



# Indian Telecom Security Assurance Requirements (ITSAR)

भारतीय दूरसंचार सुरक्षा आश्वासन आवश्यकताएँ (भा.दू.सु.आ.आ.)

---

## Mobility Management Entity (MME)

**ITSAR Number:** ITSAR102032311

**ITSAR Name:** NCCS/ITSAR/Core Equipment/Packet Core/Mobility Management Entity

---

Date of Release: 24.11.2023

Version: 1.0.1

Date of Enforcement:

जारीकर्ता  
राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)  
दूरसंचार विभाग, संचार मंत्रालय  
भारत सरकार  
सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत

Issued by  
National Centre for Communication Security (NCCS)  
Department of Telecommunications  
Ministry of Communications  
Government of India  
City Telephone Exchange, SR Nagar, Bangalore-560027, India

---

## About NCCS

National Centre for communication Security (NCCS), with headquarters at Bengaluru was set up in 2018 with the objective to establish and operationalize a framework of security testing and certification within the country. Security Assurance Standards (SAS) division of NCCS is mandated to prepare Telecom security requirements/standards called Indian Telecom Security Assurance Requirements (ITSAR) that addresses the country specific security needs in telecommunication landscape and notify the same.



## Document History

Sr No.	Title	ITSAR No.	Version	Date of Release	Remark
1.	Mobility Management Entity (MME)	ITSAR102032009	1.0.0	22.09.2020	First release
2.	Mobility Management Entity (MME)	ITSAR102032311	1.0.1	24.11.2023	Editorial Changes



## Table of Contents

Scope .....	6
Conventions.....	6
Section 1: Access and Authorization .....	6
1.1 Management Protocols Mutual Authentication.....	6
1.2 Management Traffic Protection.....	6
1.3 Role-Based access control.....	6
1.4 User Authentication – Local/Remote .....	7
1.5 Remote login restrictions for privileged users.....	7
1.6 Authorization Policy .....	8
1.7 Unambiguous identification of the user & group accounts removal.....	8
Section 2: Authentication Attribute Management .....	8
2.1 Authentication Policy.....	8
2.2 Authentication Support – External .....	8
2.3 Protection against brute force and dictionary attacks .....	9
2.4 Enforce Strong Password .....	9
2.5 Inactive Session Timeout .....	10
2.6 Password Changes .....	10
2.7 Protected Authentication feedback.....	11
2.8 Removal of predefined or default authentication attributes .....	11
Section 3: Software Security .....	11
3.1 Secure Update.....	11
3.2 Secure Upgrade.....	11
3.3 Source code security assurance .....	12
3.4 Known Malware and backdoor Check .....	12
3.5 No unused software.....	13
3.6 Unnecessary Services Removal.....	13
3.7 Restricting System Boot Source .....	13
3.8 Secure Time Synchronization.....	13
3.9 Restricted reachability of services .....	13
3.10 Avoidance of Unspecified Wireless Access.....	14
Section 4: System Secure Execution Environment.....	14
4.1 No unused functions .....	14
4.2 No unsupported components.....	14
Section 5: User Audit.....	14
5.1 Audit trail storage and protection .....	14
5.2 Audit Event Generation .....	15
5.3 Secure Log Export.....	17
Section 6: Data Protection .....	17
6.1 Cryptographic Based Secure Communication with connecting entities .....	18
6.2 Cryptographic Module Security Assurance.....	18
6.3 Cryptographic Algorithms implementation Security Assurance .....	18
6.4 Protecting data and information – Confidential System Internal Data .....	18
6.5 Protecting data and information in storage .....	18
6.6 Protection against Copy of Data .....	19
6.7 Protection against Data Exfiltration - Overt Channel .....	19

6.8 Protection against Data Exfiltration - Covert Channel.....	19
Section 7: Network Services.....	20
7.1 Traffic Separation.....	20
Section 8: Attack Prevention Mechanisms .....	20
8.1 Network Level and application level DDoS .....	20
8.2 Excessive Overload Protection.....	21
Section 9: Vulnerability Testing Requirements.....	21
9.1 Fuzzing – Network and Application Level .....	21
9.2 Port Scanning .....	21
9.3 Vulnerability Scanning .....	21
Section 10: Operating System .....	22
10.1 Growing Content Handling .....	22
10.2 Handling of ICMP .....	22
10.3 Authenticated Privilege Escalation only .....	23
10.4 System account identification .....	23
10.5 OS Hardening .....	24
10.6 No automatic launch of removable media .....	24
10.7 Protection from buffer overflows.....	24
10.8 External file system mount restrictions.....	24
10.9 File-system Authorization privileges.....	24
Section 11: Web Servers .....	25
11.1 HTTPS .....	25
11.2 Webserver logging .....	25
11.3 HTTPS input validation .....	25
11.4 No system privileges .....	26
11.5 No unused HTTPS methods.....	26
11.6 No unused add-ons .....	26
11.7 No compiler, interpreter, or shell via CGI or other server-side scripting .....	26
11.8 No CGI or other scripting for uploads .....	26
11.9 No execution of system commands with SSI .....	27
11.10 Access rights for web server configuration .....	27
11.11 No default content.....	27
11.12 No directory listings .....	27
11.13 Web server information in HTTPS headers.....	27
11.14 Web server information in error pages .....	27
11.15 Minimized file type mappings.....	28
11.16 Restricted file access.....	28
11.17 Execute rights exclusive for CGI/Scripting directory .....	28
Section 12: Other Security requirements.....	28
12.1. Remote Diagnostic Procedure – Verification.....	28
12.2 No Password Recovery.....	29
12.3 Secure System Software Revocation .....	29
12.4 Software Integrity Check – Installation.....	29
12.5 Software Integrity Check – Boot.....	29
12.6 Unused Physical and Logical Interfaces Disabling.....	30
12.7 No Default Profile.....	30
12.8 Security Algorithm Modification.....	30

