Indian Telecom Security Assurance Requirements (ITSAR)

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

Wi-Fi CPEs

Draft for Comments

ITSAR Number: ITSAR40212YYMM
ITSAR Name: NCCS/ITSAR/Customer Premises Equipment/Data Wi-Fi CPEs/Wi-Fi CPEs

Date of Release: DD.MM.YYYY
Date of Enforcement:

Version: 2.0.0

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. 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.	Wi-Fi CPEs	ITSAR402121811	1.0.0	12.11.2018	First release
2.	Wi-Fi CPEs	ITSAR402122401	1.0.1	03.01.2024	EditorialChanges
3.	Wi-Fi CPEs	ITSAR40212YYMM	2.0.0	DD.MM.2024	Second release

Table of Contents

A) Outline

This Indian Telecom Security Assurance Requirement (ITSAR) document specifies security requirements for Wi-Fi Customer Premises Equipment (Wi-Fi CPE). The Wi-Fi CPEs are the equipment that are used or deployed at customer premises in telecom networks for providing internet connectivity to end users.

The security requirements are drawn from national, international standards and best security practices for telecom networks. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 is the reference document on which the ITSAR is modelled. The security requirements are grouped into 12 sections based on the sub-areas, the Wi-Fi CPE devices seeking certification have to meet the security requirements mentioned in this document.

B) Scope

The types of devices for which ITSAR is applicable are Wi-Fi Routers, Wi-Fi Modems, Broadband Modems with Wi-Fi facility, Cable Modems with Wi-Fi facility, ONTs with Wi-Fi facility, Wi-Fi Data cards which provide Wi-Fi facility with backend 2G / 3G / 4G /5G connectivity, Access Points (with or without controllers), Controllers (monolithic or cloud hosted), Cloud Managed Access Points or Controllers etc. All the clauses by default are applicable to all types of Wi-Fi CPEs unless specified otherwise in the clause.

C) Conventions

i.

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 ignoredunder justifiable circumstances but after careful examination of its implications.
4. Should not or not Recommended denotes the opposite meaning of (3) above.

Chapter 1: Overview

1.1 Introduction

The Wi-Fi CPE products have been going through an evolution during the past decade to cater the need of different market segments (home, enterprise, ISP/TSP), to reduce the CAPEX/OPEX utilizing the newer technologies (virtualization/cloud computing), to add new radio technologies (Wi-Fi 6, Wi-Fi 7), to enhance security (OWE, WPA3) etc. Apparently, these advancements resulted in various types of Wi-Fi products ranging from home Wi-Fi Routers, stand-alone Access Points with/without mesh capabilities (meant for Home and small enterprises), Access Points with a controller (with/without redundancy), Cloud Managed Access Points, Cloud Managed Controllers etc.

1.2 Types of Wi-Fi CPE

Most of the Wi-Fi CPE implementations are driven by customer requirements and cost/ease of implementation, rather than following a standard architecture. From security point of view, we can classify the Wi-Fi CPE implementations as explained below:

i. **Integrated Wi-Fi CPE (Integrated Access Point), Popularly known as Wi-Fi Router:** These products are typically used by home/small office users for basic and small-scale Wi-Fi connectivity. Such products generally have one or more Wi-Fi band and LAN port(s) support, WAN port for ISP connectivity, Web Based administrator/user interface for basic configuration, DHCP servers, bridging and basic routing capabilities etc.

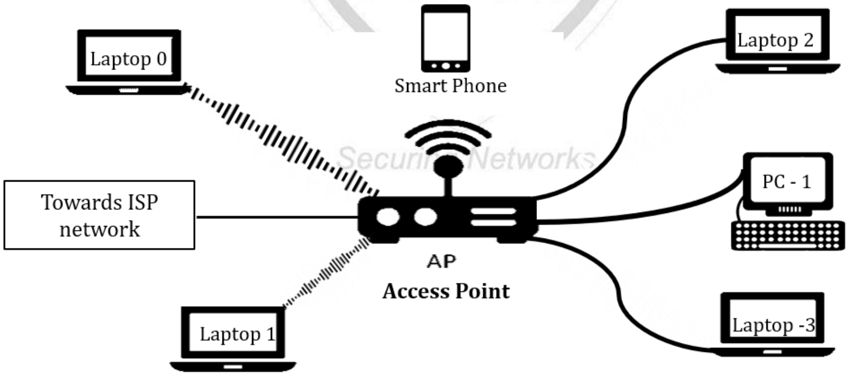

Fig 1: Integrated Access Point.

ii. **Integrated APs in Mesh**: The Mesh capable APs are mostly similar to integrated APs except for its capability to work as a gateway for other APs in the network. All the gateway and end point APs (APs which connect to Wi-Fi users) will together form a cluster. The gateway AP will get connected to the WAN or ISP network whereas the Wi-Fi users will get connected to the end point APs or gateway APs.

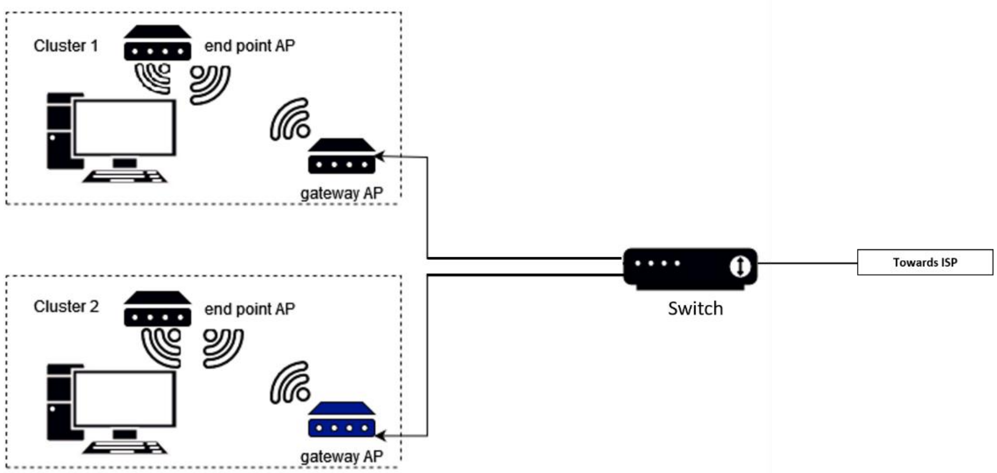

Fig 2: Integrated APs in a mesh

iii. **APs with Controllers:** These types of Wi-Fi devices are generally deployed by enterprises, campus, or ISPs. The control plane and management plane activities are handled by the controller and data plane (user plane) will be taken care by the AP itself. Optionally data plane traffic can be sent to the controller where it can be forwarded to enterprise or ISP network. APs and Controllers will use secure tunnelling such as Generic Routing Encapsulation (GRE) for packet transfer. Typically used control plane protocols include CAPWAP, LWAPP, PAPI etc. Controllers will generally be capable of doing AAA activities using internal/external servers. Controllers may support redundancy among themselves (Controller Cluster), and automatic provisioning of APs as per predefined policies. They can be implemented as a dedicated hardware or CNF (container Network function)/VNF (Virtual Network Function).

