Indian Telecom Security Assurance Requirements (ITSAR)

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

# Group-III Devices
## Common Security Requirements ITSAR

**ITSAR Number: ITSAR702032601**
**ITSAR Name:** NCCS/ITSAR/Standards Applicable for Group of Equipment/CSR Group of Devices/Group-III Devices-V1.0.0

Date of Release: 29.01.2026 Version: 1.0.0
Date of Enforcement:



MTCTE के तहत जारी:
Issued under MTCTE by:
**राष्ट्रीय संचार सुरक्षा केंद्र (रा.सं.सु.कें.)**
**दूरसंचार विभाग, संचार मंत्रालय**
**भारत सरकार**
**सिटी दूरभाष केंद्र, एसआर नगर, बैंगलोर-५६००२७, भारत**
**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. | Group-III Devices Common Security Requirements ITSAR | **ITSAR702032601** | 1.0.0 | | First release |
| | | | | | |
| | | | | | |
| | | | | | |

# Table of Contents

## A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies Common Security Requirements for Group-III devices as mentioned in ***office memorandum regarding "Expanding the scope of CSR Testing"*** Ltr No. NCCS/SAS/6-1/2024-25/ dated at Bengaluru, 2nd January, 2025. As per the above referred OM, Group III contains ITSARs of the network elements of the Evolved Packet Core (EPC) in 4G LTE architecture, i.e. Serving Gateway (S-GW), Home Subscriber Server (HSS), Packet Data Network Gateway (P-GW, PDN GW), Policy and Charging Rule Function (PCRF) and Mobility management entity (MME).

Serving Gateway (S-GW) is responsible for routing and forwarding user data packets within the LTE network. It acts as the local mobility anchor point for inter-eNodeB handovers and interfaces with the Packet Data Network Gateway (P-GW).

The Home Subscriber Server (HSS) is a central database in 4G LTE that manages user subscription information and authentication. It ensures secure access and service delivery by storing user profiles and mobility data.

Packet Data Network Gateway (P-GW or PDN GW) serves as the interface between the LTE network and external packet data networks, such as the internet. It allocates IP addresses to user equipment and enforces policy and charging rules.

Mobility Management Entity (MME) is responsible for handling the mobility of users and managing signalling messages in the control plane. It plays a key role in functions such as authentication, session management, and handovers between base stations.

Policy and Charging Rules Function (PCRF) is responsible for managing Quality of Service (QoS) and enforcing charging policies for data sessions. It determines how network resources are allocated based on user subscriptions and operator policies.

This document begins with an overview of Grouping, including its scope and objectives, and then proceeds to outline the Common Security Requirements of the ITSARs applicable to Group III devices.



## B) Scope

This document defines Common Security Requirements for Indian Telecom Security Assurance Requirements (ITSARs) of Group III devices i.e. Serving Gateway (S-GW), Home Subscriber Server (HSS), Packet Data Network Gateway (P-GW,PDN GW), Policy and Charging Rule Function (PCRF) and Mobility management entity (MME). It serves as the basis for designating Telecom Security Testing Labs (TSTLs) for testing the Common Security Requirements of these devices and security certification of these devices till TSTL capable of testing SSR is available.

## C) 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 a 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.

## D) Applicability of the clauses

If a requirement explicitly specifies the applicability of a particular device, it applies and is tested only on that device; otherwise, it applies to and is tested on any one or all Group III devices.

# Chapter 1: Introduction

The ITSARs are consisting of Common Security Requirements (CSR) and Specific Security Requirements (SSR). The CSR clauses are common across most of the ITSARs. SSR clauses are specific to the network elements of the Evolved Packet Core (EPC) in 4G LTE architecture, i.e. Serving Gateway (S-GW), Home Subscriber Server (HSS), Packet Data Network Gateway (P-GW, PDN GW), Policy and Charging Rule Function (PCRF) and Mobility management entity (MME). However, the testing infrastructure requirement, skill set requirement may vary from device to device or from group of devices to group of devices.

In an endeavor to mandate testing CSR clauses of a group of devices and designate the TSTL for testing CSR clauses of a group of devices ***"Grouping of devices"*** is done.

Chapter 2 of this ITSAR outlines the Common Security Requirements applicable for designating the TSTLs for CSR testing of Group III device ITSARs.