12.9 Control Plane Traffic Protection .....	30
Section 13: Authentication and key agreement Procedure.....	31
13.1 Access with 2G SIM forbidden .....	31
13.2 Re-synchronization .....	31
13.3 Integrity check of Attach message.....	31
13.4 Not forwarding EPS authentication data to SGSN .....	31
13.5 Not forwarding unused EPS authentication data between different security domains .....	31
Section 14: Security mode command procedure.....	32
14.1 Bidding down prevention.....	32
14.2 NAS integrity algorithm selection and use.....	32
14.3 NAS NULL integrity protection .....	32
14.4 NAS confidentiality and integrity protection .....	32
Section 15: Security in intra-RAT mobility.....	33
15.1 Bidding down prevention in X2-handovers .....	33
15.2 NAS integrity protection algorithm selection in MME change .....	33
Section 16: Security in inter-RAT mobility .....	33
16.1 No access with 2G SIM via idle mode mobility .....	33
16.2 No access with 2G SIM via handover .....	33
16.3 No access with 2G SIM via SRVCC.....	34
Section 17: Security Aspects of IMS Emergency Session Handling.....	34
17.1 Release of non-emergency bearers .....	34
Section 18: Signalling Data Protection .....	34
18.1 Signalling data and User data confidentiality .....	34
18.2 Signalling data and User data integrity .....	35
Test Procedures/Test Schedules .....	35
Annexure-I .....	36
Annexure-II.....	38

*Securing Networks*

## Scope

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to the stand-alone MME (Mobility Management Entity), an LTE (Long-Term Evolution) network Core element with a dedicated hardware and dedicated software, which includes system software as well as application software.

## Conventions

1. Must or shall or required denotes the absolute requirement of a particular clause of ITSAR.
  2. Must not or shall not denote absolute prohibition of a particular clause of ITSAR.
  3. Should or Recommended denotes that the particular clause of ITSAR may be ignored under justifiable circumstances but after careful examination of its implications.
  4. Should not or not Recommended denotes the opposite meaning of (3) above.
- 

## Section 1: Access and Authorization

### 1.1 Management Protocols Mutual Authentication

#### Requirement:

The protocols used for the MME management and maintenance shall support mutual authentication mechanisms only i.e there is mutual authentication of entities for management interfaces on the MME.

Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 “shall only be used for MME management and maintenance.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.4.4.1

---

### 1.2 Management Traffic Protection

#### Requirement:

MME management traffic shall be protected strictly using Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0 “ only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.4

---

### 1.3 Role-Based access control

#### Requirement:

MME shall support Role Based Access Control (RBAC). A role-based access control

system uses a set of controls which determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform i.e. the specific operation command or command group.

MME supports Role Based Access Control (RBAC) conforming to the globally accepted RBAC standard INCITS 359-2012(R2017), with minimum of 3 user roles, in particular, for OAM privilege management, for MME Management and Maintenance, including authorization of the operation for configuration data and software via the MME console interface.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.6.2]

---

## **1.4 User Authentication – Local/Remote**

### **Requirement:**

The various user and machine accounts on a system shall be protected from misuse. To this end, an authentication attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user.

Authentication attributes include

- Cryptographic keys
- Token
- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker. Minimum two of the above Authentication attributes shall be mandatorily combined for protecting the admin and/or system accounts from misuse.

[Reference:TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.1]

---

## **1.5 Remote login restrictions for privileged users**

### **Requirement:**

Direct login to MME as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to MME remotely i.e remote login access for root/admin/highest privileged users, by default shall be disabled permanently at the time of first installation.

This remote root user access restriction is also applicable to application softwares / tools such as TeamViewer, desktop sharing which provide remote access to the



MME.

[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.6]

---

## **1.6 Authorization Policy**

### **Requirement:**

Only Role based authorization is permitted.

Bare minimum RBAC rights are to be assigned for the task to be performed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.3.4.6.1]

---

## **1.7 Unambiguous identification of the user & group accounts removal**

### **Requirement:**

Users shall be identified unambiguously by the MME .

MME shall support assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.

MME shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Sections 4.2.3.4.1.2]

---

## **Section 2: Authentication Attribute Management**

### **2.1 Authentication Policy**

#### **Requirement:**

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes i.e dual factor authentication shall be prevented.

