Indian Telecom Security Assurance Requirements

For 4G network element - Mobility Management Entity (MME)

DRAFT FOR APPROVAL

Release Date :

Version : 1.0.0

Security Assurance Standards Facility (SASF) , Bengaluru
Department of Telecom, Ministry Of Communications
Government of India

Table of Contents

Section 1: Access and Authorization

1.1 Management Protocols Mutual Authentication

Requirement:

The protocols used for the network product management shall support mutual authentication mechanisms.

There is mutual authentication of entities for management interfaces on the network product.

HTTPS with TLS 1.2 , SNMP V3 , SSHv2 Protocols are allowed

[Reference: 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:

Network Product shall use cryptographically protected network protocols for protecting the management traffic.
The transmission of data with a need of protection shall use industry accepted cryptographic algorithms such as AES , TDES , SHA and industry standard network protocols such as IPsec VPN with sufficient security measures. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used.

[Reference: 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:

The network product 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 domains could be Fault Management (FM), Performance Management (PM), System Admin, etc. 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 (e.g. View, Modify, Execute).

The network product supports RBAC with minimum of 3 user roles , in particular, for OAM privilege management for network product Management and Maintenance,

including authorization of the operation for configuration data and software via the network product 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 (e.g. phone numbers, public IP addresses or VPN membership) is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

NOTE: Several of the above options can be combined (dual-factor authentication) to achieve a higher level of security. Whether or not this is suitable and necessary depends on the protection needs of the individual system and its data and is evaluated for individual cases.

[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 as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the system remotely.

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

1.6 Authorization Policy

Requirement:

The authorizations for accounts and applications shall be reduced to the minimum required for the tasks they have to perform.

Authorizations to a system shall be restricted to a level in which a user can only access data and use functions that he needs in the course of his work. Suitable authorizations shall also be assigned for access to files that are components of the operating system or of applications or that are generated by the same (e.g. configuration and logging files).

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.
[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 Network Product .
Network Product shall support assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.
Network Product shall not enable the use of group accounts or group credentials, or sharing of the same account between several users, by default.

[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 one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems. An exception to the authentication and authorization requirement are functions for public use such as those for a Web server on the Internet, via which information is made available to the public.

[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 Network product supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services) , then the communication between Network product and the external authentication entity shall be only through secured(encrypted) communication channels such as Tacacs , Diameter.

2.3 Protection against brute force and dictionary attacks

Requirement:

If a password is used as an authentication attribute, a protection against brute force and dictionary attacks that hinder password guessing shall be implemented.
Brute force and dictionary attacks aim to use automated guessing to ascertain passwords for user and machine accounts. Various measures or a combination of these measures can be taken to prevent this.

The most commonly used protection measures are:
(i) 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").

(ii)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.

(iii)Using CAPTCHA to prevent automated attempts (often used for Web applications).

(iv) Using a password blacklist to prevent vulnerable passwords.

In order to achieve higher security, vendor shall combine two or more of the measures indicated above .
Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.
NOTE 1: Password management and blacklist configuration may be done in a separate node that is different to the node under test, e.g. a SSO server or any other central credential manager.

[Reference: TSDSI 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 setting by the vendor shall be such that a network product 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 network product). 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 is performed on the central system and 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 Network Product.

When a user is changing a password or entering a new password the system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).

[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:

(a) 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.

[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 password management policy. In particular, the system shall enforce password expiry.
Previously used passwords shall not be allowed up to a certain number (Password History).
The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its default value shall be 3. This means that the NE shall store at least the three previously set passwords. The maximum number of passwords that the network product 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. Above requirements shall be applicable for all passwords used(e.g. application-level, OS-level, etc.). An exception to this requirement is machine accounts.
This requirement shall be met either by Network product 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 "*".

Above requirements shall be applicable for all authentication attributes used(e.g. application-level,OS-level, etc.). An exception to this requirement is machine accounts.

[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.

Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, vendor or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on first^{t} time login to the system or the vendor provides instructions on how to manually change it.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 5.2.3.4.2.3]

Section 3: Software Security

3.1 Secure Update

Requirement:

Network product's system software updates shall be carriedout via cryptographic means i.e using the signed digital certificates. Network product shall allow updates only if code signing certificate is valid and not time expired.
Software update integrity shall be verified via cryptographic means such as hashing mechanism (like SHA2).

3.2 Secure Upgrade

Requirement:

(i) Software package integrity shall be validated in the installation/upgrade stage.

(ii) Network product shall support software package integrity validation via cryptographic means, e.g. digital signature. To this end, the network product has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.

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

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

[Reference: 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:

Vendor shall scan the entire source code under the supervision of designated test lab to ensure the following :

(i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the NE Software, which includes vendor developed code, third party software and open source code libraries used/embedded in the Network Product.

(ii)The Network Product software is free from known security vulnerabilities, security weaknesses listed in the CWE database and the security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10.

(iii) The binary file for Network Product application is generated from the source code that is free from all the stated coding security vulnerabilities stated in bullet (ii) above.

Vendor shall also submit Software Test Document (STD) generated while developing Network product's OS /Application Software for scrutiny by the lab

3.4 Known Malware Check

Requirement:

Vendor shall submit Software Test Document (STD) of the network product proving that the network product is free from known malware/spyware to lab for scrutiny

3.5 No unused software

Requirement:

Unused software components or parts of software which are not needed for operation or functionality of the NE shall not be installed or shall be deleted after installation. This includes also parts of a software, which will be installed as examples but typically not be used (e.g. default web pages, example databases, test data).

Note : Vendor shall provide the list of software that are necessary for its operation.

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

3.6 Unnecessary Service Removal

Requirement:

The Network Product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on the Network Product by the vendor.

- FTP
- TFTP
- Telnet
- rlogin, RCP, RSH
- HTTP
- SNMPv1 and v2
- SSHv1
- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)
- Finger
- BOOTP server
- Discovery protocols (CDP, LLDP)
- IP Identification Service (Identd)
- PAD
- MOP

NOTE 1:As an alternative to disabling the HTTP service, it is also possible for this service to remain active for reasons of user friendliness. In this case, however, queries to the web service may not be answered directly on this port but from a redirected to HTTPS service.

NOTE 2: Full documentation of required protocols and services of the Network Product and their purpose needs to be provided by the vendor as prerequisite for the test case.

[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:

The network product can only boot from memory devices intended for this purpose (e.g. not from external memory like USB key).

[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:
Network Product shall provide reliable time and date information provided manually by itself or through NTP server. Network product should generates audit logs for all changes to time settings. Network product should support to configure authentication between itself and external NTP server

3.9 Self Testing

Requirement:

Network product shall perform self-tests to identify failures in its security Mechanisms during i)power on ii) when Administrator Instructs. (eg., integrity of the firmware and software as well as for the correct operation of cryptographic functions, etc.,)

3.10 Restricted reachability of services

Requirement:

The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces were services are active, the reachability should be limited to legitimate communication peers. This limitation shall be realized on the network product itself

EXAMPLE: Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management network to support separation of management traffic from user traffic.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.2.2]

3.11 Avoidance of Unspecified Wireless Access

Requirement:

An undertaking shall be given as follows: "The Network product does not contain any wireless, optical, magnetic or any other component that may be used as a covert channel"

Note: Network product supporting standard wireless technologies would also need to be tested for this requirement apart from wireless technology related tests.

Section 4: System Secure Execution Environment

4.1 No unused functions

Requirement:

Unused functions of the Network Product's software and hardware shall be deactivated.

During installation of software and hardware often functions will be activated that are not required for operation or function of the system. If unused functions of software cannot be deleted or de-installed individually as given under requirement " 3.5 No unused software" of this document, such functions shall be deactivated in the configuration of the network product permanently.

Also hardware functions which are not required for operation or function of the system (e.g. unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after the Network Product reboot.

Example: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the Network Product.

Note: List of the used functions of the Network Product software and hardware as given by the vendor shall match the list of used software and hardware functions that are necessary for the operation of the Network product.