# Chapter 2: Common Security Requirements

## Section 1: Access and Authorization

### 2.1.1 Management Protocols Mutual Authentication

Requirement:

The protocols used for the Group III device management and maintenance shall support mutual authentication mechanisms only. i.e there is mutual authentication of entities for management interfaces on the Group III device.
Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" shall only be used for Group III device management and maintenance.

*Applicable to P-GW only:* OEM /TSP shall disable permanently the supported Weaker algorithms other than specified in ITSAR Cryptographic control lists document

*Note: (applicable to P-GW only):* Any management protocol such as HTTP Over TLS 1.2 or later, IP Sec VPN are permitted. If TLS 1.2 is used, it should be patched up to date.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.4.1]

### 2.1.2 Management Traffic Protection

Requirement:

Group III device management traffic shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)".

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

### 2.1.3 Role-Based access control

Requirement:



Group III device 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.

Group III device 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 Group III device Management and Maintenance, including authorization of the operation for configuration data and software via the Group III device console interface.

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

### 2.1.4 User Authentication – Local and 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 username, 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.

*Applicable to S-GW, HSS only:* Minimum two of the above authentication attributes shall be mandatorily combined (single authentication attribute in case of machine account) for protecting the all accounts from misuse.

*Applicable to PCRF, MME only:* Minimum two of the above Authentication attributes shall be mandatorily combined for protecting the admin and/or system accounts from misuse.

*Applicable to P-GW only:* For remote user access, Minimum two of the above Authentication attributes shall be mandatorily combined to protect user accounts ((other than system /admin accounts) in open environment (internet)

**Machine Accounts:** These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.

**Local access:** The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from Group III device local hardware interface.

**Remote access:** The access which is not Local access. This includes access from the EMS (Element Management System) network, and access that originates or passes through the internet.

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

### 2.1.5 Remote login restrictions for privileged users

Requirement:

Direct login to Group III device as root or equivalent highest privileged user shall be

limited to the system console only. Root user will not be allowed to login to Group III device 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 software / tools such as TeamViewer, desktop sharing etc. which provide remote access to the Group III device.

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

### 2.1.6 Authorization Policy

Requirement:

*(applicable to S-GW, HSS & PCRF only. To be tested on any one of S-GW, HSS & PCRF of Group III)*
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.

Requirement:

*(applicable to P-GW & MME only. To be tested on any one of P-GW & MME of Group III)*

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]

### 2.1.7 Unambiguous Identification of the user & group accounts removal

Requirement:

Users shall be identified unambiguously by the Group III device.

Group III device shall support assignment of individual accounts per user, where a user could be a person, or, for machine accounts, an application, or a system. Group III device shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

*Applicable to P-GW only:* Group III device shall also support assignment of specific ID for individual accounts per user as configured by administrator/root user. Group III device's all inactive users' accounts shall be locked / Disabled.

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

## Section 2: Authentication Attribute Management

### 2.2.1 Authentication Policy

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes in case of user accounts (e.g. password, certificate, token) and single authentication attribute in case of machine account, 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.

Requirement:
*(applicable to MME only; to be tested only on MME of Group III)*

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.

Requirement:
*(applicable to P-GW only; to be tested only on P-GW of Group III)*

For local /Remote access, the various user accounts (other than system /admin accounts) on a PGW shall be protected from misuse. To this end, at least one authentication (Cryptographic keys or Token or Passwords) attribute is typically used, which, when combined with the user name, enables unambiguous authentication and identification of the authorized user in closed environment For Local /Remote access, Minimum two of the Authentication attributes (Cryptographic Keys, Token, Passwords) shall be mandatorily combined to protect user accounts ((other than system /admin accounts) in open environment (internet)

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

### 2.2.2 Authentication Support – External

Requirement:

If the Group III device supports external authentication mechanism such as AAA server

(for authentication, authorization, and accounting services) then the communication between Group III device 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 latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) only.

### 2.2.3 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:

(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 an authentication attribute blacklist to prevent vulnerable passwords.
(iv) Using CAPTCHA to prevent automated attempts (often used for Web applications).

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

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

### 2.2.4 Enforce Strong Password



Requirement:

The configuration setting shall be such that an Group III device 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 Group III device). It shall not be possible setting this absolute minimum length to a lower value by configuration.
ii. Password shall mandatorily comprise 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.

