with UE. UE may be simulated.

Execution Steps

The MME receives the SECURITY MODE COMPLETE message without confidentiality protection.

Expected Results:

If a confidentiality algorithm different from EEA0 was selected the MME rejects the message.

4.2.2.4 Security in intra-RAT mobility

4.2.2.4.1 Bidding down prevention in X2-handovers

Requirement Name: Bidding down prevention in X2-handovers

Requirement Reference: TS 33.401[5], clause 7.2.4.2.2

Requirement Description: "The MME shall verify that the UE EPS security capabilities received from the eNB are the same as the UE EPS security capabilities that the MME has stored." as specified in TS 33.401[5], clause 7.2.4.2.2."

Threat References: TR 33.926 [9], A.2.4.1 Bidding down on X2-Handover

Test Case:

Purpose:

Verify that bidding down is prevented in X2-handovers.

Pre-Conditions:

Test environment with (target) eNB. eNB may be simulated.

The MME is configured to log the event of a UE EPS security capability mismatch.

Execution Steps

The MME receives the path-switch message with the UE EPS security capabilities different from the ones stored in the MME for that UE.

Expected Results:

The MME logs the event.

4.2.2.4.2 NAS integrity protection algorithm selection in MME change

Requirement Name: NAS integrity protection algorithm selection in MME change

Requirement Reference: TS 33.401[5], clause 7.2.4.3.2

Requirement Description: "In case there is change of MMEs and algorithms to be used for NAS, the target MME shall initiate a NAS security mode command procedure and include the chosen algorithms and the UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see clause 7.2.4.4). The MME shall select the NAS algorithms which have the highest priority according to the ordered lists (see clause 7.2.4.3.1)." as specified in TS 33.401[5], clause 7.2.4.3.2."

Threat References: TR 33.926 [9], A.2.4.2 NAS integrity protection algorithm selection in MME change

Test Case:

Purpose:

Verify that NAS integrity protection algorithm is selected correctly.

Pre-Conditions:

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

Execution Steps

The target MME receives the UE EPS security capabilities and the NAS algorithms used by the source MME from the source MME over the S10 interface. The target MME selects the NAS algorithms which have the highest priority

according to the ordered lists. The lists are assumed such that the algorithms selected by the target MME are different from the ones received from the source MME.

Expected Results:

The target MME initiates a NAS security mode command procedure and include the chosen algorithms and the UE security capabilities.

4.2.2.5 Security in inter-RAT mobility

4.2.2.5.1 No access with GSM SIM via idle mode mobility

Requirement Name: Idle mode mobility into E-UTRAN forbidden for GSM subscribers

Requirement Reference: TS 33.401[5], clause 9.1.2

Requirement Description: "In case the MM context in the Context Response/SGSN Context Response indicates GSM security mode, the MME shall abort the procedure." as specified in TS 33.401, clause 9.1.2.

Threat References: TR 33.926 [9], A.2.5.1 GSM SIM access via idle mode mobility

Test Case:

Purpose:

Verify that GSM subscribers cannot obtain service in EPS via idle mode mobility.

Pre-Conditions:

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

Execution Steps: The target MME receives the MM context in the Context Response indicating GSM security mode.

Expected Results: The MME aborts the procedure by acknowledging the Context Response from the SGSN with an appropriate failure cause.

4.2.2.5.2 No access with GSM SIM via handover

Requirement Name: Handover into E-UTRAN forbidden for GSM subscribers

Requirement Reference: TS 33.401[5], clause 9.2.2

Requirement Description: "In case the MM context in the Forward relocation request message indicates GSM security mode (i.e. it contains a Kc), the MME shall abort the non-emergency call procedure." as specified in TS 33.401, clause 9.2.2.

Threat References: TR 33.926 [9], A.2.5.3 GSM SIM access via SRVCC

Test Case:

Purpose:

Verify that GSM subscribers cannot obtain service in EPS via handovers.

Pre-Conditions:

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

Execution Steps: The target MME receives the MM context in the Forward Location Request message indicating GSM security mode.

Expected Results: The MME aborts the procedure by responding to the Forward Relocation Request from the SGSN with an appropriate failure cause.

4.2.2.5.3 No access with GSM SIM via SRVCC

Requirement Name: SRVCC into E-UTRAN forbidden for GSM subscribers

Requirement Reference: TS 33.401[5], clause 14.3.1

Requirement Description: "If the MME receives a GPRS Kc' from the source MSC server enhanced for SRVCC in the CS to PS HO request, the MME shall reject the request." as specified in TS 33.401, clause 14.3.1.