[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:

Network product shall not contain software and hardware components that are no longer supported by their vendor, producer or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime.

[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:
(a)The security event log shall be access controlled (file access rights), so only privilege users have access to read the log files but not allowed to delete the log files.
This requirement is also applicable to Administrator.

[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 Network product shall log all important Security events with unique System Reference such as IP Address, MAC address, hostname, etc. It shall be possible to log the events as given in the Table below. The Network product shall record within each audit record at least 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
Incorrect login attempts(Mandatory)	Records any user incorrect login attempts to the DUT	• Username,
		• Source (IP address) if remote access
		Outcome of event (Success or failure)
		• Timestamp
Administrator access(Mandatory)	Records any access attempts to accounts that have system	• Username,
		• Timestamp,

	privileges.	• Length of session, Outcome of event (Success or failure) • Source (IP address) if remote access
Account administration(Mandatory)	Records all account administration activity, i.e. configure, delete, enable, and disable.	• Administrator username, • Administered account, • Activity performed (configure, delete, enable and disable) Outcome of event (Success or failure) • Timestamp
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 thresholds.	• Value exceeded, • Value reached (Here suitable threshold values shall be defined depending on the individual system.) Outcome of event (Success or failure) • Timestamp
Configuration change(Mandatory)	Changes to configuration of the network device	• Change made * 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 (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, 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 (Optional)	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)
		• Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity
		Activity performed (start, stop, etc.)
		Timestamp
		Outcome of event (Success or failure)
User login (Mandatory)	All use of identification and authentication mechanism	user identity
		origin of attempt (e.g.IP address)
		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
		outcome of event (Success or failure)
		user identity
Session unlocking/ termination (Optional)	Any attempts at unlocking of an interactive session, Termination of a remote session by the session locking mechanism, Termination of an	user identity (wherever applicable)
		Timestamp
		Outcome of event (Success or failure)
		Subject identity

	interactive session	Activity performed
		Type of event
Trusted Communication paths(with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators) (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
		Initiator identity (as applicable)
		Target identity (as applicable)
		User identity (in case of Remote administrator access)
		Type of event
		Outcome of event (Success or failure, as applicable)
Audit data changes(Optional)	Changes to audit data including deletion of audit data	Timestamp
		Type of event (audit data deletion, audit data modification)
		Outcome of event (Success or failure, as applicable)
		Subject identity
		user identity
		origin of attempt to change time (e.g.IP address)
		Details of data deleted or modified

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.Section 4.2.3.6.1]

5.3 Secure Log Export

Requirement:

(I) (a) The Network Product shall support forward of security event logging data to an external system.

(b) Log functions should support secure uploading of log files to a central location or to a system external for the Network Product that is logging

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

Network product shall be able to store generated audit data itself may be with limitations.

In the absence of External system, Network product shall support facility to drop new audit data or overwrite old audit data based on defined criteria in case of its own log buffer full.

Network product shall alert administrator when its log buffer reaches configured threshold limit .

Section 6: Data Protection

6.1 Cryptographic Based Secure Communication

Requirements:

Requirements:

Secure communication mechanism between the Network product and the connected entities shall use only the industry standard and NIST recommended cryptographic protocols such as IPSEC, VPN, SSH, TLS/SSL, etc.Also Network product shall provide all cryptographic service such as encryption , decryption, key exchange , authentication , data integrity etc using the industry accepted and NIST recommended cryptographic algorithms (with standard key lengths) such as SHA, Diffie-Hellman, AES , RSA etc.