Group III device shall have in-built mechanism to support this requirement, further 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.

And if a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Group III device.

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

*Applicable to HSS, PCRF and S-GW only:* Above requirements shall be applicable for all passwords used (e.g. application-level, OS- level, etc.).

*Applicable to P-GW only:* Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.4.3.1]

### 2.2.5 Inactive Session Timeout

Requirement:
*(applicable to HSS, S-GW and PCRF only; to be tested on any one of HSS, S-GW and PCRF of Group III)*

An OAM user inactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.

Group III device shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.

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

Requirement:
*(applicable to P-GW and MME only; to be tested on any one of P-GW and MME of Group III)*

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.

### 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. Group III device 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 Group III device shall store at least the three previously set passwords. The maximum number of passwords that the Group III device 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.

*Applicable to HSS, S-GW and PCRF only:* Above requirements shall be applicable for all passwords used (e.g. application- level, OS-level, etc.). An exception to this requirement is machine accounts. Group III device to have in-built mechanism to support this requirement. 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 change policies as laid down for the local system in this subclause. And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the Group III device.

*Applicable to P-GW and MME only:* This requirement shall be met either by Group III device 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]

### 2.2.7 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]

### 2.2.8 Removal of predefined or default authentication attributes

Requirement:

Predefined or default authentication attributes shall be deleted or disabled.

*Applicable to HSS, S-GW and PCRF only:* Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the OEM provides instructions on how to manually change it.

[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

### 2.3.1 Secure Update

Requirement:
*(applicable to HSS, S-GW and PCRF only; to be tested on any one of HSS, S-GW and PCRF of Group III)*
For software updates, Group III device shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls as prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)".

To this end, the network product has a list of public keys or certificates of authorized software sources, and uses the keys to verify that the software update is originated from only these sources.



Requirement:
*(applicable to P-GW and MME only; to be tested on any one of P-GW and MME of Group III)*

Group III device'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.

Group III device 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 Table1 of the document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0" only.

### 2.3.2 Secure Upgrade

Requirement:
*(applicable to HSS, S-GW and PCRF only; to be tested on any one of HSS, S-GW and PCRF of Group III)*

i. Software package integrity shall be validated in the installation/upgrade stage.
ii. Group III device shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using the secure cryptographic controls as prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR).. To this end, the Group III device shall have a list of public keys or certificates of authorized 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. A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in point (ii).

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

Requirement:
*(applicable to P-GW and MME only; to be tested on any one of P-GW and MME of Group III)*

(i) Group III device 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) Group III device shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the P-GW 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) Group III device'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 (ii) above.

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

### 2.3.3 Source code security assurance

Requirement:

a) OEM shall follow security practices including secure coding for software development. Source code shall be made available either at TSTL premises or at the mutually agreed location for source code review by the designated TSTL. It may be supported by furnishing the Software Test Document (STD).
b) Also, OEM 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 Group III device software, which includes vendor developed code, third party software and open source code libraries used/embedded in the Group III device.
   ii. The Group III device software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of Group III device to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.
   iii. The binaries for Group III device and upgrades/updates thereafter generated from the source code are free from CWE top 25 & OWASP top 10 security weaknesses.

### 2.3.4 Known Malware and backdoor Check

Requirement:

OEM shall submit an undertaking stating that Group III device is free from all known malware and backdoors as on the date of offer of Group III device to designated TSTL for testing and shall submit Malware test document (MTD).

### 2.3.5 No unused software

Requirement:

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

*Applicable to HSS, PCRF, P-GW and S-GW only:* Orphaned software components /packages shall not be present in Group III device.
OEM shall provide the list of software that are necessary for its operation. OEM shall furnish an undertaking as "Group III device does not contain Software that is not used in the functionality of Group III device"

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

### 2.3.6 Unnecessary Services Removal

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

Group III device 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. Group III device Shall not support following services. Any other protocols, services that are vulnerable are also to

be permanently disabled.

- 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

Full documentation of required ports, protocols and services (Communication matrix) of the Network product and their purpose needs to be provided by the OEM 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]

Requirement:
*(applicable to P-GW and MME only; to be tested only on P-GW and MME of Group III)*

Group III device 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.

### 2.3.7 Restricting System Boot Source

Requirement:

Group III device 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]

### 2.3.8 Secure Time Synchronization

Requirement:

Group III device shall provide reliable time and date information provided by itself or through NTP/PTP server. Group III device shall provide reliable time and date information provided through NTP/PTP server.

