Indian Telecom Security Assurance Requirements (ITSAR)

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

# Optical Network Terminal (ONT) - PON family Broadband Equipment

**ITSAR Number:** ITSAR403012311
**ITSAR Name:** NCCS/ITSAR/Customer Premises Equipment/PON CPEs/Optical Network Terminal (ONT) – family Broadband Equipment

Date of Release: 24.11.2023 Version: 1.0.1
Date of Enforcement: 01.01.2026



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

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

## About NCCS

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

## Document History

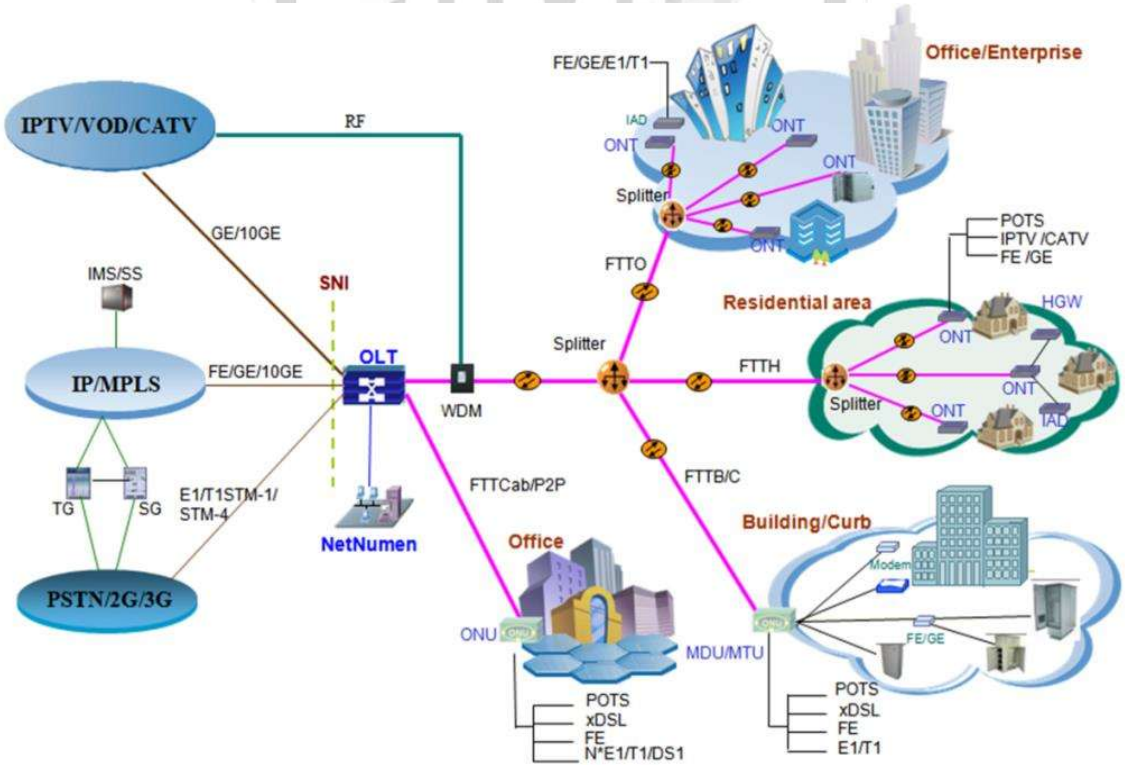
| Sr. No. | Title | ITSAR No. | Version | Date of Release | Remark |
|---|---|---|---|---|---|
| 1. | Optical Network Terminal (ONT)-PON family Broadband Equipment | ITSAR403012209 | 1.0.0 | 26.09.2022 | First release |
| 2. | Optical Network Terminal (ONT)-PON family Broadband Equipment | ITSAR403012311 | 1.0.1 | 24.11.2023 | Editorial Changes |
| | | | | | |
| | | | | | |

# Table of Contents

## Overview

This document defines the security requirements of ONT/ONU, which is an important logical functional entity in the PON. ONU converts optical signals transmitted via fibres to electrical signals. These electrical signals are then sent to individual subscribers. In general, there is a distance or other access network between ONU and end user's premises. Furthermore, ONU can send, aggregate, and groom different types of data coming from the customer and send it upstream to the OLT. Grooming is the process that optimizes and reorganizes the data stream so it would be delivered more efficiently. OLT supports bandwidth allocation that allows making smooth delivery of data float to the OLT, which usually arrives in bursts from the customer. ONU could be connected by various methods and cable types, like twisted-pair copper wire, coaxial cable, optical fiber, or through Wi-Fi.