This requirement shall also be applied to accounts that are only used for communication between systems.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.1.1]

---

### **2.2 Authentication Support – External**

#### **Requirement:**

If the MME supports external authentication mechanism such as AAA server ( for authentication, authorization and accounting services ) , then the communication between MME and the external authentication entity shall be protected using the authentication and related service protocols built strictly using the Secure

cryptographic controls prescribed in Table1 of the document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ only.

---

## **2.3 Protection against brute force and dictionary attacks**

### **Requirement:**

A protection against brute force and dictionary attacks that hinder AUTHENTICATION ATTRIBUTE guessing shall be implemented.

Brute force and dictionary attacks aim to use automated guessing to ascertain AUTHENTICATION ATTRIBUTE for user and machine accounts.

Various measures or a combination of the following measures can be taken to prevent this :

Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").

Blocking an account following a specified number of incorrect attempts,. However it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.

Using a AUTHENTICATION ATTRIBUTE blacklist to prevent vulnerable passwords.

In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by MME .

[Reference: TS/TSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.3]

---

## **2.4 Enforce Strong Password**

### **Requirement:**

(a) The configuration setting shall be such that a MME shall only accept passwords that comply with the following complexity criteria:

(i) Absolute minimum length of 8 characters (shorter lengths shall be rejected by the MME). It shall not be possible setting this absolute minimum length to a lower value by configuration.

(ii) Password shall mandatorily comprises all the following four categories of characters:

- at least 1 uppercase character (A-Z)
- at least 1 lowercase character (a-z)
- at least 1 digit (0-9)
- at least 1 special character (e.g. @;!\$.)

The minimum length of characters in the passwords and the set of allowable

special characters shall be configurable by the operator. The special characters may be categorized in sets according to their Unicode category.

If a central system is used for user authentication password policy , then additional assurance shall be provided that the central system enforces the same password complexity rules as laid down for the local system in this subclause.

If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the MME .

When a user is changing a password or entering a new password , MME/central system checks and ensures that it meets the password requirements.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3]

---

## **2.5 Inactive Session Timeout**

### **Requirement:**

An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period ranging from 2 to 5 minutes.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.5.2]

---

## **2.6 Password Changes**

### **Requirement:**

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized system for user authentication is used it is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

The system shall enforce password change based on passwordmanagement policy. In particular, the system shall enforce password expiry. MME shall support a configurable period for expiry of passwords. Previously used passwords shall not be allowed upto a certain number (Password History). The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3. This means that the MME shall store at least the three previously set passwords. The maximum number of passwords that the MME can store for each user is up to the manufacturer.

When a password is about to expire , a password expiry notification shall be provided to the user.

This requirement shall be met either by MME itself or in combination with external authentication system.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

---

## **2.7 Protected Authentication feedback**

### **Requirement:**

The Authentication attribute shall not be displayed in such a way that it could be seen and misused by a casual local observer. Typically, the individual characters of the password are replaced by a character such as "\*".

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.4 ]

---

## **2.8 Removal of predefined or default authentication attributes**

### **Requirement:**

Predefined or default authentication attributes shall be deleted or disabled.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.2.3]

---

## **Section 3: Software Security**

### **3.1 Secure Update**

#### **Requirement:**

MME's system software updates shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document " Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 " only.

MME shall allow updates only if code signing certificate is valid and not time expired.

Software update integrity shall be verified strictly using the Secure cryptographic controls prescribed in Table 1 of the document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

---

### **3.2 Secure Upgrade**

#### **Requirement:**

- (i) MME Software package integrity shall be validated in the installation and

upgrade stages strictly using the Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0” only.

(ii) MME shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the MME shall have a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software upgrade is originated from only these sources.

(iii) Tampered software shall not be executed or installed if integrity check fails.

(iv) MME’s software upgrades shall be carried out strictly using the Secure cryptographic controls prescribed in Table1 of the document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ only.

(v) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade, and modify the list mentioned in bullet (i) above.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5 ;

---

### **3.3 Source code security assurance**

#### **Requirement:**

- a) Vendor should follow best security practices including secure coding for software development and should be augmented with designated TSTL source code review duly supported by furnishing the Software Test Document ( STD) generated while developing the MME.
  - b) Also Vendor shall submit the undertaking as below :
    - (i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the MME Software, which includes vendor developed code, third party software and open source code libraries used/embedded in the MME.
    - (ii) The MME software is free from all known security vulnerabilities, security weaknesses listed in the CVE and CWE databases as on the date of testing and updates thereafter.
    - (iii) The binaries for MME and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.
- 

### **3.4 Known Malware and backdoor Check**

#### **Requirement:**

Vendor shall submit an undertaking stating that MME is free from all known

malware and backdoors as on the date of testing and shall submit Malware Test Document (MTD) of the MME to the designated TSTL.

---

### **3.5 No unused software**

#### **Requirement:**

Software components or parts of software which are not needed for operation or functionality of the MME shall not be present.