Group III device shall establish secure communication channel with the NTP/PTP server. Group III device shall establish secure communication channel strictly using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)"

with NTP/PTP server.

Group III device shall generate audit logs for all changes to time settings.

### 2.3.9 Restricted reachability of services

Requirement:

The Group III device 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.

*Applicable to HSS, S-GW and PCRF only*: Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for 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]

### 2.3.10 Self-Testing /Avoidance of Unspecified Wireless Access

**Self-Testing:**

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

Group III device shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of "self-test" of FIPS-140-2 or Later version etc.,) to identify failures in its security Mechanisms during
i) power on
ii) when Administrator Instructs
III) Periodic, with period configurable.

*(applicable to P-GW and MME only; to be tested on any one of P-GW and MME of Group III)*

**Avoidance of Unspecified Wireless Access**

Requirement:

An undertaking shall be given as follows:

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

### 2.3.11 Disable Control + Alt +Del option

Requirement:
*(applicable to P-GW only; to be tested only on P-GW of Group III)*

The P-GW Operating system may use option (Control + ALT +DEL) to forcibly to reboot, forcing the programs to stop. This feature may be misused by internal attackers. The same option shall be permanently disabled.

### 2.3.12 Disable USB stick detection

Requirement:
*(applicable to P-GW only; to be tested only on P-GW of Group III)*

System shall restrict users from using USB stick to protect and secure data from stealing.

### 2.3.13 Lock Down Cron Jobs

Requirement:
*(applicable to P-GW only; to be tested only on P-GW of Group III)*

Scheduling commands or tasks are called Cron Jobs. Cron Jobs are used for running scheduled backups, monitor disk space, and running system maintenance tasks. Running Cron Jobs should be restricted to specific users including administrator.

## Section 4: System Secure Execution Environment

### 2.4.1 No unused functions

Requirement:

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

*Applicable to S-GW, HSS and PCRF only:* List of the used functions of the Networks software and hardware as given by the OEM shall match the list of used software and hardware functions that are necessary for the operation of the Group III device.

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

### 2.4.2 No unsupported components

Requirement:

OEM/Vendor to ensure that the Group III device shall not contain software and hardware components that are no longer supported by OEM/Vendor or its third 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]

### 2.4.3 Avoidance of Unspecified mode of Access

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

Group III device shall not contain any mode of access (e.g. wireless) mechanism which is unspecified or not declared.

An undertaking shall be given by the OEM as follows:
"The Group III device 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 5: User Audit

### 2.5.1 Audit trail storage and protection

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*
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. The rights to delete or modify the log files are to be restricted, a trail of delete or modify activities may be logged in separate log file.

Requirement:
*(applicable to MME and P-GW only; to be tested on any one of MME and P-GW of Group III)*
The security event log shall be access controlled using file access conditions such that only privilege users including the administrator have access to read the log files but not allowed to delete the log files.

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

### 2.5.2 Audit Event Generation

Requirement:

The Group III device shall log all important security events with unique System Reference details as given in the Table below.
Group III device 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:

| Sl | Event Types (Mandatory | Description | Event data to be logged |
|---|---|---|---|

| No | or optional) | | |
|---|---|---|---|
| 1 | Incorrect login attempts (Mandatory) | Records any user's incorrect login attempts to the DUT | Username |
| | | | Source (IP address) if remote access |
| | | | Outcome of event (Success or failure) |
| | | | Date and Timestamp |
| 2 | Administrator access (Mandatory) | Records any access attempts to accounts that have system privileges. | Username, |
| | | | Date and Timestamp, |
| | | | Length of session |
| | | | Outcome of event (Success or failure) |
| | | | Source (IP address) if remote access |
| 3 | 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) |
| | | | Date and Timestamp |
| 4 | 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 (Threshold Exceeded) |
| | | | Date and Timestamp |
| 5 | Configuration change (Mandatory) | Changes to configuration of the system | Change made |
| | | | Date and Timestamp |
| | | | Outcome of event (Success or failure) |
| | | | Username |
| 6 | 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) |
| | | | Date and Timestamp |
| 7 | Interface status change | Change to the status of | Interface name and type |