End-user devices may also be referred to as the optical network terminal (ONT). Actually, ONT is the same as ONU in essence. ONT is an ITU-T term, whereas ONU is an IEEE term. Belong to different standard bodies, they both refer to the user side equipment in the PON system. But in practice, there is a little difference between ONT and ONU according to their location.



## Scope

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) standalone ONT/ONU of PON family with a dedicated hardware and dedicated software, which includes system software as well as application software.

## Conventions

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

## Section 1: Access and Authorization

### 1.1 Management Protocols Mutual Authentication

**Requirement:**

The protocols used for the ONU/ONT 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 ONU/ONT management and maintenance.

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

### 1.2 Management Traffic Protection

**Requirement:**

ONT 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 ]

### 1.3 Role-Based access control

**Requirement:**

ONU/ONT shall support Role-Based Access Control (RBAC) which provides at least three 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.

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

## 1.4 User Authentication – Local and Remote

**Requirement:**

Local and Remote access to the ONU/ONT 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 username 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.

**Local access:** The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from ONU/ONT 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]

## 1.5 Remote login restrictions for privileged users

**Requirement:**

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

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

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

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



**Requirement:**

The ONU/ONT shall identify each login user unambiguously. ONU/ONT 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 ONU/ONT.

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

## Section 2: Authentication Attribute Management

## 2.1 Authentication Policy

**Requirement:**

The usage of a system function without successful authentication on basis of the user identity and at least two authentication attributes (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 Authentication Support – External

**Requirement:**

If the ONU/ONT supports external authentication mechanism such as AAA server ( for authentication, authorisation and accounting services ), then the communication between ONU/ONT 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.

OEM/TSP shall disable permanently the supported weaker algorithm other than specified in ITSAR crypto control list document.

## 2.3 Protection against brute force and dictionary attacks

**Requirement:**

ONU/ONT 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.

ONU/ONT 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 ONU/ONT and on authentication attempts on ONU/ONT access through SSID with PSK

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

## 2.4 Enforce Strong Password

**Requirement:**

ONU/ONT shall only accept passwords that comply with the following complexity criteria:

a) Password containing a minimum length of 8 characters are only permitted by default. shorter lengths shall be rejected by the ONU/ONT.

b) Minimum password length - the default minimum value of 8 characters.

c) 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. @;!$.)

ONU/ONT shall support password field length of minimum 64 characters. This Feature to be enabled for ONU/ONT. Login-IDs as well as for the PSK key associated with SSID for Wi-Fi access.

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

## 2.5 Inactive Session Timeout

**Requirement:**

ONU/ONT shall monitor inactive sessions of administrative login users, Data users either on LAN or WiFi 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.

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

## 2.6 Password Changes

**Requirement:**

If a password is used as an authentication attribute, then the system shall offer a function that enables a user to change his password at any time. When an external centralized

system for user authentication is used it is possible to redirect or implement this function on this system.

Password change shall be enforced after initial login.

The system shall enforce password change based on password management policy.
In particular, the system shall enforce password expiry. ONU/ONT shall support a configurable period for expiry of passwords.
Previously used passwords shall not be allowed upto a certain number (password history).
The number of disallowed previously used passwords shall be:

- Configurable;
- Greater than 0;
- And its minimum value shall be 3. This means that the ONU/ONT shall store at least the three previously set passwords. The maximum number of passwords that the ONU/ONT 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.

ONU/ONT to have in-built mechanism to support this requirement.
If a central system is used for user authentication password policy, then additional assurance shall be provided that the central system enforces the same password change policies as laid down for the local system in this subclause.

And If a central system is not used for user authentication, the assurance on password changes rules shall be performed on the ONU/ONT.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.4.3.2]

## 2.7 Protected Authentication feedback



**Requirement:**

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

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

## 2.8 Removal of predefined or default authentication attributes

**Requirement:**

ONU/ONT may come with predefined (by the vendor, developer or producer) authentication attributes such as password or cryptographic keys. ONU/ONT 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

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

# Section 3: Software Security

## 3.1 Secure Update

**Requirement:**

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

## 3.2 Secure Upgrade

**Requirement:**

(i) ONU/ONT 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 "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

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



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

(iv) ONU's/ONT's software upgrades shall be carried out strictly using the secure cryptographic controls prescribed in Table1 of the latest document "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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.3.3.5 ]

## 3.3 Source code security assurance

**Requirement:**

a) Vendor should follow best security practices including secure coding for software development. Source code shall be offered to designated TSTL for source code review. It may be supported by furnishing the Software Test Document (STD).
b) Also, Vendor shall submit the undertaking as below:
   (i) Industry standard best practices of secure coding have been followed during the entire software development life cycle of the ONT/ONU software, which includes vendor developed code, third party software and open-source code libraries used/embedded in the ONT/ONU.
   (ii) The ONT/ONU software is free from CWE top 25 & OWASP top 10 security weaknesses on the date of offer of ONT/ONU to designated TSTL for testing. For other security weaknesses, OEM shall give mitigation plan.
   (iii) The binaries for ONT/ONU and upgrades/updates thereafter generated from the source code are free from all known security vulnerabilities stated in bullet (ii) above.