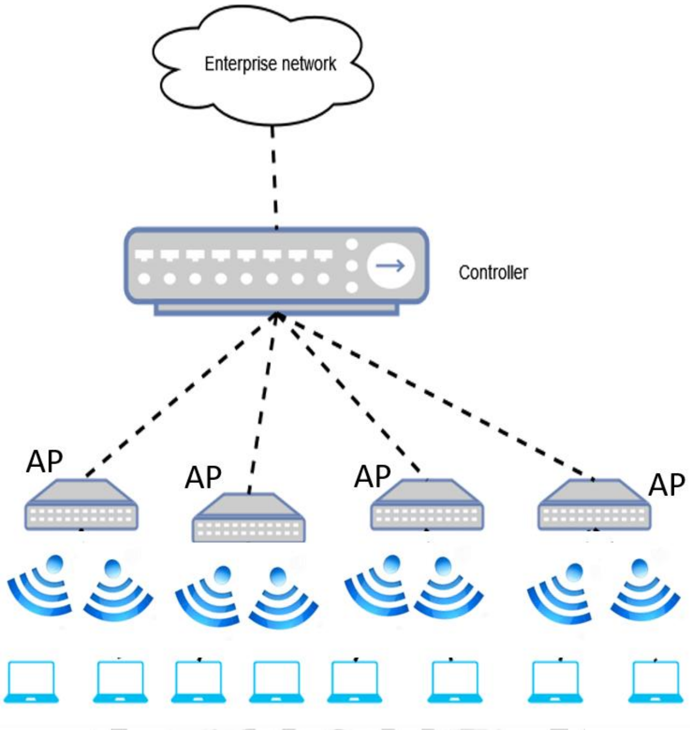

Fig 3: APs with controllers

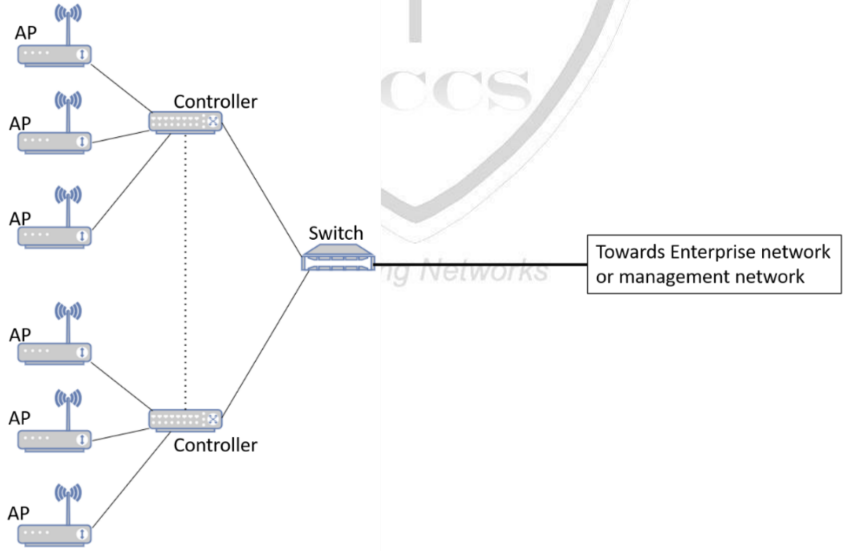

Fig 4: Controllers with redundancy

Cloud Managed Wi-Fi CPE: These products generally manage integrated APs whose O & M Plane is separated and Control plane integrated with data plane with AP. The separated O & M plane is hosted in a public or on-premise cloud for configuration and monitoring of APs from anywhere. The cloud platform and the O & M entity can also remotely manage Controllers, based on the mode of deployments. Additionally, it is possible to separate the control plane from the AP and deploy it as a CNF/VNF at a central location.

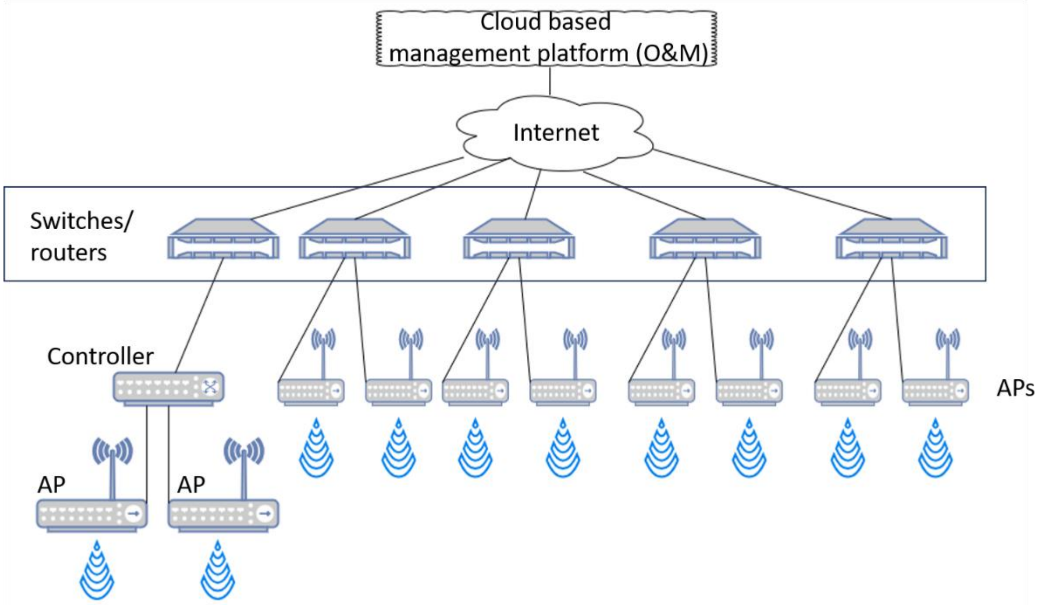

Fig 5: Cloud managed Wi-Fi CPE

Since these developments in the implementation of Wi-Fi CPEs involve additional interfaces, use of APIs, component systems hosted on cloud platforms, use of new wireless security standards etc. the security testing also will be extended to accommodate the changes.

Chapter 2: Common Security Requirements

Section 2.1: Access and Authorization

2.1.1 Authentication for Product Management and Maintenance interfaces

Requirement:

The Wi-Fi CPE shall communicate with authenticated management entities only. The protocols used for the Wi-Fi 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 Wi-Fi CPE management. (This feature shall be supported on all WAN management interfaces).

Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used for system management and maintenance.

[Ref: TEC 25848:2022 /TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.4.1]

2.1.2 Management Traffic Protection

Requirement:

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

Secure cryptographic controls prescribed in Table 1 of the latest document "Indian Telecommunication Security Assurance Requirements (ITSAR) for Cryptographic Controls" shall only be used for system management.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.2.4]

2.1.3 Role-Based access control

Requirement:

Wi-Fi 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 shall control how users are allowed access to the various domains and what types of operations.

In case of Wi-Fi CPE split into two or more devices like AP, Controller etc., the network product shall support RBAC with minimum of 3 user roles, in particular, for OAM privilege management for network product Management and Maintenance, including authorization of the operation for configuration data and software via the network product console interface. The RBAC provision shall also be extended for Wi-Fi end users (for user-based access restriction) and API users (for different privilege levels), as applicable.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.6.2]

2.1.4 User Authentication - Local/Remote

Requirement:

The various user and machine accounts on the Wi-Fi CPE 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

a) Cryptographic keys
b) Token
c) Passwords

This means that authentication based on a parameter that can be spoofed (e.g., phone numbers, public IP addresses or Virtual Private Network (VPN) membership) 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 local access and machine accounts where at least one authentication attribute shall be supported.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.2.1]

2.1.5 Remote Management Standards

Requirement:

The remote management mechanisms for Wi-Fi CPE must 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.