[Reference: TSDSI STD T1.3GPP 33.117 -14.2.0 V.1.0.0. Section 4.3.2.3]

---

### **3.6 Unnecessary Services Removal**

#### **Requirement:**

MME shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. By default all other ports and services will be permanently disabled.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.1]

---

### **3.7 Restricting System Boot Source**

#### **Requirement:**

MME shall boot only from memory devices intended for this purpose

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.2]

---

### **3.8 Secure Time Synchronization**

#### **Requirement:**

MME shall provide reliable time and date information provided manually by itself or through NTP/PTP server. MME shall establish secure communication channel with the NTP/PTP server.

MME shall generate audit logs for all changes to time settings.

---

### **3.9 Restricted reachability of services**

#### **Requirement:**

The MME shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose.

On interfaces where services are active, the reachability should be limited to legitimate communication peers.

[Reference: TSDSI STD T1.3GPP 33.117-1 4.2.0 V.1.0.0 Section 4.3.2.2]

---

### **3.10 Avoidance of Unspecified Wireless Access**

#### **Requirement:**

An undertaking shall be given by the vendor as follows:

"The MME does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.3.4.6.1]

---

## **Section 4: System Secure Execution Environment**

### **4.1 No unused functions**

#### **Requirement:**

Unused functions i.e the software and/or hardware functions which are not needed for operation or functionality of the MME shall not be present in the MME's software and/or hardware.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

---

### **4.2 No unsupported components**

#### **Requirement:**

Vendor to ensure that the MME shall not contain software and/or hardware components that are no longer supported by Vendor or its 3rd Parties including the open source communities , such as components that have reached end-of-life or end-of-support.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.2.5]

---

## **Section 5: User Audit**

### **5.1 Audit trail storage and protection**

#### **Requirement:**

The security event log shall be access controlled using file access rights such that only privilege users including the administrator have access to read the log files but not allowed to delete or modify the logfiles.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0. V.1.0.0 section 4.2.3.6.3]



---

## 5.2 Audit Event Generation

### Requirement:

The MME shall log all important Security events with unique System Reference details as given in the Table below.

MME shall record within each audit record atleast information pertaining to Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

EventTypes( Mandatory or optional )	Description	Event data to be logged
User Login including the Incorrect login attempts( Mandatory )	All use of Identification and authentication mechanism ; Records any user login actions including the incorrect login attempts to the MME	<ul style="list-style-type: none"><li>• Username,</li><li>• Source (IP address) if remote access</li><li>Outcome of event (Success or failure)</li><li>• Date &amp; Timestamp</li></ul>
Administrator access( Mandatory)	Records any access to accounts that have system privileges.	<ul style="list-style-type: none"><li>• Username,</li><li>• Date &amp; Timestamp,</li><li>Command given</li><li>• Duration of session,</li><li>Outcome of event (Success or failure)</li></ul>
		<ul style="list-style-type: none"><li>• Source (IP address) if remote access</li></ul>
Account administration( Mandatory)	Records all account administration activity, i.e. configure, delete, copy , enable, and disable along with the commands used for these activities	<ul style="list-style-type: none"><li>• Administrator username,</li><li>• Administered account,</li><li>• Activity performed (configure, delete, enable and disable)</li><li>Outcome of event (Success or failure)</li><li>• Date &amp; Timestamp</li></ul>
Resource Usage ( Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined	<ul style="list-style-type: none"><li>• Value exceeded,</li><li>• Value reached</li></ul> <p>(Here suitable threshold values shall be defined depending on the individual system.)</p>



	thresholds.	Outcome of event (Threshold Exceeded) • Date & Timestamp
Configuration change(Mandatory)	Changes to configuration of the network device	• Change made • Date & Timestamp Outcome of event (Success or failure) • Username
Reboot/shutdown/crash(Mandatory)	This event records any action on the network device that forces a reboot or shutdown OR where the network device has crashed.	• Action performed (boot, reboot, shutdown, etc.) • Username (for intentional actions) Outcome of event (Success or failure) • Timestamp
Interface status change(Mandatory)	Change to the status of interfaces on the network device (e.g. shutdown)	• Interface name and type • Status (shutdown, down, missing link, etc.) Outcome of event (Success or failure) • Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	• Administrator username, • Administered account, • Activity performed (group added or removed) Outcome of event (Success or failure) • Timestamp.
Resetting Passwords (Mandatory)	Resetting of user account passwords by the Administrator	• Administrator username, • Administered account, • Activity performed (configure, delete, enable and disable) Outcome of event (Success or failure) • Date & Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity Activity performed (start, stop, etc.) • Date & Timestamp

		Outcome of event (Success or failure)
X.509 Certificate Validation ( Optional)	Unsuccessful attempt to validate a certificate	Timestamp
		Reason for failure
		Subject identity
		Type of event
Secure Update ( Optional )	attempt to initiate manual update, initiation of update, completion of update	user identity
		Timestamp
		Outcome of event (Success or failure)
		Activity performed
Time change( optional )	Change in time settings	old value of time
		new value of time
		Timestamp
		origin of attempt to change time (e.g.IP address)
		Subject identity

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.6.1;  
2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.5]

### 5.3 Secure Log Export

#### Requirement:

(I) (a) The MME shall support forward of security event logging data to an external system by push or pull mechanism.

