Indian Telecom Security Assurance Requirements (ITSAR)

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

# Group-IV Devices
## Common Security Requirements ITSAR

**ITSAR Number: ITSAR702042504**
**ITSAR Name:** NCCS/ITSAR/Standards Applicable for Group of Equipment/CSR Group of Devices/Group-IV Devices-V1.0.0

Date of Release: 21.04.2025
Date of Enforcement:

Version: 1.0.0

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-IV Devices Common Security Requirements | ITSAR702042504 | 1.0.0 | 21.04.2025 | First release |
| | | | | | |
| | | | | | |
| | | | | | |

# Table of Contents

# A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies Common Security Requirements for Group-IV 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 IV contains ITSARs of four devices viz., Wi-Fi CPE V1.0.1, IP Router V1.0.1, Cell Broadcast Centre (CBC) V1.0.0 and Private Automatic Branch Exchange (PABX) V1.0.1.

A **Wi-Fi CPE (Customer Premises Equipment)** device is a networking device used to connect end users to an internet service provider (ISP) via Wi-Fi. These devices are commonly used in home and business networks and can take different forms depending on the type of internet connection.

An **IP router** is a networking device that directs data packets between computer networks, ensuring efficient communication between devices. It operates at the network layer (Layer 3) of the OSI model and determines the best path for data to travel across interconnected networks.

A **Cell Broadcast Center (CBC)** is a telecommunications system responsible for sending cell broadcast messages to mobile users within a specific geographic area. It is widely used for emergency alerts, weather warnings, disaster notifications, and government announcements.

A **PABX (Private Automatic Branch Exchange)** is a private telephone system used within an organization to manage internal and external calls. It enables businesses to connect multiple phone lines and extensions without requiring a separate phone line for each user.

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 IV devices.

# B) Scope

This document defines Common Security Requirements for Indian Telecom Security Assurance Requirements (ITSARs) of Group IV devices (*Wi-Fi CPE V1.0.1, IP Router V1.0.1, Cell Broadcast Centre V1.0.0 and Private Automatic Branch Exchange V1.0.1*).

It serves as the basis for designating labs as 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 to 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 IV devices

# Chapter 1

### 1.1 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 Communication device. 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 endeavour 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 labs for CSR testing of Group IV device ITSARs.

# Chapter 2 - Common Security Requirements

## Section 2.1: Access and Authorization

### 2.1.1 Management Protocols Entity Mutual Authentication

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The CPE shall communicate with authenticated management entities only. The protocols used for the CPE management shall support mutual authentication mechanisms, preferably with pre- shared key arrangements or by equivalent entity mutual authentication mechanisms. This shall be verified for all protocols used for CPE management. (This feature shall be supported on all WAN management interfaces).

### 2.1.2 Management Protocols Mutual Authentication

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

The protocols used for the device's management shall support mutual authentication mechanisms. There is mutual authentication of entities for management interfaces on the device. HTTPS with TLS 1.2, SNMP V3 Protocols are allowed.

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

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

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

### 2.1.3 Management Traffic Protection

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

All management traffic shall be protected by integrity and encryption. Unprotected sessions shall not be accepted. The remote access methods can support traffic encryption using protocols such as HTTPS, SSHv2 or can be based on lower tunneling protocols (IPsec VPN, TLS VPN, etc.).

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Usage of cryptographically protected network protocols is required. The transmission of data with a need of protection shall use industry standard network protocols with sufficient security measures and industry accepted algorithms. In particular, a protocol version without known vulnerabilities or a secure alternative shall be used. Verify the mechanisms implemented to protect data and information in transfer to and from the Device's OAM interface.

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

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Device management traffic shall be protected strictly using Secure cryptographic controls prescribed in Table1 of the latest document "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 4.2.3.2.4]

### 2.1.4 Role-Based access control

Requirement:

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE shall support Role-Based Access Control (RBAC) which provides at least two different access levels or domains to guarantee that individuals can only perform the operations that they are authorized for. The RBAC system controls how users are allowed access to the various domains and what type of operations.

Requirement:

*(applicable to CBC, PABX and IP Router of Group IV; to be tested on any one of CBC, PABX and IP Router of Group IV)*

The Group IV 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 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 Group IV device supports RBAC with minimum of 3 user roles, in particular, for OAM privilege management for device Management and Maintenance, including authorization of the operation for configuration data and software via the device console interface.

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

### 2.1.5 User Authentication - Local/Remote

Requirement:

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Local/Remote access to the CPE for configuration and maintenance purposes shall be granted only to authenticated users or machines using at least one authentication attribute. This authentication attribute when combined with the user's name shall enable unambiguous authentication and identification of the authorized user. No methods to exist providing authentication-bypass attacks to succeed under all combinations of interface / methods of authentication.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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 (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]

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

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. Minimum two of the above Authentication attributes shall be mandatorily combined for protecting all the accounts from misuse. An exception to this requirement is machine accounts where at least one authentication attribute shall be supported.

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

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

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. Minimum two of the above authentication attributes shall be mandatorily combined for protecting the all accounts from misuse.

Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from PABX 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]

### 2.1.6 Remote Management Standards

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The remote management mechanisms for CPE to be fully compliant with the remote management standards that the OEM chose to implement, example: TR-069 or any other relevant standards, such mechanisms to include entity mutual authentication, encryption of the management traffic.

### 2.1.7 Remote login restrictions for privileged users

Requirement:

*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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]

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Login to 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 device remotely. This remote root user access restriction is also applicable to application software's / tools such as TeamViewer, desktop sharing which provide remote access to the device.