2.1.6 Unambiguous identification of the user & group

Requirement:

The Wi-Fi CPE shall identify each login user unambiguously. Wi-Fi 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. The Wi-Fi CPE shall support the feature to configure user preferred USERID name in the 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 Wi-Fi CPE.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.1.2]

Section 2.2: Authentication and Attribute Management

2.2.1 Authentication Policy

Requirement:

The usage of a system function without successful authentication, on the basis of the user identity and at least two authentication attributes shall be prevented. For machine accounts and local access one authentication attribute will be sufficient. System functions comprise, for example network services (like Secure Shell (SSH), Secure File Transfer Protocol (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.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.1.1]

2.2.2 Protection against brute force and dictionary attacks

Requirement:

Wi-Fi 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.

Wi-Fi CPE to detect repeated invalid attempts to sign into an account with incorrect passwords during a short period of time and it shall implement at least one of the following, most commonly used protection measures:

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

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

Note: WPA3 also shall be part of the protection measures.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.3]

2.2.3 Enforce Strong Password

Requirement:

a. The configuration setting shall be such that Wi-Fi CPE 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 Wi-Fi CPE). 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 Wi-Fi CPE.

e. When a user is changing a password or entering a new password, Wi-Fi CPE /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.). Passwords shall not be stored in clear text in the system; passwords shall be salted and hashed.

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

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.1]

2.2.4 Inactive Session Timeout

Requirement:

Wi-Fi 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 shall be admin configurable as per requirement. When the time out occurs, the same screen must be cleared of all displayed information.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.5.2]

2.2.5 Password Change facility, 1st Installation /Factory Reset

Requirement:

Wi-Fi 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 Wi-Fi CPE shall provide a function that facilitates the user to change his password at any time. However, the Wi-Fi CPE shall not allow the previously used passwords upto a certain number (Password History).

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.3.2]

2.2.6 Protected Authentication feedback

Requirement:

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

This requirement shall be applicable for all passwords used (e.g., application-level, OS level, Wireless Access etc.). An exception to this requirement is machine accounts.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.3.4]

2.2.7 Removal of predefined or default authentication attributes

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.4.2.3]

2.2.8 Storage of Passwords in encrypted form

Requirement:

User passwords shall 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 shall not be stored in clear text. This requirement does not apply to pre-shared keys that be used in raw form, such as IKE pre-shared keys.

2.2.9 Logout function

Requirement:

The system shall have a function that allows a signed-in user to logout at any time. All processes under the logged-in user ID shall be terminated on logout. Wi-Fi CPE shall be able to continue to operate without interactive sessions.
Only for debugging purposes, processes under a logged-in user ID may be allowed to continue to run after detaching the interactive session.

[Ref [3]: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.5.1]

Section 2.3: Software Security

2.3.1 Secure Update

Requirement:

The update process shall 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 Wi-Fi CPE. (Digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only). The update mechanism shall prevent illegal software patching.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.2 Secure Upgrade

Requirement:

Wi-Fi CPE shall support authenticity and integrity check while performing software upgrade Preferably employing Digital Certificate for authenticity and hashing (example: SHA2) for integrity. (Digital signature using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only).

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.5]

2.3.3 Source Code security assurance

Requirement:

a. OEM shall follow best security practices including secure coding for software development. Source code shall be made available either at Telecom Security Testing Laboratory (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 Wi-Fi CPE software which includes OEM developed code, third party software and open-source code libraries used/embedded in the Wi-Fi CPE.
    ii. Wi-Fi CPE software shall be free from Common Weakness Enumeration (CWE) top 25, Open Worldwide Application Security Project (OWASP) top 10 security vulnerabilities and OWASP top 10 API Security vulnerabilities as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.
    iii. The binaries for Wi-Fi CPE and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in (ii) above.

[Ref: https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html]
[Ref: https://owasp.org/www-project-top-ten/]
[Ref: https://owasp.org/www-project-api-security/]

2.3.4 Known Malware Check

Requirement:

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

2.3.5 No unused software

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.3]

2.3.6 Unnecessary Service Removal

Requirement:

Wi-Fi 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 shall be initially configured to be disabled on Wi-Fi CPE by the vendor except if services are needed during deployment.

In that case those services shall be disabled according to vendor's instructions after deployment is done. Disabled protocols may still need to be enabled for other reasons by the operators, e.g., remote diagnostics.

Wi-Fi CPE shall not support following services:

a) File Transfer Protocol (FTP)
b) Trivial File Transfer Protocol (TFTP)
c) Telnet
d) rlogin, Rate Control Protocol (RCP), Remote Shell Protocol (RSH)
e) HTTP
f) Simple Network Management Protocol (SNMP) v1 and v2
g) SSHv1
h) Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Small Servers (Echo, Chargen, Discard and Daytime)
i) Finger
j) Bootstrap Protocol (BOOTP) server
k) Discovery protocols (Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP))
l) IP Identification Service (Identd)
m) Packet Assembler/Disassembler (PAD)
n) Maintenance Operations Protocol (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 Wi-Fi CPE and their purpose needs to be provided by the OEM as a prerequisite for the test case.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.1]

2.3.7 Restricting system Boot Source

Requirement:

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

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

2.3.8 Secure Time Synchronization

Requirement:

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

The Wi-Fi CPE clock shall be synchronized with NTP server in a secure manner. Wi-Fi CPE shall establish a secure communication channel strictly using Secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" with NTP server. The Wi-Fi CPE client must be able to verify the authentication and authorization of the NTP Server. The Wi-Fi CPE shall generate audit logs for all changes to time settings.

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

2.3.9 Self-Testing

Requirement:

The Wi-Fi CPE's cryptographic module shall perform power-up self-tests, periodic self-tests and conditional self- tests; to ensure that the module is functioning properly. Power-up self-tests shall be performed when the cryptographic module is powered up during System bootup/restart. Conditional self-tests shall be performed when an applicable security function or operation is invoked (i.e. security functions for which self-tests are required). If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface. The cryptographic module shall not perform any cryptographic operations while in an error state.

2.3.10 Feature / Service Activation Policy

Requirement:

The Wi-Fi CPE shall have factory default settings such that only the essential features / services and ports required for main operational needs of Wi-Fi 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:

Unused functions of the Wi-Fi CPEs' 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, such functions shall be deactivated in the configuration of the Wi-Fi CPE in permanent manner.

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 Wi-Fi CPE reboot. OEM to provide report in this regard. List of the used functions of the Wi-Fi CPE'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 Wi-Fi CPE.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.4]

2.4.2 No unsupported components

Requirement:

The Wi-Fi CPE 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.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.5]

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

Requirement:

This test is applicable for such Wi-Fi CPEs which have System on Chip solutions, where majorityof Wi-Fi CPE 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 Event Log Generation

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

Section 2.6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:

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 know attacks related to Sniffing, Disclosure, reconnaissance etc.,

The secure communication mechanisms between the Wi-Fi CPE and connected entities shall use industry standard protocols such as IPSEC, VPN, SSH, TLS/SSL, etc. with specified cryptographic algorithms with specific key sizes such as SHA, Diffie-Hellman, AES etc. The Wi-Fi CPE shall communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.