(a) Log functions should support secure uploading of log files to a central location or to a system external for the MME.

(II) MME shall be able to store generated audit data itself, may be with limitations.

(III) MME shall alert administrator when its security log buffer reaches configured threshold limit .

(IV) In the absence of External system, MME shall stop its services when its own security event log buffer is full .

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.3.6.2]

## Section 6: Data Protection

## **6.1 Cryptographic Based Secure Communication with connecting entities**

### **Requirements:**

MME shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ only.

---

## **6.2 Cryptographic Module Security Assurance**

Cryptographic module embedded inside the MME (in the form of hardware, software or firmware) that provides all the necessary security

services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

---

## **6.3 Cryptographic Algorithms implementation Security Assurance**

Cryptographic algorithms embedded in the crypto module of MME shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)

Vendor shall also submit cryptographic algorithm implementation testing document and the test results to designated TSTL for scrutiny.

---

## **6.4 Protecting data and information – Confidential System Internal Data Requirement:**

When MME is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear to users and administrators.

Access to maintenance mode shall be restricted only to authorised privileged user.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.2.2.]

---

## **6.5 Protecting data and information in storage**

### **Requirement:**

For data in storage (persistent or temporary) , read access rights shall be restricted. Files of MME system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the document

“Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ with appropriate non-repudiation controls.

In addition, the following rules apply for:

- (i) Systems that need access to identification and authentication data in the clear/readable form e.g. in order to perform an activity/operation, such systems shall not store this data in the clear/readable form, but scramble or encrypt it by implementation-specific means.
- (ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ .
- (iii) Stored files: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the document “Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “only.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3 ;

---

## **6.6 Protection against Copy of Data**

Requirement:

MME shall not create a copy of data in use and data in transit.

Protective measures shall exist against use of available system functions / software residing in MME to create copy of data for illegal transmission. The software functions, components in the MME for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

## **6.7 Protection against Data Exfiltration - Overt Channel**

Requirement:

MME shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit. Establishment of outbound overt channels shall not be allowed if they are initiated by / originated automatically from the MME.

---

## **6.8 Protection against Data Exfiltration - Covert Channel**

Requirement:

MME shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.

Establishment of outbound covert channels and tunnels shall not be allowed if they are initiated by / originated automatically from the MME i.e the MME shall not have a session or process established/initiated without a configured user or a system user.

Session logs shall be generated for establishment of any session initiated by either user or MME system.

---

## **Section 7: Network Services**

### **7.1 Traffic Separation**

#### **Requirement:**

MME shall support physical and/or logical separation of Operation & Maintenance traffic and control plane traffic. See RFC 3871 [3] for further information

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.5.1].

---

## **Section 8: Attack Prevention Mechanisms**

### **8.1 Network Level and application level DDoS**

#### **Requirement:**

MME shall have protection mechanism against known network level and Application level DDoS attacks.

MME shall provide security measures to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Potential protective measures include , but not limited , to the following:

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.3.3.1]

---

## 8.2 Excessive Overload Protection

### Requirement:

MME shall act in a predictable way if an overload situation cannot be prevented. MME shall be built in this way that it can react on an overload situation in a controlled way.

However it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that MME cannot reach an undefined and thus potentially insecure state.

In an extreme case , a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.2.3.3.3]

---

## Section 9: Vulnerability Testing Requirements

### 9.1 Fuzzing – Network and Application Level

#### Requirement:

It shall be ensured that externally reachable services of MME are reasonably robust when receiving unexpected input

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.4.4]

---

### 9.2 Port Scanning

#### Requirement:

It shall be ensured that on all network interfaces of MME , only documented ports on the transport layer respond to requests from outside the system.

Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters like Date & Time stamp, Source IP address, destination Port address etc.

The test for this requirement can be verified by using a suitable port scanning tool.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.4.2]

---

### 9.3 Vulnerability Scanning

#### Requirement:

It shall be ensured that there no known vulnerabilities exist in the MME.

The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans are in place to mitigate them) on the MME that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

The test for this requirement can be verified by using a suitable Vulnerability scanning tool.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

---

## Section 10: Operating System

### 10.1 Growing Content Handling

#### Requirements:

Growing or dynamic content on MME shall not influence system functions. A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop MME from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.1.1.1]

---

### 10.2 Handling of ICMP

#### Requirement:

Processing of ICMPv4 and ICMPv6 packets which are not required for MME operation shall be disabled on the MME.