| | | | |
|---|---|---|---|
| | (Mandatory) | interfaces on the network device (e.g., shutdown) | Status (shutdown, down missing link, etc.) |
| | | | Outcome of event (Success or failure) |
| | | | Date and Timestamp |
| 8 | 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) |
| | | | Date and Timestamp. |
| 9 | 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) |
| | | | Date and Timestamp |
| 10 | Services (Optional) | Starting and Stopping of Services (if applicable) | Service identity |
| | | | Activity performed (start, stop, etc.) |
| | | | Date and Timestamp |
| | | | Outcome of event (Success or failure) |
| 11 | User login (Mandatory) *(applicable to S-GW, HSS, PCRF and P-GW only)* | All use of identification and authentication mechanism | user identity |
| | | | origin of attempt (e.g. IP address) |
| | | | Date and Timestamp |
| | | | outcome of event (Success or failure) |
| 12 | X.509 Certificate Validation (Optional) | Unsuccessful attempt to validate a certificate | Date and Timestamp |
| | | | Reason for failure |
| | | | Subject identity |
| | | | Type of event |
| 13 | Secure Update (Optional) | Attempt to initiate manual update, initiation of update, completion of update | User identity |
| | | | Date and Timestamp |
| | | | Outcome of event (Success or failure) |
| | | | Activity performed |
| 14 | Time change (Mandatory) | Change in time settings | Old value of time |
| | | | New value of time |
| | | | Date and Timestamp |

| | | | |
|---|---|---|---|
| | | | origin of attempt to change time (e.g., IP address) |
| | | | Subject identity |
| | | | Outcome of event (Success or failure) |
| | | | User identity |
| 15 | Session unlocking/ termination (Optional) *(applicable to S-GW, HSS, PCRF and P-GW only)* | Any attempts at unlocking of an interactive session, Termination of a remote session by the session locking mechanism, Termination of an interactive session | user identity (wherever applicable) |
| | | | Date and Timestamp |
| | | | Outcome of event (Success or failure) |
| | | | Subject identity |
| | | | Activity performed |
| | | | Type of event |
| 16 | Trusted Communication paths (with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorised remote administrators) (Optional) *(applicable to S-GW, HSS, PCRF and P-GW only)* | Initiation, Termination and Failure of trusted Communication paths | Date and 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) |
| 17 | Audit data changes (Optional) *(applicable to S-GW, HSS, PCRF and P-GW only)* | Changes to audit data including deletion of audit data | Date and 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 |
| 18 | Port Scan Attempts *(applicable to S-GW, HSS and PCRF only)* | Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters | Date & Time Stamp |
| | | | Source IP Address |
| | | | Destination Port Address |
| 19 | Access to personal data ( Mandatory) *(applicable to P-GW only)* | All use of identification and authentication mechanism | user identity |
| | | | origin of attempt (e.g.IP address) |
| | | | Date and Timestamp |

| | | | |
|---|---|---|---|
| | | | Personal data in encrypted text(Optional) |
| | | | Outcome of event (Success or failure) |

[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]

### 2.5.3 Secure Log Export

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

i. (a) The Group III device shall support forwarding of security event logging data to an external system by push or pull mechanism.
   (b) Log functions should support secure uploading of log files to a central location or to a system external for the Group III device.
ii. Group III device shall be able to store generated audit data itself, may be with limitations.
iii. Group III device shall alert administrator when its security log buffer reaches configured threshold limit.
iv. In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), Group III device shall have mechanism to store audit data locally. Group III device shall have sufficient memory (minimum 100 MB) allocated for this purpose. OEM to submit justification document for sufficiency of local storage requirement.
v. Secure Log export shall comply the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

Requirement:
*(applicable to MME and P-GW only; to be tested on any one of MME and P-GW of Group III)*



i. (a)The Group III device shall support forward of security event logging data to an external system by push or pull mechanism.
   (b)Log functions should support secure uploading of log files to a central location or to a system external for the Group III device.
ii. Group III device shall be able to store generated audit data itself, may be with limitations.
iii. Group III device shall alert administrator when its security log buffer reaches configured threshold limit.
iv. In the absence of External system, Group III device 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

### 2.6.1 Cryptographic Based Secure Communication with connecting entities

Requirement:

Group III device shall Communicate with the connected entities strictly using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

*Applicable to P-GW only:* Vendor shall submit to TSTL, the list of the connected entities with Group III device and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration and detailed procedure of establishing the communication with each entity.