OEM shall submit to TSTL, the list of the connected entities with Wi-Fi CPE and the method of secure communication with each entity with details of interface, protocol stack implemented, configuration, detailed procedure of establishing communication with each entity and any other details required for verifying this requirement.

2.6.2 Crypto-Key Protection Mechanism

Requirement:

The Wi-Fi CPE shall have protection mechanisms against access to keys in the Wi-Fi CPE against Key disclosure, reconnaissance, re-installation attacks, nonce-resets, Zeroing blocks of key etc.

2.6.3 Protecting data and information - Confidential System Internal Data

Requirement:

When Wi-Fi 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). Access to maintenance mode shall be restricted only to authorized privileged users.

[Ref: TSDSI STD T1.33.117-17.1.0 V1.1.0. Section 4.2.3.2.2.]

2.6.4 Protecting data and information in storage

Requirement:

a) For sensitive data (persistent or temporary) in storage, read access rights shall be restricted. Sensitive files of Wi-Fi CPE that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” with appropriate non-repudiation controls.
b) 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 (e.g., user passwords) in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.
   iii. Stored files in the Wi-Fi CPE shall be protected against manipulation strictly using Secure cryptographic controls prescribed in Table 1 of the latest document “ITSAR for Cryptographic Controls” only.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.2.3]

2.6.5 Protection against Copy of Data

Requirement:

Wi-Fi CPE shall have protection against creating a copy of data in use / data in transit. Protective measures shall exist against use of available system functions / software residing in Wi-Fi CPE to create copy of data for illegal transmission. The software functions, components in the Wi-Fi CPE for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.6 Protection against Data Exfiltration - Overt Channel

Requirement:

Wi-Fi CPE 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 Wi-Fi CPE. Outbound-use of such services are to be disabled in the Wi-Fi CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels. Session logs shall be generated for establishment of any session initiated by either user or Wi-Fi CPE.

2.6.7 Protection against Data Exfiltration - Covert Channel

Requirement:

Wi-Fi CPE 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 Wi-Fi CPE. Outbound-use of such services are to be disabled in the Wi-Fi CPE, if it is essential to have some of these services for outbound-use (remote management etc.,), facility to exist for monitoring anomalous channels. Session logs shall be generated for establishment of any session initiated by either user or Wi-Fi CPE.

Section 2.7: Network Services

2.7.1Traffic Filtering - Network Level

Requirement:

Wi-Fi CPE shall provide a mechanism to filter incoming IP packets on any interface (Refer to RFC 3871) In particular the Wi-Fi CPE shall provide a mechanism:

a) To filter incoming IP packets on any IP interface at Network Layer and Transport layer of the stack ISO/Open Systems Interconnection (OSI).

b) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:
   i. Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
   ii. Accept: the matching message is accepted.
   iii. 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.

c) To enable/disable for each rule the logging for Dropped packets, i.e. details on messages matching the rule for troubleshooting.

d) To filter on the basis of the value(s) of source IP, destination IP and port addresses of the protocol header

e) To reset the accounting.

f) Wi-Fi CPE shall provide a mechanism to disable/enable each defined rule.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.6.2.1]
[Ref: RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure]

2.7.2 Traffic Separation

(applicable for both split configuration and cloud hosted/managed configuration)

The Network product shall support physical or logical separation of O&M and control plane traffic. See RFC 3871 [3] for further information.

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

2.7.3 Traffic Protection – Anti-Spoofing

Requirement:

Wi-Fi CPE 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.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.3.3.1.1]

Section 2.8: Attack Prevention Mechanism

2.8.1 Excessive Overload Protection

Requirement:

Wi-Fi CPE shall act in a predictable way if an overload situation cannot be prevented. Wi-Fi CPE shall be built in such a way that it can react to 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 a case it shall be ensured that Wi-Fi CPE 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. OEM shall provide a technical description of the Wi-Fi CPE 's overload control mechanisms. (especially whether these mechanisms rely on cooperation of other network elements)

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.3.3]

2.8.2 Network-level and Application-level DDoS

Requirement:

Wi-Fi CPE shall have protection mechanisms against Network-level and Application-level Distributed Denial of Service (DDoS) attacks. Wi-Fi CPE 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 may include:

a) Restricting available RAM per application
b) Restricting maximum sessions for a Web/Database application
c) Defining the maximum size of a dataset
d) Restricting Central Processing Unit (CPU) resources per process
e) Prioritizing processes
f) Limiting amount or size of transactions of a user or from an IP address in a specific time range
g) Limiting amount or size of transactions to an IP address/Port Address in a specific time range

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.1]

2.8.3 Filtering IP Options

Requirement:

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.

Section 2.9 Vulnerability Testing Requirements

2.9.1 Fuzzing - Network and Application Level

Requirement:

The protocols supported by the Wi-Fi 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.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.4]

2.9.2 Port Scanning

Requirement:

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 necessaryfor the operation of the Wi-Fi CPE.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.4.2]

2.9.3 Vulnerability Scanning

Requirement:

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 Network Product, both in the OS and in the applications installed, that can be detected by means of automatic testing tools via the Internet Protocol enabled network interfaces.

The vulnerabilities found during the Vulnerability Scanning/Assessment process shall be remediated as below. For other than critical vulnerabilities, OEM shall provide a remediation plan.

Sr. No.	CVSS Score	Severity	Remediation
1	9.0 - 10.0	Critical	To be patched immediately
2	7.0 - 8.9	High	To be patched within a month
3	4.0 - 6.9	Medium	To be patched within three months
4	0.1 - 3.9	Low	To be patched within a year

Zero-day vulnerabilities shall be remediated immediately or as soon as possible.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.4.3]
[Ref: https://nvd.nist.gov/vuln-metrics/cvss]
[Ref: GSMA NG 133 Cloud Infrastructure Reference Architecture]

Section 2.10: Operating System

2.10.1 Growing Content Handling

Requirement:

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 Wi-Fi CPE from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided. The countermeasures are usage of dedicated filesystems, separated from main system functions, or quotas, or at least a file system monitoring.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:

Processing of ICMP version 4 (ICMPv4) and ICMP version 6 (ICMPv6) packets which are not required for operation shall be disabled on the Wi-Fi CPE. In particular, there are certain types of ICMPv4 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. Those are marked as "Permitted" in the table below.
Wi-Fi CPE shall not send certain ICMP types by default but it may support the option to enable utilization of these types (e.g., for debugging) 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

Wi-Fi CPE shall not respond to, or process (i.e. do changes to configuration) under any circumstances certain ICMP message types as marked in the 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

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.1.2.]

2.10.3 Authenticated Privilege Escalation only

Requirement:

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

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.4.1.2.1]

2.10.4 System account identification

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.4.2.2]

2.10.5 OS-Hardening Kernel Security

Requirement:

Kernel based network functions not needed for the operation of the network element shall be deactivated.
In particular, the following ones shall be disabled by default:

a) IP Packet Forwarding between different interfaces of the network product.
b) Proxy Address Resolution Protocol (ARP) (to prevent resource exhaustion attack and man-in-the-middle attacks)
c) Directed broadcast (to prevent attacks like Smurf, Denial of Service etc.,)
d) IPv4 Multicast handling. In particular, all packets with IP source or destination address belonging to the multicast IP ranges (224.0.0.0 through 239.255.255.255) shall be discarded by default and multicast route caching and forwarding shall be disabled to prevent Smurf and Fraggle attacks. A configuration option shall be available to enable the IPv4 multicast handling if required.
e) Gratuitous ARP messages (to prevent ARP Cache Poisoning attacks)

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section - 4.3.3.1.2]

2.10.6 No automatic launch of removable media

Requirement:

The Network product 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.