---

## 3.4 Known Malware and backdoor Check

**Requirement:**

Vendor shall submit an undertaking stating that ONU/ONT is free from all known malware and backdoors as on the date of offer to the TSTL for testing and shall submit Malware test document (MTD).

---

## 3.5 No unused software

**Requirement:**

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

Orphaned software components /packages shall not be present in ONT/ONU.

OEM shall provide the list of software that are necessary for its operation.

OEM shall furnish an undertaking as “ONT/ONU does not contain Software that is not used in the functionality of ONT/ONU”

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

---

## 3.6 Insecure Services/protocol Removal (changed as per Wi-Fi)

**Requirement:**

The OEM to provide list of essential services and the related ports required for functioning of ONU/ONT, list of optimal services supported by ONU/ONT and their related ports. The ONU/ONT 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 ONU/ONT 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
- PAD
- MOP

Full documentation of required protocols and services (Communication matrix) of the Network product and their purpose needs to be provided by the OEM as prerequisite for the test case.

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



## 3.7 Restricting System Boot Source

**Requirement:**

ONU/ONT shall boot only from memory devices intended for this purpose

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

## 3.8 Secure Time Synchronization

**Requirement:**

The ONU/ONT shall support time synchronization feature for its core functionality or for the additional supported functionality. For ONU/ONT 's that have time synchronization feature,

it shall support the secure time synchronization feature preferably by using Network Time Protocol NTP. The ONU/ONT clock shall be synchronized with NTP server in a secure manner. The ONU/ONT 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.

## 3.9 Restricted reachability of services

**Requirement:**

The ONU/ONT 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 ONU/ONT to only LAN ports and not to permit access on Wi-Fi, WAN side

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

## 3.10 Avoidance of Unspecified Mode of Access

**Requirement:**

An undertaking shall be given by the vendor as follows:

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

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

# Section 4: System Secure Execution Environment

## 4.1 No unused functions



**Requirement:**

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

List of the used functions of the Networks s software and hardware as given by the vendor shall match the list of used software and hardware functions that are necessary for the operation of the ONU/ONT.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.3.2.4]

## 4.2 No unsupported components

**Requirement:**

The ONU/ONT 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.

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

# Section 5: User Audit

## 5.1 Audit Event Generation

**Requirement:**

ONU/ONT 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.

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

2) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0.Section 4.2.3.2.5]

## 5.2 Secure Log Export

**Requirement:**

(I) (a) The ONT/ONU 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.

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

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

(IV) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), ONT/ONU shall have mechanism to store audit data locally. ONT/ONU shall have sufficient memory (minimum 15 MB) allocated for this purpose. vendor to submit justification document for sufficiency of local storage requirement.

(V) Secure Log export shall comply the secure cryptographic controls as prescribed in Table 1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

## Section 6: Data Protection

### 6.1 Cryptographic Based Secure Communication with connecting entities

**Requirement:**

ONU/ONT 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.

---

### 6.2 Cryptographic Module Security Assurance

**Requirement:**

An undertaking is to be submitted by the vendor mentioning that "Cryptographic module embedded inside the ONU/ONT (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."

Vendor shall submit cryptographic Module testing document and the detailed self / Lab test report along with test results for scrutiny.

---

### 6.3 Cryptographic Algorithms implementation Security Assurance

**Requirement:**

An undertaking is to be submitted by the vendor mentioning that "Cryptographic algorithms embedded in the crypto module of ONU/ONT shall be implemented in compliance with respective FIPS standards (for the specific crypto algorithm)."

Vendor shall submit cryptographic algorithm implementation testing document and the detailed self / Lab test report along with test results for scrutiny.

---

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

**Requirement:**

When ONU/ONT is in normal operational mode (i.e., not in maintenance mode PINs, Cryptographic Keys, passwords, cookies) there shall be no system function that reveals confidential system internal data in the clear to users and administrators.

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

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

## 6.5 Protecting data and information in storage

**Requirement:**

For Sensitive (eg PINs, cryptographic keys, password, cookies) data in storage (persistent or temporary), read access rights shall be restricted. Files of ONU/ONT 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)" only with appropriate non-repudiation controls.