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

### 2.1.8 Authorization Policy

*(applicable to CBC, PABX and IP Router only; to be tested on any one of CBC, PABX and IP Router of Group IV)*

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]

### 2.1.9 Unambiguous identification of the user & group

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The CPE shall identify each login user unambiguously. CPE shall be able to assign individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system. It is a desirable feature to configure user preferred USERID name in configuration menu instead of pre-configured ADMIN User ID. Use of group accounts or group credentials or sharing of the same account between several users shall not be enabled by CPE.

### 2.1.10 Unambiguous identification of the user & group accounts removal

*(applicable to CBC, PABX and IP Router only; to be tested on any one of CBC, PABX and IP Router of Group IV)*

Requirement:

Users shall be identified unambiguously by the Group IV device. Group IV 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. Device 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]

### 2.1.11Remote Management Standards for Connected Devices, Additional Features

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The remote management mechanisms for devices connected to CPE, or for configuration of additional features of CPE like DDNS, UPnP etc., are to be compliant with the respective latest standards published at the time of commencement of security testing. These additional features are to be configured as disabled in the factory default settings, with provision for user to enable individual features on menu-selection. Such mechanisms to include entity mutual authentication, encryption of the management traffic.

## Section 2.2: Authentication and Attribute Management

### 2.2.1 Authentication Policy

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The usage of a system functions such as network services (like SSH, SFTP, Web services), management access, local usage of operating systems and applications shall be allowed only after successful authentication on the basis of the user identity and at least one authentication attribute (e.g., password, certificate). This requirement shall also be applied to accounts that are only used for communication between systems.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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]

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (e.g. password, certificate, token) shall be prevented. For machine-to-machine accounts one authentication attribute will be sufficient. 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.

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

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

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

[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:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

If CPE supports external authentication (for the Cyber- Cafe use-case scenario), the user authentication credentials should be protected and securely communicated if the authentication credentials are managed by external authentication servers

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

External authentication mechanism if supported by IP router (support authentication, authorization, and accounting server capabilities) should be through secure (encrypted) communication channel.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

CBC shall support external authentication mechanism such as AAA server (for authentication, authorization, and accounting services), then the communication between CBC 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 “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

If the PABX supports external authentication mechanism such as AAA server (for authentication, authorization, and accounting services) then the communication between PABX 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:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE shall have a mechanism that provides a protection against brute force and dictionary attacks which aim to use manual/automated guessing to obtain the passwords for user and machine accounts. CPE to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it may implement at least one of the following most commonly used protection measures:

(a) Increasing the delay (e.g., doubling) for each newly entered incorrect password.
(b) Blocking an account after a specified number of incorrect attempts (typically 5) for a certain period of time.
(c) Using CAPTCHA to prevent automated attempts.

This feature to be enabled for login attempts for CPE and on authentication attempts on Wi-Fi access through SSID with PSK.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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 on 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, it is often meaningful to combine two or more of the measures named here. It is left to the vendor to select appropriate measures. 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. Section4.2.3.4.3.3]

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in device. 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:

- (a) Using the timer delay (this delay could be the same or increased depending on the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
- (b) 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.
- (c) Using an authentication attribute blacklist to prevent vulnerable passwords.
- (d) 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 CBC. An exception to this requirement is machine accounts.

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

### 2.2.4 Enforce Strong Password

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE shall only accept passwords that comply with the following complexity criteria:

- i. Password containing a minimum length of 8 characters are only permitted by default. Shorter lengths shall be rejected by the NE.
- ii. Minimum password length - the default minimum value of 8 characters.
- iii. Password comprises at least three of the following categories:
  - 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., @; $.)

CPE shall support password field length of minimum 64 characters.

This Feature to be enabled for CPE Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

Requirement:

*(applicable to IP Router and PABX only; to be tested on any one of IP Router, and PABX of Group IV)*

a) The configuration setting shall be such that Group IV 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 IV 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. @;!$.)

b) 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.

c) 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 sub-clause.

d) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Group IV device.

e) When a user is changing a password or entering a new password, Group IV device /central 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.).

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]

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

f) The configuration setting shall be such that Group IV device shall only accept passwords that comply with the following complexity criteria:

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

  iv. 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. @;!$.)

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.

h) 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 sub-clause.

i) If a central system is not used for user authentication, the assurance on password complexity rules shall be performed on the Group IV device.

j) When a user is changing a password or entering a new password, Group IV device /central 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.).

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 Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE shall monitor inactive sessions of administrative login users, Data users either on LAN or Wi-Fi 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. When the time out occurs, the same screen must be cleared of all displayed information.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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.

NOTE: The kind of activity required to reset the timeout timer depends on the type of user session.

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

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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. 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]

### 2.2.6 Password Change facility, 1st Installation /Factory Reset

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

CPE shall enforce change of authentication attribute (eg: - password) on 1st installation configuration or on factory reset conditions. If a password is used as an authentication attribute, then the CPE shall provide a function that facilitates the user to change his password at any time. However, the CPE shall not allow the previously used passwords up to a certain number (Password History)

### 2.2.7 Password Changes

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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 Device shall store at least the three previously set passwords. The maximum number of passwords that the 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. 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 Device itself or in combination with external authentication system.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

Password change shall be enforced after initial login.

Device shall enforce password change based on password management policy. In particular, the system shall enforce password expiry. Device shall support a configurable period for expiry of passwords. 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 minimum value shall be 3. This means that the CBC shall store at least the three previously set passwords. The maximum number of passwords that the CBC 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. 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 sub-clause. And if a central system is not used for user authentication, the assurance on password changes rules shall be performed on the device.

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

### 2.2.8 Protected Authentication feedback

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

When a user enters the password at the local console, local or remote management GUI, the CPE should give obscure feedback by displaying characters like "*".