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

2.10.7 Protection from buffer overflows

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.5]

2.10.8 External file system mount restrictions

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.6]

Section 2.11: Web Interface

2.11.1 HTTPS Support

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.1]

2.11.2 Logging

Requirement:

Access to the webserver (both successful as well as failed attempts) shall be logged. Theweb 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 must be included whenever possible.
- Status code of web server response

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.2]

2.11.3 HTTP input validation

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.4]

2.11.4 No unused HTTP methods

Requirement:

HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.3]

2.11.5 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.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.4]

2.11.6 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).

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.5]

2.11.7 No CGI or other Scripting for uploads

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.6]

2.11.8 No execution of system Commands with SSI

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.7]

2.11.9 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.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.9]

2.11.10 No Directory Listing

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.10]

2.11.11 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.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.11]

2.11.12 Information in Error Page

Requirement:

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

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.3.4.12]

2.11.13 Restricted file access

Requirement:

Restrictive access rights shall be assigned to all files which are directly or indirectly (e.g., via links or in virtual directories) in the web server's document directory. In particular, the web server shall not be able to access files which are not meant to be delivered.

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

2.11.14 HTTP User sessions

Requirement:

i. The session ID shall uniquely identify the user and distinguish the session from allother 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 Time out.
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 Wi-Fi CPE shall not use persistent cookies to manage sessions but only session 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 thecookie can only be sent to the specified domain.
x. Where session cookies are used the 'path' attribute shall be set to ensure that thecookie can only be sent to the specified directory or sub-directory.
xi. The Wi-Fi CPE shall not accept session identifiers from GET/POST variables.
xii. The Wi-Fi CPE shall be configured to only accept server generate session ID's.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. section 4.2.5.3]

Section 2.12: Other Security Requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:

If Wi-Fi CPE 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:

a) User id
b) Time stamp
c) Interface type
d) Event type (e.g., CRITICAL, MAJOR, MINOR)
e) Command/activity performed
f) Result type (e.g., SUCCESS, FAILURE).
g) IP Address of remote machine

[Ref: GSMA NG 133: GSM Association Non-confidential Official Document NG.133 - Cloud Infrastructure Reference Architecture managed by OpenStack section 2.2.7.7]

2.12.2 Software Integrity Check – Installation

Requirement:

Wi-Fi CPE shall validate the software package integrity before the installation / upgrade. Tampered software shall not be executed or installed if integrity check fails.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.3.5]

2.12.3 Software Integrity Check - Boot

Requirement:

The Wi-Fi 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.

2.12.4 No Default Profile

Requirement:

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.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.2.2]

Chapter 3: Specific Security Requirements

Section 3.1: Wi-Fi Access

3.1.1 SSID Scanning

Requirement:

The Wi-Fi CPE shall not disclose sensitive information, PIN details on SSID scan / attack techniques. It must 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.

3.1.2 Unused Physical and logical Interfaces Disabling

Requirement:

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

3.1.3 Avoidance of Unspecified Wireless Access

Requirement:

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

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

3.1.4 Authentication Support - External

Requirement:

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

In case of Wi-Fi CPE split into two or more devices like AP, Controller etc., the user authentication credentials shall be protected and securely communicated (between AP & External authentication server or Controller and Authentication Server as applicable) if the authentication credentials are managed by external authentication servers (AAA servers).

3.1.5 Remote Management Standards for Connected Devices, Additional Features

Requirement:

The remote management mechanisms for devices connected to Wi-Fi CPE, or for configuration ofadditional features of Wi-Fi CPE like DDNS, UPnP etc., must be compliant with the respective latest standards published at the time of commencement of security testing. These additional features shall 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.

3.1.6 Restricted reachability of services

Requirement:

The Wi-Fi 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 Wi-Fi CPE to only LAN ports and not to permit access on Wi-Fi, WAN side.

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.3.2.2]

3.1.7 Cryptographic Algorithm selection for Wi-Fi Access

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.

Additionally, WPA2 version must support PMF (Protected Management Frames). WPA2 must have built in KRACK (Key Reinstallation Attack) Mitigation. Also, all the ciphers used must be in compliance with Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)”. All types of Wi Fi CPEs shall also support WPA3 and WPA shall not be supported.

3.1.8 Cryptographic Based Secure Communication on Wi-Fi Access

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 shall be made available under configuration menu for user choice selection.

Section 3.2: Controller Related

(applicable to controller or similar entity)

3.2.1 Audit Event Generation

Requirement:

In case of Wi-Fi CPE split into two or more devices like AP, Controller etc., the controller (or a similar entity) shall store all the log data.

Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Sr. No.	**Event Types (Mandatory or Optional)**	**Description**	**Event data to be logged**
1.	Incorrect login attempts (Mandatory)	Records any user's incorrect login attempts to the Wi-Fi CPE	Username Source (IP address) if remote access Outcome of event (Success or failure) Timestamp
2.	Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username Timestamp Length of session Outcome of event (Success or failure) Source (IP address) if

			remote access
3.	Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username
			Administered account
			Activity performed (configure, delete, enable and disable)
			Outcome of event (Success or failure)
			Timestamp
4.	Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded
			Value reached
			(Here suitable threshold values shall be defined depending on the individual system.)
			Outcome of event (Success or failure)
			Timestamp
5.	Configuration change (Mandatory)	Changes to configuration of the Wi-Fi CPE	Change made
			Timestamp
			Outcome of event (Success or failure)
			Username
6.	Reboot/shutdown/ crash (Mandatory)	This event records any action on the network device/ Wi-Fi CPE that forces a reboot or shutdown OR where the network device/ Wi-Fi CPE has crashed.	Action performed (boot, reboot, shutdown, etc.)
			Username (for intentional actions)
			Outcome of event (Success or failure)
			Timestamp
7.	Interface status change (Mandatory)	Change to the status of interfaces on the Wi-Fi CPE (e.g., shutdown)	Interface name and type
			Status (shutdown, down, missing link, etc.)
			Outcome of event (Success or failure)
			Timestamp
8.	Change of group	Any change of group	Administrator

	membership or accounts (Mandatory)	membership for accounts	username Administered account Activity performed (group added or removed) Outcome of event (Success or failure) Timestamp
9.	Resetting Passwords (Mandatory)	Resetting of user account passwords by the Administrator	Administrator username Administered account Activity performed (configure, delete, enable and disable) Outcome of event (Success or failure) Timestamp
10.	Services (Mandatory)	Starting and Stopping of Services (if applicable)	Service Identity Activity performed (start, stop, etc.) Timestamp Outcome of event (Success or failure)
11.	X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp Reason for failure Subject identity Type of event
12.	Secure update (Mandatory)	Attempt to initiate manual update, initiation of update, completion of update	User identity Timestamp Outcome of event (Success or failure) Activity performed
13.	Time change (Mandatory)	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
14.	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
15.	Trusted Communication paths with IT entities such as Authentication Server, Audit Server, NTP Server, etc. and for authorized remote administrators (Optional)	Initiation, Termination and Failure of trusted Communication paths	Timestamp
			Initiator identity (as applicable)
			Target identity (as applicable)
			User identity (in case of Remote administrator access)
			Type of event
			Outcome of event (Success or failure, as applicable)
16.	Audit data changes (Mandatory)	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)
			Subject identity
			User identity
			Origin of attempt to change time (e.g., IP address)
			Details of data deleted or modified
17.	User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
			Origin of attempt (IP address)
			Outcome of event (Success or failure)
			Timestamp