MME shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table :

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	129	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet Too Big	Permitted	N/A

N/A	135	Neighbour Solicitation	Permitted	Permitted
N/A	136	Neighbour Advertisement	Permitted	N/A

MME shall not respond to, or process (i.e. do changes to configuration), under any circumstances certain ICMP message types as marked in below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e. do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp	N/A	Not Permitted	N/A
	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

[[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.2.4.2.2]

### 10.3 Authenticated Privilege Escalation only

#### Requirement:

MME shall not support a privilege escalation method in interactive sessions (both CLI and GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.2.1]

### 10.4 System account identification



**Requirement:**

Each system account in MME shall have a unique identification with appropriate non-repudiation controls.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.2.2]

---

**10.5 OS Hardening****Requirement:**

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in MME Kernel based network functions not needed for the operation of the MME shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.2]

---

**10.6 No automatic launch of removable media****Requirement:**

MME shall not automatically launch any application when removable media device is connected.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.3.1.3]

---

**10.7 Protection from buffer overflows****Requirement:**

MME shall support mechanisms for buffer overflow protection.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . Section 4.3.3.1.5]

---

**10.8 External file system mount restrictions****Requirement:**

If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in MME in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

---

**10.9 File-system Authorization privileges****Requirement:**

MME shall be designed to ensure that only users that are authorized to modify files,

data, directories or file systems have the necessary privileges to do so.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.7]

---

## Section 11: Web Servers

This entire section of the security requirements is applicable if the MME supports web management interface.

---

### 11.1 HTTPS

#### Requirement:

The communication between Web client and Web server shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ only.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.2.5.1]

---

### 11.2 Webserver logging

#### Requirement:

Access to the MME webserver ( for both successful as well as failed attempts) shall be logged by MME.

The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.2.5.2.1]

---

### 11.3 HTTPS input validation

#### Requirement:

The MME shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks.

MME shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.4]

---

#### **11.4 No system privileges**

##### **Requirement:**

No MME web server processes shall run with system privileges. [Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

---

#### **11.5 No unused HTTPS methods**

##### **Requirement:**

HTTPS methods that are not required for MME operation shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]

---

#### **11.6 No unused add-ons**

##### **Requirement:**

All optional add-ons and components of the web server shall be deactivated if they are not required for MME operation.

In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required. [Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.3.4.4]

---

#### **11.7 No compiler, interpreter, or shell via CGI or other server-side scripting**

##### **Requirement:**

If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.3.4.5]

---

#### **11.8 No CGI or other scripting for uploads**

##### **Requirement:**

If CGI or other scripting technology is used, the associated CGI/script directory shall not be used for uploads.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.6]

---

### **11.9 No execution of system commands with SSI**

**Requirement:**

If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.7]

---

### **11.10 Access rights for web server configuration**

**Requirement:**

Access rights for MME web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

---

### **11.11 No default content**

**Requirement:**

Default content that is provided with the standard installation of the MME web server shall be removed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]

---

### **11.12 No directory listings**

**Requirement:**

Directory listings (indexing) / "Directory browsing" shall be deactivated.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.10]

---

### **11.13 Web server information in HTTPS headers**

**Requirement:**

The HTTPS header shall not include information on the version of the MME web server and the modules/add-ons used.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.11]

---

### **11.14 Web server information in error pages**

**Requirement:**

User-defined error pages and Error messages shall not include version information and other internal information about the MME web server and the modules/add-ons used.

Default error pages of the MME web server shall be replaced by error pages defined by the vendor.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.12]

---

### **11.15 Minimized file type mappings**

#### **Requirement:**

File type or script-mappings that are not required for MME operation shall be deleted.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

---

### **11.16 Restricted file access**

#### **Requirement:**

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the MME web server's document directory.

In particular, the MME web server shall not be able to access files which are not meant to be delivered.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

---

### **11.17 Execute rights exclusive for CGI/Scripting directory**

#### **Requirement:**

If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

---

## **Section 12: Other Security requirements**

---

### **12.1. Remote Diagnostic Procedure – Verification**

#### **Requirement:**

If the MME is providing Remote access for troubleshooting purposes/alarm maintenance, then it shall be allowed only for authorized users , other than the root user.

All activities performed by the remote user are to be logged with the following

parameters:

- User id
- time stamp
- interface type
- Event level (e.g. CRITICAL, MAJOR, MINOR)
- Command/activity performed and
- Result type (e.g. SUCCESS, FAILURE).

[Reference TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2

---

## **12.2 No Password Recovery**

### **Requirement:**

---

In the event of MME system password reset with appropriate authentication and access control , the entire configuration of the MME shall be irretrievably deleted .  
No provision shall exists for MME system password recovery.

---

## **12.3 Secure System Software Revocation**

### **Requirement:**

Once the MME software image is legally updated/ upgraded with New Software Image , it shall not be possible to roll back to a previous software image.  
In case roll back is essential, it shall be done only by the administrator with appropriate non-repudiation controls.  
MME shall support a well-established control mechanism for rollingback to previous software image.

---

## **12.4 Software Integrity Check – Installation**

### **Requirement:**

MME shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ only  
Tampered software shall not be executed or installed if integrity check fails.

---

## **12.5 Software Integrity Check – Boot**

### **Requirement:**

The MME shall verify the integrity of a software component by comparing the result of a measurement of the component , typically a standard cryptographic hash generated strictly using the Secure cryptographic controls prescribed in Table1 of the

document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ to the expected reference value.

MME shall support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates.

---

## **12.6 Unused Physical and Logical Interfaces Disabling**

### **Requirement:**

MME shall support the mechanism to verify both the physical and logical interfaces exist in the product.