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

The Authentication attributes 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 "*". Under certain circumstances it may be permissible for an individual character to be displayed briefly during input. Such a function is used, for ex ample, on smartphones to make input easier. However, the entire password is never output to the display in plaintext.

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]

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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 is 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]

### 2.2.9 Removal of predefined or default authentication attributes

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE may come with predefined (by the vendor, developer, or producer) authentication attributes such as password or cryptographic keys. CPE shall remove the predefined / default authentication attributes from its run-time configuration. Such predefined authentication attributes can be restored only through factory reset, preferably through operating a physical button.

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX of Group IV)*

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 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]

### 2.2.10 Storage of Passwords in encrypted form

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

User passwords should be stored using password hashes or encrypted, based on a strong hashing mechanism designed for use with passwords (example: HMAC, PBKDF2, Argon2), OEM may choose his own hashing mechanism for implementation. Passwords may not be stored in clear text. This requirement does not apply to pre-shared keys that must be used in raw form, such as IKE pre-shared keys.

## Section 2.3: Software Security

### 2.3.1 Secure Update

*Requirement:*

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The update process should verify the authenticity of the source repository and the integrity of the software patch preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity before updating the software in the CPE. The update mechanism should prevent illegal software patching.

Requirement:

*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Device's system software updates should be secure and shall be based on signed certificates. Device shall allow updates only if code signing certificate is valid and time not expired, the software update integrity shall be verified by hashing mechanism (like SHA2).

Note: TSPs are responsible to ensure that Software updates/patches implemented are secure and safe from any vulnerability. TSPs to maintain information about updates as per Licensing agreement /amendment conditions. However, if there is any patch/update/version change which affects the security functionality then the details of the same should be reported to TTSC/DOT by vendor /TSPs.

Requirement:

*(applicable to CBC only; to be tested only on CBC of Group IV)*

For software updates, 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 prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

To this end, the device 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 PABX only; to be tested only on PABX of Group IV)*

PABX's system software updates shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

PABX 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 latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

### 2.3.2 Secure Upgrade

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE should support authenticity and integrity check while performing software upgrade Preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

(i) Software package integrity shall be validated in the installation/upgrade stage.
(ii) Device shall support software package integrity validation via cryptographic means, e.g., digital signature. To this end, the device 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.
(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).

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

Requirement:

*(applicable to CBC only; to be tested only on CBC of Group IV)*

(a) CBC Software package integrity shall be validated in the installation /upgrade stage.
(b) CBC 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 prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only. To this end, the CBC shall have 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.
(c) Tampered software shall not be executed or installed if integrity check fails.
(d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (b) above

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

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

(i) PABX Software package integrity shall be validated in the installation and upgrade stages strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

(ii) PABX shall allow upgrades only if code signing certificate is valid and not time expired. To this end, the PABX 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) PABX's software upgrades shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

(v) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade.

[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

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

Source code of the CPE (in high level programming language) shall be free from known security vulnerabilities, the high security critical weaknesses listed in the CWE database and all the exploitable security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10. OEM may provide Software Test Document (STD) in this regard.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Vendor shall ensure the following while developing device's OS /Application Software

i. Industry standard best practices of secure coding during the entire software development life cycle of the Device Software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the Device.

ii. The Device software is free from known security vulnerabilities, security weaknesses listed in the CWE database, and all the exploitable security vulnerabilities listed in the latest SANS Top 25 and OWASP Top 10

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

Vendor shall submit Software Test Document (STD) to lab for scrutiny.

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

a) OEM shall follow the best 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 device Software which includes OEM developed code, third party software and open-source code libraries used/embedded in the device.

ii. CBC/PABX software shall be free from CWE top 25 and OWASP top10 security weaknesses on the date of offer of product to the designated TTSL for testing. For other security weaknesses, OEM shall give mitigation plan.

iii. The binaries for device and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

### 2.3.4 Known Malware Check

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The Operating System and the applications installed in the CPE shall be free from any known malware. The CPE shall support mechanism to carry out anti-malware checks. OEM to submit Software Test document (STD) to establish that the CPE is free from Known Malware.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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

### 2.3.5 Known Malware and backdoor Check

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

OEM shall submit an undertaking stating that CBC/PABX is free from all known malware and backdoors as on the date of offer of CBC/PABX to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the CBC/PABX to the designated TSTL.

### 2.3.6 No unused software

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Unused software components or parts of software which are not needed for operation or functionality of the CPE 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). OEM to provide Software Test Document (STD) in this regard.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Unused software components or parts of software which are not needed for operation or functionality of the Device shall not be installed or shall be deleted after installation. This also includes 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.

Requirement:

*(applicable to CBC only; to be tested only on CBC of Group IV)*

Software components or parts of software packages which are not needed for operation or functionality of the CBC shall not be present. Orphaned software components /packages shall not be present in CBC. OEM shall provide the list of software that are necessary for CBC's operation. In addition, OEM shall furnish an undertaking as "CBC does not contain Software that is not used in the functionality of CBC"

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

Software components or parts of software which are not needed for operation or functionality of the PABX shall not be present. Orphaned software components /packages shall not be present in PABX. OEM 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]

### 2.3.7 Unnecessary Service Removal

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The OEM to provide list of essential services and the related ports required for functioning of CPE, list of optimal services supported by CPE and their related ports. The CPE 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 and their ports shall be initially configured to be disabled on the CPE by the vendor.

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

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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. device shall not support following services

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

Any other protocols, services that are vulnerable are also to be permanently disabled. Full documentation of required protocols and services (communication matrix) of the device and their purpose needs to be provided by the OEM as prerequisite for the test case. OEM shall submit “Communication Matrix” clearly showing the services and ports used.