[Ref: TEC 25848:2022 / TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section 4.2.3.6.1]

3.2.2 Secure Log Export Requirement:

Requirement:

a) Wi-Fi CPE shall support (near real time) forwarding of security event logging data to an external system available in redundant configuration by push or pull mechanism through diverse links.
b) Log functions should support secure uploading of log files to a central location or to a system external for the Wi-Fi CPE.
c) Wi-Fi CPE shall be able to store the generated audit data locally. The memory for this purpose shall be dimensioned to cater for the continuous storage of two days of audit data. OEM shall submit justification document for sufficiency of local storage requirement.
d) Secure Log export shall comply with the secure cryptographic controls prescribed in Table 1 of the latest document "ITSAR for Cryptographic Controls" only.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.6.2]

3.2.3 Remote login restrictions for privileged users

Requirement:

Direct Login to Wi-Fi CPE as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to Wi-Fi CPE 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 Wi-Fi CPE.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.3.2.6]

3.2.4 Authorization Policy

Requirement:

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

Alongside access to data, execution of applications and components shall also take place with rights that are as low as possible. Applications should not be executed with administrator or system rights.

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 Section 4.2.3.4.6.1]

3.2.5 Interface robustness requirements

Requirement:

Wi-Fi CPE shall be not affected in its availability or robustness by incoming packets, from other network elements, that are manipulated or differing the norm. This means that appropriate packets shall be detected as invalid and be discarded. The process shall not be affecting the performance of Wi-Fi CPE. This robustness shall be just as effective for a great mass of invalid packets as for individual or a small number of packets.

Examples of such packets are:

a) Mass-produced TCP packets with a set Synchronize (SYN) flag to produce half-open TCP connections (SYN flooding attack).
b) Packets with the same IP sender address and IP recipient address (Land attack).
c) Mass-produced ICMP packets with the broadcast address of a network as target address (Smurf attack).
d) Fragmented IP packets with overlapping offset fields (Teardrop attack).
e) ICMP packets that are larger than the maximum permitted size (65,535 Bytes) of IP version 4 (IPv4) packets (Ping-of-death attack).
f) Uncorrelated reply packets (i.e. packets which cannot be correlated to any request).

[Ref: TSDSI STD T1.3GPP 33.117 17.2.0 V1.2.0 section 4.2.6.2.2]

Section 3.3: API Related

(applicable if APIs are supported by the Wi-Fi CPE)

3.3.1 Cryptographic Based Secure Communication for API transactions

Requirement:

If APIs are supported then the communication between API Server & Client shall be protected strictly using the Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)” only.

3.3.2 Avoidance of OWASP Top 10 API Security Risks

Requirement:

If APIs are supported, Wi-Fi CPE shall be free from OWASP top 10 API Security risks as on the date of latest release of product or three months prior to the date of offer of product for testing, whichever is latest. For security weaknesses, vulnerabilities identified or discovered during the interim period, OEM shall give mitigation plan.

3.3.3 The client and authorization servers shall mutually authenticate

Requirement:

APIs shall only allow themselves to be accessed by authorized users. One solution for authorizing access is the use of OAuth2.0 with access token. The client shall authenticate the resource server and vice versa. Mutual authentication is done by the transport layer protection and is required.

[Ref: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T23, BP-P1]

3.3.4 Authentication of the Request Originator

Requirement:

Before accepting the token as valid, the resource server shall authenticate the originator of the request as the legitimate owner of the token. The token is bound to the subject through the subject Identifier, which ensures that the token has been provided for this consumer.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.5 Requirements for client credentials

Requirement:

a) The client credentials shall be stored in a secure and tamper-resistant location or stored encrypted with the key protected in a tamper-resistant location.
b) The client credentials shall not be included in the source code and software packages.
c) The client credentials shall be installed in the client in a secure way, eliminating any possibility of gaining access to these credentials during installation.
d) The client credentials shall be possible for the authorization server to revoke the client credentials.

[Ref: 1) ETSI GS NFV-SEC 022 V2.7.1 Section 4.3 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T23]

3.3.6 Access Token shall be signed

Requirement:

The access token shall be signed to detect manipulation of the token or production of fake tokens. Access tokens shall be secured with digital signatures or Message Authentication Codes (MAC) based on JSON Web Signature (JWS). It shall be possible to encrypt the content of the access token.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.7 Format of Access Token

Requirement:

The access token shall be defined in a standard format (SAML or JWT).

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.8 Access tokens shall have limited lifetimes

Requirement:

The access token shall include a claim for the expiration time (expiration).

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.9 Access tokens shall be restricted to a particular number of operations

Requirement:

There shall be a restriction on the number of operations that an access token can perform in order to mitigate the replay attack by a malicious client.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.10 Access token shall be bound to the intended resource server

(applicable for cloud hosted/managed configuration)

Requirement:

The access token shall include a claim for the NF Instance Id of the Service Producer (audience). By using token binding, a client can enforce the use of a specified external authentication mechanism with the token.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.11 Tokens shall be bound to the client ID

Requirement:

The access token shall include a claim for the NF Instance Id of the Service Consumer (subject) which is the "Client ID."

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

3.3.12 Token Revocation

Requirement:

Token Revocation shall be possible. Unbound tokens shall not be used under any circumstance. The authorization server shall provide a mechanism for token revocation. If not, the lifetime of the Access token shall be kept very short, or the access token shall be single use. If a scheme to bind access tokens to the underlying transport layer relies on non- standard extensions, and those extensions are not available, the system shall fail securely, preventing a bid-down attack.

[Ref: ETSI GS NFV-SEC 022 V2.7.1 Section 4.3]

Section 3.4: VNF/CNF Related

(Applicable only for Wi-Fi CPE or any of its components implemented as Virtual Network Function (VNF)/Container Network Function (CNF)):

3.4.1 VNF/CNF network security profile

Requirement:

a) Each VNF/CNF supporting VNFC functions shall have a predefined network security profile describing its requirements for vNICs, ports, port group, VLANs and the requirement for internal VXLAN connections.
b) The security profile shall also define the vNIC firewall rules related to protocols (port numbers) that need to be supported on each VLAN or VXLAN connection.

There shall never be a requirement for all ports to be open, particularly on external standard-based interfaces (e.g. GTP).

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.4.2 Protection from buffer overflows

Requirement:

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

[Ref: TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0. Section - 4.3.3.1.5]

3.4.3 Data at rest storage

Requirement:

All user related data removed from the data at rest and the storage shall be cleaned.

Note: Cleaned here means overwrite storage by using organizationally approved software and perform verification on the overwritten data. The Clear pattern shall be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

[Ref: NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-at-rest]

3.4.4 VNF/CNF Startup

Requirement:

VNF/CNF startup shall include a secure boot process.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

3.4.5 Trusted Time Source

Requirement:

The VNF/CNF shall synchronize with trusted time source.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Ref: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.20]

3.4.6 VNF/CNF integration with authentication and authorization services

Requirement:

The VNF/CNF shall integrate with the organization's authentication and authorization services, e.g., IDAM (Identity Access Management). Limiting the number of repeated failed login attempts (configurable) reduces the risk of unauthorized access via password guessing (Bruce force attack). The restriction on the number of consecutive failed login attempts ("lockout_failure_attempts") and any actions post such access attempts (such as locking the account where the "lockout duration" is left unspecified) shall abide by the organization's policies.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfilment of this clause.