### 2.6.2 Cryptographic Module Security Assurance

Requirement:

Cryptographic module embedded inside the Group III device (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 Level 2.

*Applicable to P-GW only:* Vendor shall also submit cryptographic module implementation testing document and the test results to designated TSTL for scrutiny.

*Applicable to HSS, PCRF and S-GW only:* Till further instructions, this clause will be considered complied by submission of an undertaking by the OEM in specified format along with self-certified test reports. An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the Group III device (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. " OEM cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

### 2.6.3 Cryptographic Algorithms implementation Security Assurance

Cryptographic algorithms embedded in the crypto module of Group III device shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm). OEM shall submit Cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results. for scrutiny.

*Applicable to HSS, PCRF and S-GW only:* Till further instructions, this clause will be considered complied by submission of an undertaking by the OEM in specified format along with self-certified test reports. An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms embedded in the crypto module of Group

III device shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)."

### 2.6.4 Protecting data and information – Confidential System Internal Data

Requirement:

When Group III device 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 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.]

### 2.6.5 Protecting data and information in storage

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

For Sensitive data in storage (persistent or temporary), read access rights shall be restricted. Files of Group III device 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/readable form e.g. in order to perform an activity/operation, such systems shall not store this data in the clear/readable form, encrypt it by implementation-specific means, strictly using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) .
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 latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0".
iii. Stored files: Files having sensitive data shall be protected against manipulation strictly using checksum or cryptographic methods as defined in NCCS approved secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)"

**Sensitive data:** data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.

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

Requirement:

*(applicable to MME and P-GW only; to be tested on any one of MME and P-GW of Group III)*

For sensitive data (persistent or temporary), read access rights shall be restricted. Files of Group III 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" only.
iii. Stored files in the Group III device: 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: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3]

### 2.6.6 Protection against Copy of Data

Requirement:

Without authentication, Group III device shall not create a copy of data in use or data in transit.

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

### 2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement:

Group III device shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound overt channels such as, HTTPS IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network product.

*Applicable to HSS, PCRF and S-GW only:* Session logs shall be generated for establishment of any session initiated by either user or Group III device.

### 2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:

Group III device 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 auto-initiated by / auto-originated from the Network Product.

Session logs shall be generated for establishment of any session initiated by either user or Group III device.

## Section 7: Network Services

### 2.7.1 Traffic Filtering – Network Level

Requirement:
*(applicable to HSS, PCRF, S-GW and P-GW only; to be tested on any one of HSS, PCRF, S-GW and P-GW of Group III)*

Group III device 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. *Applicable to HSS, PCRF and S-GW only:* 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]

### 2.7.2 Traffic Separation

Requirement:

Group III device 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].

### 2.7.3 Traffic Protection – Anti-Spoofing

Requirement:
*(applicable to HSS, PCRF, S-GW and P-GW only; to be tested on any one of HSS, PCRF, S-GW and P-GW of Group III)*

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

### 2.8.1 Network Level and application-level DDoS

Requirement:

Group III device shall have protection mechanism against known network level and application-level DDoS attacks.
*Applicable to P-GW only: "supported by itself or supported in tandem by external firewall device"*

Group III device 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 p rotective 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 a 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]

### 2.8.2 Excessive Overload Protection

Requirement:

Group III device shall act in a predictable way if an overload situation cannot be prevented. Group III device 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 Group III device 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]

### 2.8.3 Filtering IP Options

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

IP packets with unnecessary options or extension headers shall not be processed. IP options and extension headers (e.g. source routing) are only required in exceptional cases. So, all packets with enabled IP options or extension headers shall be filtered.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.4.1.1.3]

## Section 9: Vulnerability Testing Requirements

### 2.9.1 Fuzzing – Network and Application Level

Requirement:

It shall be ensured that externally reachable services of Group III device are reasonably robust when receiving unexpected input /Malformed input requests.

*Applicable to P-GW only:* Vendor should document the list of Protocol stacks supported by P-GW for all traffic planes (Management, Control, Data plane and Service /Application plane)

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

### 2.9.2 Port Scanning

Requirement:



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

*Applicable to P-GW and MME only:* 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]

### 2.9.3 Vulnerability Scanning

Requirement:

*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

It shall be ensured that no known critical/ high/medium (as per CVE-IDs of NIST- NVD) vulnerabilities (as on date of offer of Group III device to designated TSTL for testing) shall exist in the Group III device. For low/uncategorized (as per CVE-IDs of NIST- NVD) category vulnerabilities remediation plan is to be provided.