***Note (applicable to IP router only):*** 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.

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

### 2.3.8 Secure Time Synchronization

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The CPE shall support time synchronization feature for its core functionality or for the additional supported functionality. For CPEs that have time synchronization feature, it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP.

The CPE clock shall be synchronized with NTP server in a secure manner. The CPE client should be able to verify the authentication and authorization of the NTP Server.

OEM shall plugin well known vulnerabilities, input validation vulnerabilities related to NTP feature.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Device shall provide reliable time and date information provided manually by itself or through NTP server. Device should generate audit logs for all changes to time settings. Device should support to configure authentication between itself and external NTP server.

Requirement:
*(applicable to CBC and PABX only; to be tested any one of CBC and PABX of Group IV)*

CBC/PABX shall provide reliable time and date information provided through NTP/PTP server. CBC/PABX shall establish secure communication channel with the NTP/PTP server. CBC/PABX shall establish secure communication channel strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” with NTP/PTP server. CBC/PABX shall generate audit logs for all changes to time settings.

### 2.3.9 Self-Testing

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The CPE shall support the detection mechanism for identification of failure of underlying security mechanisms (such as software image integrity, runtime integrity, cryptographic modules etc.) used. The CPE to perform such self-tests periodically/at the time of booting, visual indication on failure is a desirable feature.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Device shall perform self-tests to identify failures in its security Mechanisms during i) power on ii) when administrator instructs. (e.g., integrity of the firmware and software as well as for the correct operation of cryptographic functions, etc.,)

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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 FIPS140-2 or Later version etc.,) to identify failures in its security mechanisms during i) power on ii) when the Administrator Instructs iii) Periodic, with period configurable and iv) at the time of restart.

### 2.3.10 Restricted reachability of services

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The CPE shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. OEM to map the essential services required to be accessed from WAN side, LAN side to limit access to services only on need / functionality basis. For Interfaces on which services are active, the reachability to be limited to legitimate communication peers. One such Use-case scenario is to restrict web-management access of CPE to only LAN ports and not to permit access on Wi-Fi, WAN side.

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of CBC, PABX and IP Router of Group IV)*

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

### 2.3.11 Restricting System Boot Source

*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX and of Group IV)*

Requirement:

The Group IV device can boot only from the memory devices intended for this purpose. The device 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.]

### 2.3.12 Avoidance of Unspecified Wireless Access

*(applicable to IP Router, CBC and PABX only; to be tested on any one of CBC, PABX and IP Router of Group IV)*

Requirement:

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

*Note (applicable for IP router only)*: IP router supporting standard wireless technologies would also need to be tested for this requirement apart from wireless technology related tests.

### 2.3.13 Feature / Service Activation Policy

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement

The CPE shall have factory default settings such that only the essential features / services and ports required for main operational needs of CPE are only enabled. Optional features, added services, futuristic service / applications are disabled by default. Such disabled services could only be enabled after successful authentication and selection by ADMIN user.

## Section 2.4: System Secure Execution Environment

### 2.4.1 No unused functions

Requirement:

*(applicable to Wi-Fi CPE and IP Router only of Group IV; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

Unused functions of the Group IV device 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 "2.3.6 No unused software" of this document, such functions shall be deactivated in the configuration of the Group IV device 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 Group IV device reboot. Example: A debugging function in software which can be used for troubleshooting shall not be activated during normal operation of the Group IV device.

OEM to provide report in this regard, List of the used functions of the Group IV device 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 IV device.

*Requirement:*
*(applicable to CBC and PABX only; to be tested only on CBC and PABX of Group IV)*

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

[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:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The Group IV device 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. OEM to provide report and declaration to this effect.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

The Group IV device 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.

*Requirement:*
*(applicable to PABX only; to be tested only on PABX of Group IV)*

OEM to ensure that the PABX shall not contain software and/or hardware components that are no longer supported by OEM or its third parties including the open-source communities, such as components that have reached end-of-life or end-of-support.

*Requirement:*
*(applicable to CBC only; to be tested only on CBC of Group IV)*

OEM to ensure that the CBC shall not contain software and hardware components that are no longer supported by OEM or its 3rd Parties including the open-source communities, such as components that have reached end-of-life or end-of-support.
An undertaking in this regard shall be given by OEM.

### 2.4.3 No Known Vulnerabilities in System on Chip (SOC) solution

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

This test is applicable for such Group IV devices which have System on Chip solutions, where majority of Group IV device functions are realized in a VLSI chip. OEM to provide self-test / third-party / Chip-vendor test report indicating that the SOC is free from malware, known-vulnerabilities.

`

## Section 2.5: User Audit

### 2.5.1 Audit trail storage and protection

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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]

Requirement:
*(applicable to CBC and PABX only; to be tested only on CBC and PABX of Group IV)*

The security event log shall be access controlled (file access rights) such that only privilege users including the administrator have access to read the log files. The only allowed operations on security event log are archiving/saving and viewing.

[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:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

CPE to have capability to log important security events. The audit logs may preferably be stored in non-volatile memory. If applicable (for cyber-cafe, Public Data Office usage scenario) provision for secure log export should exist and logs may capture unique System Reference such as website address, IP Address, MAC address, hostname, login attempts etc.

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX of Group IV)*

The Group IV device shall log all important security events with unique system reference details as given in the Table below.