6.2 Cryptographic Module Security Assurance

An undertaking shall be provided for the following:
Vendor shall ensure that the Cryptographic module embedded inside the Network product (which may be in the form of hardware, software or firmware) which provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 standards for different levels of security.
Vendor shall submit crypto module Security Policy document and other related documents to lab for scrutiny

6.3. Cryptographic Algorithms implementation Security Assurance

An undertaking shall be provided by the vendor as below:

Cryptographic algorithms embedded in the crypto module of Network product are implemented in compliance with respective FIPS standards (for the specific crypto algorithm)

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

6.4. Protecting data and information – Confidential System Internal Data

Requirement :

When Network product 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. Such system functions could be, for example, local or remote OAM CLI or GUI, error messages, logging messages, alarms, configuration file exports etc. Confidential system internal data contains authentication data (i.e. PINs, cryptographic keys, passwords, cookies) as well as system internal data that is not required for systems administration and could be of advantage to attackers (i.e. stack traces in error messages).

Access to maintenance mode should 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 sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of a system that are needed for the functionality shall be protected against manipulation.

In addition, the following rules apply for:

(i)Systems that need access to identification and authentication data in the clear, e.g. in order to perform an authentication. Such systems shall not store this data in the clear, but scramble or encrypt it by implementation-specific means.

(ii)Systems that do not need access to sensitive data (e.g. user passwords) in the clear. Such systems shall hash this sensitive data .

(iii)Stored files: examples for protection against manipulation are the use of checksum or cryptographic methods.

[Reference: 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 :

Network product shall have protection against creating a copy of data in use / data in transit. Protective measure should exists against use of available system functions / software residing in Network product to create copy of data for illegal transmission. The software functions, components in the Network product 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 :

Network product shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as FTP, HTTP, HTTPS IM, P2P, Email etc are to be forbidden if they are initiated by / originate from the Network product. Outbound-use of such services are to be disabled in the Network product, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

6.8 Protection against Data Exfiltration - Covert Channel

Requirement :

Network product shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are initiated by / originate from the Network Product. Outbound-use of such services are to be disabled in the Network product, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Section 7: Network Services

7.1 Traffic Filtering – Network Level

Requirement:

The Network product shall provide a mechanism to filter incoming IP packets on any IP interface

In particular the Network product shall provide a mechanism:

(i) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.
(ii) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
 Discard/Drop: the matching message is discarded, no subsequent rules are applied and no answer is sent back.
 Accept: the matching message is accepted.
 Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.
(iii) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.
(iv) To filter on the basis of the value(s) of any portion of the protocol header.
(v) To reset the accounting.
(vi) The Network product shall provide a mechanism to disable/enable each defined rule.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.6.2.1]

[Reference: RFC 3871]

7.2 Traffic Separation

Requirement:

The Network product shall support physical or logical separation of O&M 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].

7.3 Traffic Protection –Anti-Spoofing

Requirement:

Systems shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.3.1.1]

Section 8: Attack Prevention Mechanisms

8.1 Network Level and application level DDoS

Requirement:

The system 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:

- 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

Note : Network product should have protection mechanism against known network level and Application DDoS attacks.

[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:

The system shall act in a predictable way if an overload situation cannot be prevented. A system 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 the system cannot reach an undefined and thus potentially insecure state. In an extreme case this means that a controlled system shutdown is preferable to uncontrolled failure of the security functions and thus loss of system protection.

The vendor shall provide a technical description of the network products' Over Load Control mechanisms (especially whether these mechanisms rely on cooperation of other network elements) and the accompanying test case for this requirement will check that

the description provides sufficient detail in order for an evaluator to understand how the mechanism is designed.

[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 are reasonably robust when receiving unexpected input

Note: Vendor is expected to provide the list of protocols supported by the Network product .
[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, only documented ports on the transport layer respond to requests from outside the system.

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

Vulnerability scanning tools may also report false positives and they shall be investigated and documented in the test report.

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 (e.g. log files, uploads) shall not influence system functions. A file system that reaches its maximum capacity shall not stop a system from operating properly. Therefore, countermeasures shall be taken such as usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring 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 operation shall be disabled on the Network Product. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk.

ICMP message types which on receipt lead to responses or to configuration changes are not mentioned in this requirement, but they may be necessary to support relevant and specified networking features. Those must be documented.

Certain ICMP types are generally permitted and do not need to be specifically documented.