[Ref: 1) ONAP - VNF API security requirements, October 2022 2) GSMA NG.133 Cloud Infrastructure Reference Architecture v 1.0 section: 6.3.2.2]

3.4.7 VNF/CNF Host Spanning

Requirement:

a) All control plane data in transit between hosts shall be sent over an encrypted and authenticated channel using the protocols as prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)."
b) User plane traffic between hosts shall be protected.
c) The system shall prevent and detect unauthorized VNF/CNF host spanning.

[Ref: 3GPP TR 33.848-0.11.0 Section 5.15]

3.4.8 Input validation

Requirement:

The VNF/CNF must implement the following input validation controls:

a) Size (length) of all input shall be checked.

b) Large-size input that can cause the VNF/CNF to fail shall not be allowed. If the input is a file, the VNF /CNF API must enforce a size limit.
c) Input that contains content or characters inappropriate to the input expected by the design shall not be permitted. Inappropriate input, such as SQL expressions shall not be allowed.

[Ref: ONAP- VNF API security requirements, October 2022]

3.4.9 Key Management and security within cloned images

Requirement:

Cloned images shall not possess cryptographic key pairs utilized by their original image. Propagation of two or more images with the same key pairs immediately cancels out the notion of utilizing key pairs for the purpose of establishing identity.

[Ref: ETSI GS NFV-SEC 003 V1.1.1 Section 4.4.3.3.1]

3.4.10 Encrypting VNF/CNF volume/swap areas

Requirement:

a) The VNF/CNF volumes shall be secured by encrypting them and storing the cryptographic keys at safe locations. TPM or HSM modules must be used to securely store these keys.
b) VM or Container or container swap areas shall be encrypted.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Ref: ENISA NFV Security in 5G - Challenges and Best Practices (February 2022) BP- T14]

3.4.11 Encrypted Data Processing

Requirement:

a) Sensitive data shall only be decrypted or handled in an unencrypted format in VNFs/CNFs on trusted and well-known hosts.
b) Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.
c) It shall be possible to further restrict VNFs/CNFs on a single host depending on whether they handle decrypted sensitive data.
d) These controls shall be verified by secure hardware backed attestation of the

health and security of the host. Controls shall be verified and enforced at boot time and each time a function is migrated.

e) The system shall prevent and detect unauthorized data manipulation and leakage (e.g., modification of VNF/CNF images, instantiating parallel VM(s) on same physical CPU).

[Ref: 3GPP TR 33.848-0.11.0 Section 5.16]

3.4.12 GVNP Life Cycle Management Security

Requirement:

a) VNF shall authenticate VNFM when VNFM initiates a communication to VNF.
b) VNF shall be able to establish securely protected connection with the VNFM.
c) VNF shall check whether VNFM has been authorized when VNFM access VNF's API.
d) VNF shall log VNFM's management operations for auditing.

Note: This test case is optional when the VNF and VNFM belongs to the same VNF vendor. If the VNF and VNFM belongs to the same VNF vendor and the interface between VNF and VNFM is proprietary interface, the API level authorization is not needed

[Ref: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.1]

3.4.13 Instantiating VNF from trusted VNF image

Requirement:

A VNF shall be initiated from one or more trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the organization.

[Ref: 3GPP TS 33.818-17.1.0. Section 5.2.5.5.7.3]

3.4.14 Inter-VNF and intra-VNF Traffic Separation

Requirement:

The network used for the communication between the VNFCs of a VNF (intra-VNF traffic) and the network used for the communication between VNFs (inter-VNF traffic) shall be separated to prevent the security threats from the different networks affecting each other.

[Ref: 3GPP TS 33.818-17.1.0 Section 5.2.5.5.8.5.2]

3.4.15 Security functional requirements on virtualization resource management

Requirement:

To prevent a compromised VIM from changing the assigned virtualized resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, and the VNF shall alert the OAM when the VNF cannot detect a VNFC message.
A VNF shall log the access from the VIM.

[Ref: 1) 3GPP TS 33.818 v17.1.0 Section 5.2.5.6.7.2 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022)]

3.4.16 VNF package and VNF image integrity

Requirement:

a) VNF package and the image shall contain integrity validation value (e.g. MAC).
b) VNF package shall be integrity protected during on boarding.

[Ref: 1) 3GPP TS 33.818- 17.1.0 Section 5.2.5.5.3.3.5.1 2) ENISA NFV Security in 5G - Challenges and Best Practices (February 2022), BP-T2]

3.4.17 Proper image management of VM images must be done

Requirement:

Images shall be carefully protected against unauthorized access, modification, and replacement by both systems and human actors.

a) Small number of images must be kept.
b) Images must be kept updated to avoid known vulnerability exploits.
c) Cryptographic checksum protection must be used to detect unauthorized changes to images and snapshots.
d) Strict control around access, creation and deployment of images/instances must be implemented. Such activities must be recorded for audit purposes.

[Ref: ENISA Security Aspects of Virtualization (Feb 2017) G-07, PG 37, OS-01, OS-02]

3.4.18 Secrets in NF Container/VM Image

Requirement:

The VNF/CNF images shall not be packaged with embedded secrets such as passwords or credentials, or any other critical configuration data.

[Ref: 3GPP TR 33.848-17.1.0 V.0.11.0. Section 5.28]

Section 3.5: SDN (Software Defined Network) Related

(For SDN Capable split & cloud-based Wi-Fi CPE implementations, as applicable)

3.5.1 Mutual authentication within SDN

Requirement:

There must be mutual authentication between the controller and the switching/forwarding entities in SDN.

[Ref: ETSI GS NFV SEC 001 V1.1.1 (2014-10) clause 6.1.3.1.1]

3.5.2 Centralized Log Auditing

Requirement:

All the SDN elements shall submit security events (e.g. authentication, authorization and accounting, login attempts, administration functions and configurations etc) to a centralized platform, which shall monitor and analyses in real time the messages for possible attempts at intrusion.

Note: The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Ref: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T17]

3.5.3 Software compliance and integrity preservation

Requirement:

A software checksum (hash or signature) shall be created by the OEM/vendor during SDN Controller software compilation that can be validated with a corresponding checksum (hash or signature) created during any testing and validation process operated by the operator or a third party.

[Ref: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T10]

3.5.4 Host Security

Requirement:

SDN elements shall be hosted on secure server.

3.5.5 SDN controller and associated SDN communications

Requirement:

An SDN controller shall always communicate with its associated SDN resources using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

[Ref: ETSI GS NFV-EVE 005 Section 6.1, REC#1]

3.5.6 Prevent attacks via forwarding plane

Requirement:

There shall be mechanisms to prevent attacks mounted via the Forwarding Plane against SDN switches and controllers. OEMs shall submit the list of measures taken to prevent reconnaissance attacks, DoS and resource exhaustion attacks and vulnerability exploits.

[Ref: ETSI GS NFV-EVE 005 Section 6.2, REC#1]

3.5.7 Prevent attacks via control network

Requirement:

There shall be mechanisms to mitigate attacks from the control network. TLS shall be used to protect integrity.
There shall be High-Availability (HA) controller architecture.
The configuration of secure and authenticated administrator access to controllers shall be enabled.
Role-Based Access Control policies shall be implemented for controller administrators.