Group IV 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.no | Event Types (Mandatory or optional) | Description | Event data to be logged |
|---|---|---|---|
| 1 | Incorrect login attempts (Mandatory) | Records any user incorrect login attempts to the Group IV device | • Username,<br>• Source (IP address) if remote access<br>Outcome of event (Success or failure)<br>• Timestamp |
| 2 | Administrator access (Mandatory) | Records any access attempts to accounts that have system privileges. | • Username,<br>• Timestamp,<br>• Length of session,<br>Outcome of event (Success or failure)<br>• Source (IP address) if remote access |
| 3 | Account administration (Mandatory) | Records all account administration activity, i.e. configure, delete, enable, and disable. | • Administrator username,<br>• Administered account,<br>• Activity performed (configure, delete, enable and disable)<br>Outcome of event (Success or failure)<br>• 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 | • Value exceeded,<br>• Value reached<br>(Here suitable threshold values shall be defined depending on the individual system.)<br>Outcome of event (Success or failure) |

| | | | |
|---|---|---|---|
| | | defined thresholds. | • Timestamp |
| 5 | Configuration change (Mandatory) | Changes to configuration of the Group IV device | • Change made<br>* Timestamp<br>Outcome of event (Success or failure)<br>• Username |
| 6 | Reboot/shutdown/crash (Mandatory) | This event records any action on the Group IV device that forces a reboot or shutdown OR where the Group IV device has crashed | • Action performed (reboot, shutdown, etc.)<br>• Username (for intentional actions)<br>Outcome of event (Success or failure)<br>• Timestamp |
| 7 | Interface status change (Mandatory) | Change to the status of interfaces on the Group IV device (e.g. shutdown) | • Interface name and type<br>• Status (shutdown, missing link, etc.)<br>Outcome of event (Success or failure)<br>• Timestamp |
| 8 | Change of group membership or accounts (Optional) | Any change of group membership for accounts | • Administrator username,<br>• Administered account,<br>• Activity performed (group added or removed)<br>Outcome of event (Success or failure)<br>• Timestamp. |
| 10 | Resetting Passwords (Optional) | Resetting of user account passwords by the Administrator | • Administrator username,<br>• Administered account,<br>• Activity performed (configure, delete, enable and disable)<br>Outcome of event (Success or failure)<br>• Timestamp |
| 11 | Services (Optional) | Starting and Stopping of Services (if applicable) | Service identity<br>Activity performed (start, stop, etc.)<br>Timestamp<br>Outcome of event (Success or failure) |
| 12 | User login (Mandatory) | All use of identification and authentication mechanism | user identity<br>origin of attempt (e.g. IP address)<br>Timestamp<br>outcome of event (Success or failure) |
| 13 | X.509 Certificate | Unsuccessful | Timestamp |

| | | | |
|---|---|---|---|
| | Validation (Optional) | attempt to validate a certificate | Reason for failure |
| | | | Subject identity |
| | | | Type of event |
| 14 | 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 |
| 15 | 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 |
| 16 | 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 interactive session | user identity (wherever applicable) |
| | | | Timestamp |
| | | | Outcome of event (Success or failure) |
| | | | Subject identity |
| | | | Activity performed |
| | | | Type of event |
| 17 | Trusted Communication paths (with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorized remote administrators)<br>( 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) |
| 18 | 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 and section 4.2.3.2.5]

### 2.5.3 Secure Log Export

Requirement:
*(applicable IP Router only; to be tested only on IP Router of Group IV)*

a) The Group IV device 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 Group IV device that is logging.

   i. Group IV device shall be able to store generated audit data itself may be with limitations.

   ii. In the absence of external system, Group IV device 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.

   iii. Group IV device shall alert administrator when its log buffer reaches configured threshold limit.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

a) The Group-IV devices 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-IV devices.

   iv. Group-IV devices shall be able to store generated audit data itself, may be with limitations.

   v. Group-IV devices shall alert administrator when its security log buffer reaches configured threshold limit.

   vi. In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), Group-IV devices shall have mechanism to store audit data locally. Group-IV devices shall have sufficient memory to be allocated for storing minimum 10000 security events for this purpose. OEM to submit justification document for sufficiency of local storage requirement.

   vii. 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]

## Section 2.6: Data Protection

### 2.6.1 Cryptographic Based Secure Communication

Requirement

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The data is protected against well-known attacks related to Sniffing, Disclosure, reconnaissance etc.,

The secure communication mechanisms between the CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc., and NIST specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc.

Requirement:

*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Secure communication mechanism between the group IV device and the connected entities shall use only the industry standard and NIST recommended cryptographic protocols such as IPSEC, VPN, SSH, TLS/SSL, etc.

Also, group IV device 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.

Requirement:

*(applicable to CBC only; to be tested only on CBC of Group IV)*

CBC shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only. OEM shall submit to TSTL, the list of the connected entities with CBC and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing the communication with each entity and any other details required for verifying this requirement.

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

PABX shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)”

### 2.6.2 Cryptographic Module Security Assurance

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

An undertaking shall be provided by the vendor as below: Cryptographic module embedded inside the Group IV device (which may be in the form of hardware, software, or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality are designed and implemented in compliance with FIPS 140-2 standards for different levels of security.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

Cryptographic module embedded inside the CBC (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. 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 CBC (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 shall also submit cryptographic module testing document and the detailed self / Lab test report along with test results for scrutiny CBC shall support the minimum-security level of 2 as defined in FIPS 140-2.

Requirement:
*(applicable to PABX only; to be tested only on PABX of Group IV)*

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the PABX (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 shall submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

### 2.6.3 Cryptographic Based Secure Communication on Wi-Fi Access

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The communication security dimension on Wi-Fi access ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points). The security mechanism to protect against well-known attacks like capture-decrypting, PIN detection, Key recovery, Key reinstallation attacks.

It shall support WPA2-PSK with AES as default standard. Other encryption options stronger than WPA2 may be made available under configuration menu for user choice selection.