The Network Product shall not send certain ICMP types by default, but it may support the option to enable utilization of these types (e.g. for debugging). This is marked as "Optional" in below table

Type (IPv4)	Type (IPv6)	Description	Send	Respond to

0	128	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	129	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

The Network Product 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
14	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 4.2.4.1.1.2.]

10.3 Authenticated Privilege Escalation only

Requirement:

There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a user to gain administrator/root privileges from another user account without re-authentication. Implementation example: Disable insecure privilege escalation methods so that users are required to (re-)login directly into the account with the required permissions.

[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 Operating system of the Network product shall have a unique identification, the Vendor to provide information on implementation mechanism for this requirement.

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

10.5 OS Hardening - Kernel Security

Requirement:

Vendor shall submit the process for OS Hardening undertaken to justify that the OS is sufficiently hardened and Kernel based applications / functions not needed for the operation of the Network product are deactivated

Vendor shall provide information on steps taken in this regard.

[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:

The NE shall not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.

[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:

The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided.

[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 order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.3.1.6]

10.9 File-system Authorization privileges

Requirement:

The system 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.

Section 11: Web Servers

The following security requirements are applicable for NEs supporting web server functionality.

11.1 HTTPS

Requirement:

The communication between Web client and Web server shall be protected using industry standard secured communication protocols such as TLS/HTTPS.

Cipher suites with NULL encryption shall not be supported.

[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 webserver (both successful as well as failed attempts) shall be logged. 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 HTTP User sessions

Requirement:

To protect user sessions the Network Product shall support the following session ID and session cookie requirements:

(i). The session ID shall uniquely identify the user and distinguish the session from all other active sessions.

(ii). The session ID shall be unpredictable.

(iii). The session ID shall not contain sensitive information in clear text (e.g. account number, social security, etc.).

(iv). In addition to the Session Idle Timeout (see clause 2.5 Inactive session timeout), the Network Product shall terminate automatically sessions after a configurable maximum lifetime This maximum lifetime defines the maximum session span. When the maximum lifetime expires, the session shall be closed, the session ID shall be deleted and the user

shall be forced to (re)authenticate in the web application and to establish a new session. The default value for this maximum lifetime shall be set to 8 hours.

(v). Session ID's shall be regenerated for each new session (e.g. each time a user logs in).

(vi). The session ID shall not be reused or renewed in subsequent sessions.

(vii). The Network Product shall not use persistent cookies to manage sessions but only session cookies. This means that neither the "expire" nor the "max-age" attribute shall be set in the cookies.

(viii). Where session cookies are used the attribute 'HttpOnly' shall be set to true.

(ix). Where session cookies are used the 'domain' attribute shall be set to ensure that the cookie can only be sent to the specified domain.

(x). Where session cookies are used the 'path' attribute shall be set to ensure that the cookie can only be sent to the specified directory or sub-directory.

(xi). The Network Product shall not accept session identifiers from GET/POST variables.

(xii). The Network Product shall be configured to only accept server generate session ID's.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.5.3]

11.4 HTTP input validation

Requirement:

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

11.5 No system privileges

Requirement:

No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by

a user with system privileges, execution shall be transferred to a different user without system privileges after the start.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

11.6 No unused HTTP methods

Requirement:

HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.3]

11.7 No unused add-ons

Requirement:

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

11.8 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 (e.g. PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.section 4.3.4.5]

11.9 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]

11.10 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]

11.11 Access rights for web server configuration

Requirement:

Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.8]

11.12 No default content

Requirement:

Default content (examples, help files, documentation, aliases) that is provided with the standard installation of the web server shall be removed.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.9]

11.13 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]

11.14 Web server information in HTTP headers

Requirement:

The HTTP header shall not include information on the version of the 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]

11.15 Web server information in error pages

Requirement:

User-defined error pages shall not include version information about the web server and the modules/add-ons used. Error messages shall not include internal information such as internal server names, error codes, etc. Default error pages of the 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]

11.16 Minimized file type mappings

Requirement:

File type- or script-mappings that are not required shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.13]

11.17 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g. via links or in virtual directories) in the web server's document directory. In particular, the 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]

11.18 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 Network product is providing Remote access for troubleshooting purposes/alarm maintenance, then it should be allowed only for authorized users and all activities performed by the remote user is to be logged with parameters like User id , time stamp, interface type, event level (e.g. CRITICAL, MAJOR, MINOR), result type (e.g. SUCCESS, FAILURE).