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

Requirement:
*(applicable to MME and P-GW only; to be tested on any one of MME and P-GW of Group III)*

It shall be ensured that there are no known vulnerabilities exist in the Group III device at the date of product release. The purpose of vulnerability scanning is to ensure that there are no known vulnerabilities (or that relevant vulnerabilities are identified and remediation plans in place to mitigate them) on the Group III device 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

### 2.10.1 Growing Content Handling

Requirement:

Growing or dynamic content on Group III device 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 Group III device 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]

### 2.10.2 Handling of ICMP

Requirement:

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

Group III device 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 | Neighbor Solicitation | Permitted | Permitted |
| N/A | 136 | Neighbor Advertisement | Permitted | N/A |

Group III device 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.]

### 2.10.3 Authenticated Privilege Escalation only

Requirement:



Group III device 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]

### 2.10.4 System account identification

Requirement:

Each system account in Group III device shall have a unique identification with appropriate nonrepudiation controls.

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

### 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 Group III device. Kernel based network functions not needed for the operation of the Group III device shall be deactivated.

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

### 2.10.6 No automatic launch of removable media

Requirement:

Group III device 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]

### 2.10.7 Protection from buffer overflows

Requirement:

Group III device shall support mechanisms for buffer overflow protection.

*Applicable to HSS, S-GW and PCRF only:* Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided by the OEM.

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

### 2.10.8 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 Group III device in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.

*Applicable to HSS, S-GW and PCRF only:* OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

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

### 2.10.9 File-system Authorization privileges

Requirement:

Group III device 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]

### 2.10.10 Restrictions on running Scripts / Batch-processes

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

Group III device shall have feature to restrict Scripts / Batch-processes / Macros usage among various users. It shall be administratively configurable to permit or deny the use. E.g. It is possible to administratively configure scheduled tasks usage (permit / deny) among various users like Normal users, privileged users.

### 2.10.11 Restrictions on Soft-Restart

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

Group III device shall restrict software-based system restart options usage among various users. The software reset / restart either through command or use of key-combinations like CTRL+ALT+DEL is not available to normal users for prevention of unintended / malicious trigger of system reset / restart.

## Section 11: Web Servers

This entire section of the security requirements is applicable if the Group III device supports web management interface.

### 2.11.1 HTTPS

Requirement:



The communication between web client and web server shall be protected strictly using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

### 2.11.2 Webserver logging

Requirement:

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

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]

### 2.11.3 HTTPS input validation

Requirement:

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

Group III device 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]

### 2.11.4 No system privileges

Requirement:

No Group III device 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]

### 2.11.5 No unused HTTPS methods

Requirement:

HTTPS methods that are not required for Group III device operation shall be deactivated.



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

### 2.11.6 No unused add-ons

Requirement:

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

### 2.11.7 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]

### 2.11.8 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]

### 2.11.9 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]

### 2.11.10 Access rights for web server configuration

Requirement:

Access rights for Group III device 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]

### 2.11.11 No default content



Requirement:

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

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

### 2.11.12 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]

### 2.11.13 Web server information in HTTPS headers

Requirement:

The HTTPS header shall not include information on the version of the Group III device 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]

### 2.11.14 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 Group III device web server and the modules/add-ons used.
Default error pages of the Group III device web server shall be replaced by error pages defined by the OEM.

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

### 2.11.15 Minimized file type mappings

Requirement:

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

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

### 2.11.16 Restricted file access

Requirement:

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

In particular, the Group III device 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]

### 2.11.17 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

### 2.12.1 Remote Diagnostic Procedure – Verification

Requirement:
*(applicable to HSS, MME, PCRF and S-GW only; to be tested on any one of HSS, MME, PCRF and S-GW of Group III)*

If the Group III device 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:

1. User id
2. Time stamp
3. Interface type
4. Event level (e.g. CRITICAL, MAJOR, MINOR)
5. Command/activity performed and
6. Result type (e.g. SUCCESS, FAILURE).
7. IP address of remote machine

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

### 2.12.2 No System/Root Password Recovery

Requirement:

No provision shall exist for Group III device System / Root password recovery.