Physical and logical accessible Interfaces which are not under use shall be permanently disabled so that they remain inactive even in the event of a reboot.

---

## **12.7 No Default Profile**

Requirement: Predefined or default user accounts in MME shall be deleted or disabled.

---

## **12.8 Security Algorithm Modification**

### **Requirement:**

It shall not be possible to modify security algorithms supported by MME .

---

## **12.9 Control Plane Traffic Protection**

### **Requirement:**

Control plane traffic between the MME and the connected/connecting entities shall be protected in MME strictly using the secure cryptographic controls prescribed in Table1 of the document “ Cryptographic Controls For Indian Telecom Security Assurance Requirements ( ITSAR ) version 1.0.0 “ only.

Excluded are the entities within the mobile network domain that follow the mobile technology standards such as 2G Mobile network elements ( MS, BTS , BSC, MSC SMS-G ,VLR,HLR,EIR,AUC) , 3G Mobile network elements ( UE,NodeB, RNS,RNC,GMSC,SGSN,GGSN ,HLR,EIR,AUC) , 4G Mobile network elements ( ENodeB, SGWY, PGWY,MME,PCRF,HSS ) , 5G Mobile network elements ( UE,RAN,UPF,DN,AF,PCF,SMF,AMF,AUSF,UDM) connected to MME for call processing.

This exemption is applicable only for control plane and data plane communication for call processing.

---

## **Section 13: Authentication and key agreement Procedure**

### **13.1 Access with 2G SIM forbidden**

#### **Requirement:**

Access to E-UTRAN with a 2G SIM or a SIM application on a UICC shall not be granted by MME.

[Reference: 1) TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. Section 4.2.2.2.1;  
2) TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 6.1.1]

---

### **13.2 Re-synchronization**

#### **Requirement:**

In the case of a synchronization failure, the MME shall also include the stored RAND and the received AUTS in the authentication data request to the HSS.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0, section 4.2.2.2.2. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 6.1.2.]

---

### **13.3 Integrity check of Attach message**

#### **Requirement:**

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 and the event shall be logged with appropriate parameters.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. , section 4.2.2.2.3. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 6.1.4.]

---

### **13.4 Not forwarding EPS authentication data to SGSN**

#### **Requirement:**

EPS authentication data shall not be forwarded from the MME towards an SGSN.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. , section 4.2.2.2.4. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 6.1.4.]

---

### **13.5 Not forwarding unused EPS authentication data between different security domains**

#### **Requirement:**

Unused EPS authentication vectors, or non-current EPS security contexts, shall not be distributed between MMEs belonging to different serving domains (PLMNs).

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. , section 4.2.2.2.5. ;



2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 6.1.5.]

## **Section 14: Security mode command procedure**

---

### **14.1 Bidding down prevention**

#### **Requirement:**

MME shall include the replayed security capabilities of the UE in the SECURITY MODE COMMAND message.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0, section 4.2.2.3.1. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 7.2.]

---

### **14.2 NAS integrity algorithm selection and use**

#### **Requirement:**

The MME shall protect the SECURITY MODE COMMAND message with the integrity algorithm, which has the highest priority according to the ordered lists and is contained in the UE EPS security capabilities and is different from Null integrity algorithm.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0, section 4.2.2.3.2. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 7.2.4.3.1]

---

### **14.3 NAS NULL integrity protection**

#### **Requirement:**

Null integrity algorithm shall only be used for unauthenticated emergency calls.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0, section 4.2.2.3.3. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 5.1.4.1.]

---

### **14.4 NAS confidentiality and integrity protection**

#### **Requirement:**

NAS security mode command message shall be ciphered using the 128 bit SNOW 3G based / 128 bit AES based / 128 bit ZUC based ciphering algorithms and shall be integrity protected using the 128 bit SNOW 3G based / 128 bit AES based / 128 bit ZUC based integrity algorithms.

MME shall reject the message if the NAS security mode complete message received from UE is not ciphered and/or not integrity protected using the above stated algorithms.

Ciphering using Null Encryption algorithm and integrity protection using Null integrity algorithm shall be strictly forbidden.

Though the specified algorithms are with a 128-bit input key, support for larger bit input keys like 192 bit , 256 bit is preferable.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0 ,section 4.2.2.3.4. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 7.2.4.3.1.]

---

## Section 15: Security in intra-RAT mobility

---

### 15.1 Bidding down prevention in X2-handovers

#### Requirement:

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.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0 , section 4.2.2.4.1. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 7.2.4.2.2.]

---

### 15.2 NAS integrity protection algorithm selection in MME change

#### Requirement:

In case there is change of MMEs and the algorithms to be used for NAS, the target MME shall initiate a NAS security mode command procedure and include the chosen algorithms, the UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE.

MME shall select the NAS algorithms which have the highest priority according to the ordered lists and which are different from Null ciphering and Null Integrity algorithms

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0 ,section 4.2.2.4.2. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 7.2.4.3.2.]

---

## Section 16: Security in inter-RAT mobility

### 16.1 No access with 2G SIM via idle mode mobility

#### Requirement:

In case the MM context in the Context Response/SGSN Context Response indicates GSM security mode, the MME shall abort the procedure.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0 , section 4.2.2.5.1. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 9.1.2.]