12.2 No Password Recovery

Requirement:

Network devices have a function that resets the current system password .In the event of system password reset , the entire configuration of the Network product shall be irretrievably deleted .

No provision shall exists for password recovery

12.3 Secure System Software Revocation

Requirement:

Once the software image is legally updated, it should not be possible to roll back to a previous exploitable software image. In case roll back is essential, it shall be done only by the administrator. NE shall support a well-established control mechanism for rolling back to previous exploitable software image.

12.4 Software Integrity Check – Installation

Requirement:

Network product should validate the software package integrity before the installation/upgrade stage. Tampered software shall not be executed or installed if integrity check fails.

12.5 Software Integrity Check – Boot

Requirement:

The Network Product shall verify the integrity of a software component typically by comparing the result of a measurement (typically a cryptographic hash) of the component to the expected reference value.

The Network Product 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:

The network product shall support the mechanism to verify both the physical and logical interfaces exist in the product. Both 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.

Note : List of the default used Physical and logical Interfaces/Ports as given by the vendor shall match the list of Physical and logical Interfaces/Ports that are necessary for the operation of the Network Product.

12.7 No Default Profile

Requirement:

Predefined or default user accounts shall be deleted or disabled. Default accounts such as guest, master are generally pre-configured with known or nil authentication attribute and therefore such standard users shall be deleted or disabled.

12.8 Security Algorithm Modification

Requirement:

It shall not be possible from unauthorized access, to modify security algorithms supported by the target network product, e.g. to perform a downgrade attack by configuring the use of a weaker algorithm.

12.9 Control Plane Traffic Protection

Requirement:

Control plane traffic shall be protected in the NE using standard cryptographic mechanisms i.e by using the industry standard cryptographic secure protocols such as TLS, IPSec, etc. Control plane traffic shall be protected in the NE using standard cryptographic mechanisms i.e by using the industry standard cryptographic secure protocols such as TLS, IPSec, etc

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

[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

[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:

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.

[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:

The SECURITY MODE COMMAND shall include the replayed security capabilities of the UE

[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.

[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:

EIA0 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 protection

Requirement:

The UE…sends the NAS security mode complete message to MME ciphered and integrity protected.

[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 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. The MME shall select the NAS algorithms which have the highest priority according to the ordered lists.

[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 or UE shall always release any established non-emergency bearers, when the authentication fails in the UE 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 industry standard ciphering algorithms such as EEA0 (Null ciphering algorithm) ,128-EEA1 (SNOW 3G) , 128-EEA2 (AES) and 128-EEA3 (ZUC). Though the specified algorithms are with a 128-bit input key, support for larger bit input keys like 192 bit , 256 bit is preferable.

EEA0 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 industry standard integrity algorithms such as 128-EIA0 (Null integrity algorithm) ,128-EIA1 (SNOW 3G) and 128-EIA2 (AES) and 128-EEA3 (ZUC). Though the specified algorithms are with a 128-bit input key, support for larger bit input keys like 192 bit , 256 bit is preferable.

EIA0 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.]

ABBREVIATIONS

AAA Server	Authentication, Authorization, and Accounting Server
ACL	Access Control Lists
AES	Advanced Encryption Standard
CERT	Computer emergency response teams
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDOS	Distributed Denial of Service
NE	Network Element
EMS	Element management System
FIPS	Federal Information Processing Standards
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPSec VPN	Internet Protocol Security Virtual Private Network
MC/DC	Modified Condition / Decision Coverage
MD5	Message Digest Algorithm
MISRA	Motor Industry Software Reliability Association
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