### 2.6.4 Cryptographic Algorithms implementation Security Assurance

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

An undertaking shall be provided by the vendor as below:
Cryptographic algorithms embedded in the crypto module of Group IV device are implemented in compliance with respective FIPS standards (for the specific crypto algorithm).

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

Cryptographic algorithm implemented inside the Crypto module of CBC shall be in compliance with the respective FIPS standards (for the specific crypto algorithm). 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 algorithm implemented inside the Crypto module of CBC is in compliance with the respective FIPS standards (for the specific crypto algorithm embedded inside the CBC)" OEM shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny

Requirement:
*(applicable to PABX only; to be tested only on PABX of Group IV)*

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithms embedded in the crypto module of PABX 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.

### 2.6.5 Cryptographic Algorithm selection for Wi-Fi Access

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

It shall support WPA2-PSK with AES-128 as default standard. Other internationally accepted encryption standards stronger like AES-192 etc., may also be made available with user choice selection. Weaker encryption options like WEP, WPS, TKIP etc., are not to be available for selection / configuration.

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

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

When CPE is not in debug (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).

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

When Group IV 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. 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 authorized privileged user.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

i. When Group IV 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 text to users and administrators.
ii. Access to maintenance mode shall be restricted only to authorized privileged user.

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

### 2.6.7 Crypto-Key Protection Mechanism

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The Group IV device to have protection mechanisms against access to keys in the Group IV device against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key etc.

### 2.6.8 Protecting data and information in storage

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

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.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

For sensitive data in (persistent or temporary) storage read access rights shall be restricted. Files of 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.

Requirement:
*(applicable to PABX only; to be tested only on PABX of Group IV)*

For Sensitive data in storage (persistent or temporary), read access rights shall be restricted. Files of PABX 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 the 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)".

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.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted.
b) Sensitive files of CBC system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.

c) 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 latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.
   iii. Stored files in the CBC: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "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 4.2.3.2.3]

### 2.6.9 Protection against Copy of Data

Requirement:
*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

Group IV device shall have protection against creating a copy of data in use / data in transit. Protective measures should exit against use of available system functions / software residing in Group IV device to create copy of data for illegal transmission. The software functions, components in the Group IV device for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

i. Without authentication, CBC shall not create a copy of data in use or data in transit.
ii. Protective measures should exist against use of available system functions /

software residing in CBC to create copy of data for illegal transmission.

iii. The software functions, components in the CBC for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

### 2.6.10 Protection against Data Exfiltration - Overt Channel

Requirement:
*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

Group IV 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 FTP, HTTP, HTTPS IM, P2P, Email etc. are to be forbidden if they are initiated by / originate from the Group IV device. Outbound-use of such services are to be disabled in the Group IV device, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

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

b) 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 CBC. Session logs shall be generated for establishment of any session initiated by either user or CBC.

### 2.6.11 Protection against Data Exfiltration - Covert Channel

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Group IV 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 initiated by / originate from the Group IV device. Outbound-use of such services are to be disabled in the Group IV device, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

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

b) 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 CBC.

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

## Section 2.7: Network Services

### 2.7.1 Traffic Filtering - Network Level

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The CPE shall provide a mechanism to filter incoming IP packets on any IP interface. It is preferable to configure Access Control List (ACL) as default deny-all on WAN port, with feature to enable the types of traffic permitted on user selection.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

The Group IV device shall provide a mechanism to filter incoming IP packets on any IP interface. In particular the Device 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 Group IV device 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

*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and*

*PABX of Group IV)*

Requirement:

The device shall support physical or logical separation of O&M and control plane traffic. See RFC 3871 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

*(applicable to IP Router and CBC only; to be tested on any one of IP Router and CBC of Group IV)*

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 2.8: Attack Prevention Mechanism

### 2.8.1 Excessive Overload Protection

Requirement:

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The Group IV device may provide security measures to deal with overload situations which may occur during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Requirement:

*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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 devices' Overload 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.

Requirement:

*(applicable to PABX only; to be tested only on PABX of Group IV)*

PABX shall act in a predictable way if an overload situation cannot be prevented. PABX 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 PABX 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.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

CBC shall act in a predictable way if an overload situation cannot be prevented. CBC 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 CBC cannot reach an undefined and thus potentially insecure, state. In an extreme case, CBC shall continue to work in degraded mode with less traffic handling capacity but without loss of system security functions.

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

### 2.8.2 **Filtering IP Options**

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

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. OEMs may refer to standards such as RFC 6192, RFC 7126.

Requirement:

*(applicable to IP Router and CBC only; to be tested on any one of IP Router and CBC of Group IV)*

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]

### 2.8.3 Network Level and application-level DDoS

*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX of Group IV)*

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:

i. Restricting of available RAM per application
ii. Restricting of maximum sessions for a Web application
iii. Defining the maximum size of a dataset
iv. Restricting CPU resources per process
v. Prioritizing processes
vi. Limiting of amount or size of transactions of a user or from an IP address in a specific time range

*Note (applicable to IP router only):* Device 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]

## Section 2.9 Vulnerability Testing Requirements

### 2.9.1 Fuzzing - Network and Application Level

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The protocols supported by the CPE shall be robust when receiving unexpected or malformed inputs. This requirement shall be applicable for both network level as well as application-level protocols supported by the equipment.

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of the IP Router, CBC and PABX of Group IV)*

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 Device.

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

### 2.9.2 Port Scanning

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

It shall be ensured that on all network interfaces, only vendor documented/identified ports on the transport layer respond to requests from outside the system. List of the identified open ports shall match the list of network services that are necessary for the operation of the CPE.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

[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 Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

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 IV device, 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. OEM to provide self-test report establishing that no publicly known vulnerability exists.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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 Device, 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.