Note on c) and d): These clauses require support from TSP. The parameters/features that are required to be configured/enabled for successful testing are to be made available in the system/DUT in fulfillment of this clause.

[Ref: ETSI GS NFV-EVE 005 Section 6.2, REC#2]

3.5.8 Prevent attacks via SDN controller's Application Control Interface

Requirement:

a) There shall be mechanisms to mitigate attacks via the SDN Controller's Application Control Interface such as TLS 1.2 or higher shall be used to secure northbound communications and secure controller management.
b) The SDN systems shall be configured to validate flows in network device tables against controller policy.

[Ref: ETSI GS NFV-EVE 005 Section 6.2, REC#3]

3.5.9 Prevent attacks via virtualized environment

Requirement:

There shall be mechanisms to mitigate attacks against controllers and switches (forwarding entities) via the Virtualized environment. OEMs shall submit the list of measures taken to prevent such attacks.

[Ref: ETSI GS NFV-EVE 005 Section 6.2, REC#4]

3.5.10 Northbound Applications

Requirement:

a) Northbound applications, including the orchestrators, shall not be assigned admin level access to the controllers.
b) The identity of northbound applications shall be confirmed through certificates.

3.5.11 SDN security management

Requirement:

a) The controls below shall be applied if message bus technology for communication between SDN elements is used.
    i. A strong mechanism to authenticate the integrity of messages must be deployed between the ‘publisher’ and ‘producer’ over the message bus.
    ii. No messages shall be accepted or processed by the message broker or ‘consumer’ systems from unknown, ‘fake’ or unauthenticated users.
    iii. The communications shall be secured using TLS 1.2 and above security or certificates where supported (e.g. Kafka).
    iv. The message bus shall be monitored for any unauthenticated messages or

'fake' or default usernames and a security alarm raised for investigation.

b) The security functionality shall be deployed that identifies potential attacks on any SDN elements. Any security functionality shall provide automated alarms and the ability to change the network or element configuration to mitigate the attack.

c) A high availability architecture shall be implemented for key SDN components (e.g. SDN Controllers) to ensure operational service is maintained. The design shall include primary and secondary IP links with, where possible, diverse routing to allow for single point of network failure.

d) Any changes to network, service and virtual environments shall be restricted to the orchestrator. The SDN Controller and the VNFM/CNFM and VIM/CISM shall have additional controls applied to them to restrict such access for normal operation. Restricting the SDN Controller and the VNFM/CNFM and VIM/CISM will prevent the application of rules and changes that may break policy and rules during deployment of service templates.

e) The orchestration layer and SDN must be architected so that SDN networks and NFV environments are not operationally dependent on the orchestration layer to maintain operating services under circumstances that may render the orchestration platform unavailable.

[Ref: ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022), BP-T22]

Annexure-I

Definitions

1. **Access Point (AP):** An access point is a device that creates a wireless network and allows other devices, such as laptops, smartphones, and tablets, to connect to the internet.
2. **API:** An API is a set of definitions and protocols for building and integrating application software. In the context of Wi-Fi CPE, APIs can be used to manage and configure the Wi-Fi CPE device remotely, integrate the Wi-Fi CPE with other network devices and services and collect and analyze data from the Wi-Fi CPE.
3. **Cloud Hosted Configuration:** One or more of the Wi-Fi CPE components/ devices such as Controller, O & M Platform etc. are deployed as VNFs or CNFs.
4. **Cloud Managed Configuration:** A deployment model where Wi-Fi CPEs or its components such as APs, Controllers etc. are configured or managed from a centralized cloud hosted O & M Platform.
5. **CNF:** A CNF is a network function that is designed to be deployed in a cloud-native environment. CNFs are typically containerized and can be deployed on any cloud platform.
6. **Controller:** A controller is a device that manages multiple access points. Controllers can be used to configure and provision access points, monitor the performance of the wireless network and troubleshoot problems with the wireless network.
7. **KRACK:** KRACK is short for Key Reinstallation Attack. It is an attack that leverages a vulnerability in the Wi-Fi Protected Access 2 (WPA2) protocol, which keeps your Wi-Fi connection secure.
8. **SDN:** SDN is a network architecture that separates the control plane from the data plane. This allows for more flexible and programmable networks. In the context of Wi-Fi CPE, SDN can be used to centralize the management of multiple Wi-Fi CPE devices, automate the provisioning and configuration of Wi-Fi CPE devices, optimize the performance of the Wi-Fi network.
9. **Split Configuration:** Wi-Fi CPE split into two or more devices like Access Point (AP), Controller, (Cloud) Management Platform etc.
10. **Virtualized Network Function (VNF):** implementation of an NF that can be deployed on a Network Function Virtualization Infrastructure (NFVI)
11. **WPA2:** WPA2 is a security protocol that is used to encrypt wireless communication. WPA2 is more secure than WEP and WPA.
12. **WPA3:** WPA3 is the latest version of the Wi-Fi Protected Access security protocol. WPA3 is more secure than WPA2.

Annexure-II

Acronyms

AAA Server	Authentication, Authorization, And Accounting Server
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
CAPWAP	Control and Provisioning of Wireless Access Points
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DDoS	Distributed Denial of Service
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IPSec VPN	Internet Protocol Security Virtual Private Network
KRACK	Key Reinstallation Attacks
LWAPP	Light Weight Access Point Protocol
MD5	Message Digest Algorithm
NE	Network Element
NIST	National Institute of Standards And Technology
NMS	Network Management System
NTP	Network Time Protocol
OS	Operating System
PAPI	Process Application Programming Interface
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
TKIP	Temporal Key Integrity Protocol
TLS VPN	Transport Layer Security Virtual Private Network
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Annexure III

List of Submissions

List of Undertakings to be furnished by the OEM for Wi-Fi CPEs Security testing submissions.

1. Source Code security assurance (against test case 2.3.3)
2. Known Malware Check (against test case 2.3.4)
3. No unused software (against test case 2.3.5)
4. Avoidance of Unspecified Wireless Access (against test case 3.1.3)

Annexure IV

References

1. 3GPP TR 33.848-17.1.0 V.0.11.0
2. 3GPP TS 33.818-17.1.0.
3. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 "Catalogue of General Security Assurance Requirements".
4. TEC 25848:2022/ TSDSI STD T1.3GPP 33.117-16.7.0 V.1.0.0.
5. ETSI GS NFV SEC 001 V1.1.1 (2014-10)
6. ETSI GS NFV-SEC 022 V2.7.1
7. ETSI GS NFV-SEC 003 V1.1.1
8. ETSI GS NFV-EVE 005
9. ENISA Security Aspects of Virtualization (Feb 2017)
10. ENISA NFV Security in 5G - Challenges and Best Practices (Feb 2022)
11. NSA-CISA SECURITY GUIDANCE FOR 5G CLOUD INFRASTRUCTURES Part III: Data Protection (2021), Section-Protection of Data-at-rest
12. ONAP - VNF API security requirements, October 2022
13. GSMA NG.133 Cloud Infrastructure Reference Architecture v 1.0
14. RFC 3871 - Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure
15. https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html
16. https://owasp.org/www-project-top-ten/
17. https://owasp.org/www-project-api-security/
18. https://nvd.nist.gov/vuln-metrics/cvss