In the event of system password reset (e.g., through press of Hard-reset button), the entire configuration of the Group III device shall be irretrievably deleted."

### 2.12.3 Secure System Software Revocation

Requirement:

Once the Group III device 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.

Group III device shall support a well-established control mechanism for rolling back to previous software image.

### 2.12.4 Software Integrity Check – Installation

Requirement:

Group III device shall validate the software package integrity before the installation/upgrade stage strictly using the Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)." only.

*Applicable to S-GW,P-GW,MME and HSS only:* Tampered software shall not be executed or installed if integrity check fails.

### 2.12.5 Software Integrity Check – Boot

Requirement:

The Group III device shall verify the integrity of software component(s) at boot time by comparing the result of a standard cryptographic hash generated strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" to the expected reference value.

*Applicable to MME and P-GW only:* The Group III device shall support the possibility to verify software image integrity at boot time, detecting, for example, software image tampering and/or unauthorized software image updates.

### 2.12.6 Unused Physical and Logical Interfaces Disabling

Requirement:

Group III device 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 disabled so that they remain inactive even in the event of a reboot.

### 2.12.7 No Default Profile

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

No pre-defined user accounts other than one Highest privilege (Admin / Root) user account would be available.

Requirement:
*(applicable to MME and P-GW only; to be tested on any one of MME and P-GW of Group III)*

Predefined or default user accounts in the Group III device shall be deleted or disabled.

### 2.12.8 Security Algorithm Modification

Requirement:
*(applicable to HSS, PCRF and S-GW only; to be tested on any one of HSS, PCRF and S-GW of Group III)*

It shall not be possible to modify security algorithms supported by Group III device without admin / root credentials. Bidding-down beyond prescribed security / cryptographic algorithms by means of negotiation by communicating entities is not permitted.

Requirement:
*(applicable to MME only; to be tested only on MME of Group III)*

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

Requirement:
*(applicable to P-GW only; to be tested only on P-GW of Group III)*

It shall not be possible to modify security algorithms supported by P-GW through unauthorized access, e.g. to perform a downgrade attack by deceiving the nodes to use a weaker algorithm.

## 12.9 Control Plane Traffic Protection

Requirement:
*(applicable to MME only; to be tested only on MME of Group III)*

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.

# Annexure-I

**Acronyms**

| | |
|---|---|
| AAA Server | Authentication, Authorization, and Accounting |
| ACL | Access Control Lists |
| AES | Advanced Encryption Standard |
| AF | Application Function |
| 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 |
| AVP | Attribute value Pair |
| 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 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 Centre |
| 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 |
| PCRF | Policy Charging and Rule Function |
| 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 |
| Server CVE | Common Vulnerabilities and Exposures |
| SFTP | Secure File Transfer Protocol |
| SGSN | Serving GPRS Support Node |
| S-GW | Network Element |
| 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 |
| TDF | traffic detection function |
| 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 |

# Annexure-II

**List of Submissions**

List of undertakings to be furnished by the OEM for Group III devices Security testing submissions.

1) Source Code Security Assurance (against test case 2.3.3)
2) Known Malware and backdoor Check (against test case 2.3.4)
3) No unused Software/ No unused Software Packages (against test case 2.3.5)
4) No unsupported Components (against test case 2.4.2)
5) Avoidance of Unspecified Modes of Access (against test case 2.4.3)
6) Cryptographic Based Secure Communication (against test case 2.6.1)
7) Cryptographic Module Security Assurance (against test case 2.6.2)
8) Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)

# Annexure-III

**References**

1.TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0: "Catalogue of General Security Assurance Requirements".
2. TSDSI STD T1.3GPP 33.250-14.0.0 V.1.0.0:Security Assurance Specification for the PGW network product class.
3. TSDSI STD T1.3GPP 33.210 14.0.0 V.1.0.0:Network Domain Security (NDS)/IP Network Layer Security.
4. TSDSI STD T1.3GPP 33.401 14.5.0 V.1.0.0 : "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".
5. TSDSI STD T1.3GPP 33.926-14.0.0 V1.0.0 Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes.
6. 3GPP TS 23.203: "Policy and charging control architecture".
7. 3GPP TS 32.251: " Packet Switched (PS) domain charging"
8. NIST FIPS 140-2 specification.
9. Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0