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

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

Requirement:
*(applicable to PABX only; to be tested only on PABX of Group IV)*

It shall be ensured that no known vulnerabilities (as on date of offer of PABX to designated TSTL for testing) shall exist in the PABX.

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.4.3]

### 2.9.4 SSID Scanning

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Requirement:

The CPE shall not disclose sensitive information, PIN details on SSID scan / attack techniques. It needs to provide disguised feedback to users on unsuccessful attempts without revealing of reason for failures. Option to hide / unhide SSID on user selection is an essential feature.

## Section 2.10: Operating System

### 2.10.1 Handling of ICMP

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the CPE. In particular, there are certain types of ICMP4 and ICMPv6 that are not used in most networks, but represent a risk. Refer standards such as RFC 6192, RFC 7279, RFC 4890.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the Group IV device. 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 Group IV device 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 (IPv4 | 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 | Neighbor Solicitation | Permitted | Permitted |
| N/A | 136 | Neighbor Advertisement | Permitted | N/A |

The Group IV 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 |

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

Processing of ICMPv4 and ICMPv6 packets which are not required for PABX operation shall be shall be blocked by defining the appropriate filtering rule on the PABX.

Group IV device shall not send certain ICMPv4 and ICMPv6 packets 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 | 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 | Neighbor Solicitation | Permitted | Permitted |
| N/A | 136 | Neighbor Advertisement | Permitted | N/A |

Group IV 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 | Group IV device Solicitation | N/A | Not Permitted | Not Permitted |
| N/A | 134 | Group IV device 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]

### 2.10.2 Growing Content Handling

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

a) Growing or dynamic content shall not influence system functions.
b) A file system that reaches its maximum capacity shall lead to an event getting logged with appropriate message parameters and shall not stop Group IV 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]

### 2.10.3 Authenticated Privilege Escalation only

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

There shall not be a privilege escalation method in interactive sessions (CLI or GUI) which allows a lower privileged / guest user to gain administrator/root privileges from another user account without re-authentication or thru exploitation of authentication bypass vulnerabilities.

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of the IP routers, CBC and PABX of Group IV)*

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]

### 2.10.4 System account identification

Requirement:

*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

Each system account in Operating system of the device shall have a unique identification, the OEM to provide information on implementation mechanism for this requirement.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Each system account in CBC/PABX 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 Kernel Security

Requirement:
*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

OEM may 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 Group IV device are deactivated. OEM to provide information on steps taken in this regard.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in CBC/PABX. Kernel based network functions not needed for the operation of the CBC/PABX 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 Protection from buffer overflows

*(applicable to Wi-Fi CPE, CBC and PABX only; to be tested on any one of Wi-Fi CPE, CBC and PABX of Group IV)*

Requirement:

The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and 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]

### 2.10.7 External file system mount restrictions

Requirement:
*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

### 2.10.8 No automatic launch of removable media

Requirement:
*(applicable to IP router only; to be tested only on IP router of Group IV)*

The Group IV device 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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.3.1.3]

### 2.10.9 File-system Authorization privileges

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Requirement:

Group IV 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

*(applicable to CBC only; to be tested only on CBC of Group IV)*

Requirement:

Scheduled tasks for carrying out the activities such as taking the backups, monitoring disk space and system maintenance activities shall be executed by the privileged user such as administrator only. Similarly, CBC shall have feature to restrict Scripts / Batch processes / Macros usage among various users. It shall be possible to administratively configure scheduled tasks usage i.e. Cron-Job usage (permit / deny) among various users like Normal users, privileged users.

### 2.10.11 Restrictions on Soft-Restart

*(applicable to CBC only; to be tested only on CBC of Group IV)*

Requirement:

CBC 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 2.11: Web Interface

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

### 2.11.1 HTTPS Support

Requirement:

*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The communication between Web client and Web server to be protected using industry standard secured communication protocols TLS/HTTPS. Cipher suites with NULL encryption shall not be supported. CPE to be protected against sniffing and side jacking attacks.

Requirement:

*(applicable to IP router only; to be tested only on IP router of Group IV)*

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.

Requirement:

*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

The communication between web client and web server shall be protected strictly using 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 4.2.5.1]

### 2.11.2 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]

### 2.11.3 HTTP User sessions

*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

Requirement:

To protect user sessions the Group IV device shall support the following session ID and session cookie:

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 2.2.5 Inactive Session Timeout), the Group IV device shall automatically terminate 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 IDs 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 Group IV device 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 'Http Only' 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 cookie can only be sent to the specified directory or sub-directory.
xi. The Group IV device shall not accept session identifiers from GET/POST variables.
xii. The Group IV device shall be configured to only accept server generate session IDs.

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

### 2.11.4 HTTP input validation

Requirement:

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

### 2.11.5 No unused HTTP methods

Requirement:
*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

HTTPS methods that are not required for Group IV 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. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

### 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 (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]

### 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 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]

### 2.11.11 No Directory Listing

Requirement:

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

[Reference: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.3.4.10]

### 2.11.12 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]

### 2.11.13 Web Server Information in Error Page

Requirement:

*(applicable to Wi-Fi CPE and IP router only; to be tested on any one of Wi-Fi CPE and IP router of Group IV)*

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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

User-defined error pages shall not include version information and other internal information about the Group IV device web server and the modules/add-ons used. Default error pages of the Group IV 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]

### 2.11.14 No system privileges

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

No 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]

### 2.11.15 Access rights for web server configuration

*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX of Group IV)*

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]

### 2.11.16 Minimized file type mappings

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

File type- or script-mappings that are not required shall be deleted, e.g. php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

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

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

### 2.11.17 Restricted file access

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX of Group IV)*

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]

### 2.11.18 Execute rights exclusive for CGI/Scripting directory

Requirement:
*(applicable to IP Router, CBC and PABX only; to be tested on any one of IP Router, CBC and PABX of Group IV)*

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 2.12: Other Security Requirement

### 2.12.1 Remote Diagnostic Procedure - Verification

Requirement:

If the Group IV 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 Password Recovery

Requirement:

Group IV device have a function that resets the current system password. In the event of system password reset, the entire configuration of the Group IV device shall be irretrievably deleted. No provision shall exist for system/root password recovery.