Threat References: TR 33.926 [9], A.2.6 Threats related to release of non-emergency bearer

Test Case:

Purpose:

Verify that GSM subscribers cannot obtain service in EPS via SRVCC into E-UTRAN.

Pre-Conditions:

Test environment with source MSC server and target MME. Source MSC server may be simulated.

Execution Steps

The target MME receives the GPRS Kc' and the $CKSN'_{PS}$ in the CS to PS handover request.

Expected Results:

The MME rejects the request.

4.2.2.6 Security Aspects of IMS Emergency Session Handling

4.2.2.6.1 Authentication failure for emergency bearers

NOTE: The use of NULL integrity is addressed in clause D.3.2.3.3.

Requirement Name: Emergency bearer establishment when authentication fails

Requirement Reference: TS 33.401 [5], clause 15.1.

Requirement Description: "The MME or UE shall always release any established non-emergency bearers, when the authentication fails in the UE or in the MME." as specified in TS 33.401, clause 15.1.

Threat References: TBA

Test Case:

Purpose:

Ensure that the MME enforces that only emergency bearers can be used without successful authentication.

Pre-Conditions:

Test environment with MME and UE. UE may be simulated. The serving network policy allows unauthenticated IMS Emergency Sessions.

Execution Steps

The UE sends the initial attach request for EPS emergency bearer services, then the MME initiates an authentication, which fails. The UE attached for EPS emergency bearer services sends the PDN Connectivity request for EPS non-emergency bearer services.

Expected Results:

The MME allows to continue the set up of the emergency bearer, and will reject the PDN Connectivity request for EPS non-emergency bearer services.

4.2.3 Technical Baseline

4.2.3.1 Introduction

This 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 MME-specific additions to clause 4.2.3.2.1 of TS 33.117.

4.2.3.2.2 Protecting data and information – unauthorized viewing

There are no MME-specific additions to clause 4.2.3.2.2 of TS 33.117.

4.2.3.2.3 Protecting data and information in storage

There are no MME-specific additions to clause 4.2.3.2.3 of TS 33.117.

4.2.3.2.4 Protecting data and information in transfer

There are no MME-specific additions to clause 4.2.3.2.4 of TS 33.117:

4.2.3.2.5 Logging access to personal data

There are no MME-specific additions to clause 4.2.3.2.5 of TS 33.117.

4.2.3.3 Protecting availability and integrity

There are no MME-specific additions to clause 4.2.3.3 of TS 33.117.

4.2.3.4 Authentication and authorization

There are no MME-specific additions to clause 4.2.3.4.

4.2.3.5 Protecting sessions

There are no MME-specific additions to clause 4.2.3.5 of TS 33.117.

4.2.3.6 Logging

All text from TS 33.117, clause 4.2.3.6 also applies to MMEs. There are no MME-specific adaptations or additions to this text.

4.2.4 Operating Systems

There are no MME-specific additions to clause 4.2.4 of TS 33.117.

4.2.5 Web Servers

There are no MME-specific additions to clause 4.2.5 of TS 33.117.

4.2.6 Network Devices

All text from TS 33.117, clause 4.2.6 also applies to MMEs. There are no MME-specific adaptations or additions to this text.

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

4.3.1 Introduction

4.3.2 Technical Baseline

All text from TS 33.117, clause 4.3.2 also applies to MMEs. There are no MME-specific adaptations or additions to this text.

4.3.3 Operating Systems

There are no MME-specific additions to clause 4.3.3 of TS 33.117.

4.3.4 Web Servers

There are no MME-specific additions to clause 4.3.4 of TS 33.117.

4.3.5 Network Devices

There are no MME-specific additions to clause 4.3.5 of TS 33.117.

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

All text from TS 33.117, clause 4.4 also applies to MMEs. There are no MME-specific adaptations or additions to this text.

Annex A (informative): Change history

Change history							
date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
09-2016	SA#73	SP-160572				Presented for approval	2.0.0
09-2016	SA#73					Upgrade to change control version	14.0.0
06-2017	SA#76	SP-170423	0001	-	F	Resolution of editor's notes in 33.116	14.1.0
2018-06	-	-	-	-	-	Update to Rel-15 version (MCC)	15.0.0
2020-07	-	-	-	-	-	Update to Rel-16 version (MCC)	16.0.0
2021-12	SA#94e	SP-211369	0004	1	A	Clarification on the emergency test - Rel16	16.1.0
2022-03	-	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0
2024-03	-	-	-	-	-	Update to Rel-18 version (MCC)	18.0.0
2025-03	SA#107	SP-250098	0005	-	F	Added missing references	19.0.0