---

### 16.2 No access with 2G SIM via handover

Requirement:

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

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. , section 4.2.2.5.2. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 9.2.2.]

---

### **16.3 No access with 2G SIM via SRVCC**

Requirement:

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.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. , section 4.2.2.5.3. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 14.3.1.]

---

## **Section 17: Security Aspects of IMS Emergency Session Handling**

---

### **17.1 Release of non-emergency bearers**

Requirement:

The MME shall always release any established non-emergency bearers, when the authentication fails in the UE and/or in the MME.

[Reference: 1. TSDSI STD T1.3GPP 33.116-14.1.0 V1.0.0. , section 4.2.2.6.1. ;  
2. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 15.1.]

---

## **Section 18: Signalling Data Protection**

---

### **18.1 Signalling data and User data confidentiality**

Requirement:

Confidentiality of NAS signalling data and user data ( sent via MME ) shall be protected using the 128 bit SNOW 3G based / 128 bit AES based / 128 bit ZUC based ciphering algorithms.

Though the specified algorithms are with a 128-bit input key, support for larger bit input keys like 192 bit , 256 bit is preferable.

Null ciphering algorithm shall be used only for unauthenticated emergency calls.

---

[Reference: 1. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 5.1.3.2.]

---

## **18.2 Signalling data and User data integrity**

### **Requirement:**

All user data packets sent via the MME shall be integrity protected using the 128 bit SNOW 3G based / 128 bit AES based / 128 bit ZUC based integrity algorithms .

Though the specified algorithms are with a 128-bit input key, support for larger bit input keys like 192 bit , 256 bit is preferable.

Null integrity algorithm shall be used only for unauthenticated emergency calls.

[Reference: 1. TSDSI STD T1.3GPP 33.401-14.5.0 V1.0.0, section 5.1.4.2.]

---


## **Test Procedures/Test Schedules**

In respect of the above MME Security Assurance test requirements where reference to 3GPP/TSDSI/NCCS sections/clauses is made, the test procedure/test schedule and execution steps given in the respective 3GPP/TSDSI/NCCS documents under the reference clauses/Sections shall be followed.

---

*Securing Networks*

## Acronyms



ACL	Access Control Lists
AAA Server	Authentication, Authorization, and Accounting Server
AES	Advanced Encryption Standard
AK	Anonymity Key
AKA	Authentication and Key Agreement
AMF	Authentication Management Field
AN	Access Network
AS	Access Stratum
ASME	Access Security Management Entity
AUTN	Authentication token
AV	Authentication Vector
CERT	Computer emergency response teams
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
DoS	Denial of Service
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EMS	Element management System
eNB	Evolved Node-B
EPC	Evolved Packet Core
EPS	Evolved Packet System
EPS-AV	EPS authentication vector
E-UTRAN	Evolved UTRAN
FIPS	Federal Information Processing Standards
GUTI	Globally Unique Temporary Identity
HE	Home Environment
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IK	Integrity Key
IKE	Internet Key Exchange
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IPSec VPN	Internet Protocol Security Virtual Private Network
KDF	Key Derivation Function
KSI	Key Set Identifier
MAC	Message Authentication Code
MC/DC	Modified Condition / Decision Coverage
MD5	Message Digest Algorithm
ME	Mobile Equipment

MISRA	Motor Industry Software Reliability Association
MME	Mobility Management Entity
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Station Identification Number
NAS	Non-Access Stratum
NCCS	National Centre for Communication Security
NE	Network Element
NIST	National Institute of Standards and Technology
NMS	Network management System
NTP	Network Time Protocol
OMC	Operation and maintenance Console
OS	Operating System
OSPF	Open Shortest Path First
PLMN	Public Land Mobile Network
PRNG	Pseudo Random Number Generator
PTP	Precision Time protocol
RADIUS	Remote Authentication Dial-In User Service
RAND	RANdOm number
RIP	Routing Information Protocol
SFTP	Secure File Transfer Protocol
SGSN	Serving GPRS Support Node
SHA	Secure hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SN	Serving Network
SN id	Serving Network identity
SNMP	Simple Network Management Protocol
SQN	Sequence Number
SRVCC	Single Radio Voice Call Continuity
SSH	Secure Shell
SSL	Secure Sockets Layer
S-TMSI	S-Temporary Mobile Subscriber Identity
TAI	Tracking Area Identity
TAU	Tracking Area Update
TFTP	Trivial File Transfer Protocol
TLS VPN	Transport Layer Security Virtual Private Network
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
UP	User Plane
URPF	Unicast Reverse Path Forwarding
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
XRES	Expected Response

### List of Undertakings to be Furnished by the Vendor For MME Security Testing

1. Source Code Security Assurance (against test case 3.3)
2. Known Malware and backdoor Check (against test case 3.4)
3. Avoidance of Unspecified Wireless Access (against test case 3.10)
4. Cryptographic Module Security Assurance (against test case 6.2)
5. Cryptographic Algorithms implementation Security Assurance (against test case 6.3)