### 2.12.3 Secure System Software Revocation

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

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

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*

Once the CBC 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. CBC shall support a well-established control mechanism for rolling back to previous software image.

Requirement:
*(applicable to PABX only; to be tested only on PABX of Group IV)*

Once the PABX 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. PABX shall support a well-established control mechanism for rolling back to previous software image. Whosoever is performing roll-back, the privilege rights, all the activities, commands, etc should be logged in.

### 2.12.4 Software Integrity Check - Installation

Requirement:
*(applicable to Wi-Fi CPE and IP router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

Group IV device should validate the software package integrity before the installation/ upgrade. Tampered software shall not be executed or installed if integrity check fails.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Group IV 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 “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only. Tampered software shall not be executed or installed if integrity check fails.

### 2.12.5 Software Integrity Check - Boot

Requirement:
*(applicable to Wi-Fi CPE only; to be tested only on Wi-Fi CPE of Group IV)*

The CPE shall verify the integrity of a software component at the time of boot / re-boot typically by comparing the result of a measurement (typically a cryptographic hash / CRC) of the component to the expected reference value.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

The Group IV device shall verify the integrity of a software component typically by comparing the result of a measurement (typically a cryptographic hash/CRC) of the component to the expected reference value. The Group IV 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.

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

The Group IV 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.

### 2.12.6 Unused Physical Interfaces Disabling

Requirement:
*(applicable to Wi-Fi CPE, CBC and PABX only; to be tested on any one of Wi-Fi CPE, CBC and*

*PABX of Group IV)*

The Group IV device shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces (including LAN ports) which are not under use shall be disabled by configuration so that they remain inactive even in the event of a reboot.

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

The device shall support the mechanism to verify all the physically accessible interfaces. Physically accessible Interfaces which are not under use shall be disabled by configuration that they remain inactive even in the event of a reboot.

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

### 2.12.7 No Default Profile

Requirement:
*(applicable to Wi-Fi CPE and IP Router only; to be tested on any one of Wi-Fi CPE and IP Router of Group IV)*

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

Requirement:
*(applicable to CBC and PABX only; to be tested on any one of CBC and PABX of Group IV)*

Predefined or default user accounts in CBC/PABX shall be deleted or disabled. No pre-defined user accounts other than Admin / Root user account would be available.

### 2.12.8 Security Algorithm Modification

Requirement:
*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

When Group IV device is establishing session/ communication channel with other Group IV device or while communication in the progress, Group IV device shall have protection against a downgrade attack/bidding down attack for the use of a weaker algorithm.

Requirement:
*(applicable to PABX only; to be tested only on PABX of Group IV)*

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

Requirement:
*(applicable to CBC only; to be tested only on CBC of Group IV)*
It shall not be possible to downgrade security algorithms/protocols supported by CBC to those not listed in Table 1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0"

### 2.12.9 Management Interface Isolation

*(applicable to PABX only; to be tested only on PABX of Group IV)*

Requirement:

Group IV device shall support management software usage/critical command execution only through a dedicated management interface.

### 2.12.10 External Alert Generation

*(applicable to PABX only; to be tested only on PABX of Group IV)*

Requirement:

PABX shall support configuring the thresholds for system parameter values such as memory, hard disk space, CPU load and it shall generate an external alert when these system parameter values exceed their defined thresholds.

### 2.12.11 Secure VPN connection

*(applicable to PABX only; to be tested only on PABX of Group IV)*

Requirement

PABX shall establish VPN connections with its peers strictly using the secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

### 2.12.12 Control Plane Traffic Protection

*(applicable to IP Router only; to be tested only on IP Router of Group IV)*

Requirement

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

# Annexure I

## Acronyms

| | |
|---|---|
| AAA | Authentication, Authorization, And Accounting |
| ACL | Access Control List |
| ACS | Auto-Configuration Servers |
| AES | Advanced Encryption Standard |
| BGP | Border Gateway Protocol |
| CERT | Computer Emergency Response Teams |
| CVE | Common Vulnerabilities and Exposures |
| CWE | Common Weakness Enumeration |
| DDOS | Distributed Denial of Service |
| DoS | Denial of Service |
| EME | Element Management System |
| FIPS | Federal Information Processing Standards |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| ICMP | Internet Control Message Protocol |
| IPSec VPN | Internet Protocol Security Virtual Private Network |
| MAC | Message Authentication Code |
| MD5 | Message Digest Algorithm |
| 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 |
| 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 | Transport Layer Security |
| TSF | Toe Security Functionality |
| URPF | Unicast Reverse Path Forwarding |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |

# Annexure-II

## List of Submissions

List of undertakings to be furnished by the OEM for Group IV device Security testing submissions.

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and Backdoor Check (against test case 2.3.5)
3. No unused software (against test case 2.3.6)
4. Avoidance of Unspecified Wireless Access (against test case 2.3.12)
5. No unsupported Components (against test case 2.4.2)
6. Cryptographic Module Security Assurance (against test case 2.6.2)
7. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.4)
8. OS-Hardening Kernel Security (against test case 2.10.5)

# Annexure-III

## References

1. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.