PTP	Precision Time protocol
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure hash Algorithm
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS VPN	Transport Layer Security Virtual Private Network
URPF	Unicast Reverse Path Forwarding
ST	Security Traget
TOE	Target Of Evaluation
TSF	TOE Security Functionality

AES Advanced Encryption Standard
AK Anonymity Key
AKA Authentication and Key Agreement
AMF Authentication Management Field
AN Access Network
AS Access Stratum
AUTN Authentication token
AV Authentication Vector
ASME Access Security Management Entity
Cell-ID Cell Identity as used in TS 36.331 [21]
CK Cipher Key
CKSN Cipher Key Sequence Number
C-RNTI Cell RNTI as used in TS 36.331 [21]
CRL Certificate Revocation List
DeNB Donor eNB
DoS Denial of Service
DSCP Differentiated Services Code Point
EARFCN-DL E-UTRA Absolute Radio Frequency Channel Number-Down Link
ECM EPS Connection Management
EDT Early Data Transmission
EEA EPS Encryption Algorithm
EIA EPS Integrity Algorithm
eKSI Key Set Identifier in E-UTRAN
EMM EPS Mobility Management
eNB Evolved Node-B
EPC Evolved Packet Core
EPS Evolved Packet System
EPS-AV EPS authentication vector
E-UTRAN Evolved UTRAN
gNB Next Generation Node-B

GERAN GSM EDGE Radio Access Network
GUTI Globally Unique Temporary Identity
HE Home Environment
HFN Hyper Frame Number
HO Hand Over
HSS Home Subscriber Server
IK Integrity Key
IKE Internet Key Exchange
IMEI International Mobile Station Equipment Identity
IMEISV International Mobile Station Equipment Identity and Software Version number
IMSI International Mobile Subscriber Identity
IOPS Isolated E-UTRAN Operation for Public Safety
IRAT Inter-Radio Access Technology
ISR Idle Mode Signaling Reduction
KDF Key Derivation Function
KSI Key Set Identifier
LWIP LTE WLAN RAN Level Integration using IPSec
LSB Least Significant Bit
LSM Limited Service Mode
LWA LTE-WLAN Aggregation
MAC-I Message Authentication Code for Integrity (terminology of TS36.323 [12])
MACT Message Authentication Code T used in AES CMAC calculation
MeNB Master eNB
ME Mobile Equipment
MME Mobility Management Entity
MME-RN MME serving the RN
MS Mobile Station
MSC Mobile Switching Center
MSIN Mobile Station Identification Number
NAS Non Access Stratum
NAS-MAC Message Authentication Code for NAS for Integrity (called MAC in TS24.301 [9])
NASDVM Non Access Stratum - Data via MME
NCC Next hop Chaining Counter
NH Next Hop
OCSP Online Certificate Status Protocol
OTA Over-The-Air (update of UICCs)
PCI Physical Cell Identity as used in TS 36.331 [21]
PDCP Packet Data Convergence Protocol
PLMN Public Land Mobile Network
PRNG Pseudo Random Number Generator
PSK Pre-shared Key
P-TMSI Packet- Temporary Mobile Subscriber Identity
RAND RANDom number

RAU Routing Area Update
RN Relay Node
RRC Radio Resource Control
SCG Secondary Cell Group
SEG Security Gateway
SGSN Serving GPRS Support Node
SIM Subscriber Identity Module
SMC Security Mode Command
SeNB Secondary eNB
SgNB Secondary gNB
SN Serving Network
SN id Serving Network identity
SQN Sequence Number
SRB Source Route Bridge
SRVCC Single Radio Voice Call Continuity
S-TMSI S-Temporary Mobile Subscriber Identity
TAI Tracking Area Identity
TAU Tracking Area Update
UE User Equipment
UEA UMTS Encryption Algorithm
UIA UMTS Integrity Algorithm
UICC Universal Integrated Circuit Card
UMTS Universal Mobile Telecommunication System
UP User Plane
USIM Universal Subscriber Identity Module
UTRAN Universal Terrestrial Radio Access Network
WT WLAN Termination as used in TS 36.300 [30]
XRES Expected Response