In addition, the following rules apply for:

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

(ii) Systems that do not need access to sensitive data in the clear. Such systems shall hash this sensitive data strictly using the secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only.

(iii) Stored files: 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: 1) TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 Section 4.2.3.2.3 ;

## 6.6 Protection against Copy of Data

**Requirement:**



Without authentication, ONU/ONT shall not create a copy of data in use or data in transit.

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

## 6.7 Protection against Data Exfiltration - Overt Channel

**Requirement:**

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

Session logs shall be generated for establishment of any session initiated by either user or ONU/ONT.

## 6.8 Protection against Data Exfiltration - Covert Channel

**Requirement:**

NE shall have mechanisms to prevent data exfiltration attacks for theft of data in use / data in transit. Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the Network Product.

Session logs shall be generated for establishment of any session initiated by either user or ONU/ONT.

# Section 7: Network Services

## 7.1 Traffic Separation

**Requirement:**

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

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

## 7.2 Traffic Filtering -Network Level

**Requirement:**

ONT/ONU shall provide a mechanism to filter incoming IP packets on any IP interface

In particular the Network product shall provide a mechanism:

(i) To filter incoming IP packets on any IP interface at Network Layer and Transport Layer of the stack ISO/OSI.

(ii) To allow specified actions to be taken when a filter rule matches. In particular at least the following actions should be supported:

- Discard/Drop: the matching message is discarded; no subsequent rules are applied and no answer is sent back.
- Accept: the matching message is accepted.

- Account: the matching message is accounted for i.e. a counter for the rule is incremented. This action can be combined with the previous ones. This feature is useful to monitor traffic before its blocking.

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

(iv) To filter on the basis of the value(s) of any portion of the protocol header.

(v) To reset the accounting.

(vi) The Network product shall provide a mechanism to disable/enable each defined rule.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.6.2.1]

---

## 7.3. Traffic Protection –Anti-Spoofing

**Requirement:**

ONT shall not process IP packets if their source address is not reachable via the incoming interface. This feature can be implemented in several ways like use of IPsec, TLS , "Reverse Path Filter" (RPF).

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

# Section 8: Attack Prevention Mechanisms

## 8.1 Network Level and application level DDoS

**Requirement:**

ONU/ONT shall have protection mechanism against network level and Application level DDoS attacks.

ONU/ONT 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.

Any one or more of the following protective measures can be used, but not limited to the following.

- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes

- Limiting of amount or size of transactions of an user or from an IP address in a specific time range

- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

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

## 8.2 Excessive Overload Protection

**Requirement:**

The ONU/ONT 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.

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

# Section 9: Vulnerability Testing Requirements

## 9.1 Fuzzing – Network and Application Level

**Requirement:**

It shall be ensured that externally reachable services of ONU/ONT are reasonably robust when receiving unexpected input.

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

## 9.2 Port Scanning

**Requirement:**

It shall be ensured that on all network interfaces, 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 ONU/ONT.

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

## 9.3 Vulnerability Scanning

**Requirement:**

It shall be ensured that no known critical/ high/medium vulnerabilities (as on date of offer of ONU/ONT to designated TSTL for testing) shall exist in the ONU/ONT. For low category vulnerabilities remediation plan is to be provided.

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

# Section 10: Operating System

## 10.1 Handling of ICMP

**Requirement:**

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

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.2.]

## 10.2 Authenticated Privilege Escalation only

**Requirement:**

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.

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

## 10.3 System account identification

**Requirement:**

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

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

## 10.4 OS Hardening

**Requirement:**

Appropriate OS hardening procedures including security measures required to ensure the kernel security and miniaturization etc. shall be implemented in ONU/ONT

Kernel based network functions not needed for the operation of the ONU/ONT shall be deactivated.

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

## 10.5 No automatic launch of removable media

**Requirement:**

ONU/ONT shall not automatically launch any application when removable media device is connected.

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

## 10.6 Protection from buffer overflows

**Requirement:**

ONU/ONT shall support mechanisms for buffer overflow protection.

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

## 10.7 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 ONU/ONT 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]

## 10.8 File-system Authorization privileges

**Requirement:**

ONU/ONT shall be designed to ensure that only users that are authorized to modify files, data, directories or file systems have the necessary privileges to do so.

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

# Section 11: Web Servers

This entire section of the security requirements is applicable if the ONU/ONT supports web management interface.



## 11.1 HTTPS

**Requirement:**

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. ONU/ONT to be protected against sniffing and side jacking attacks.

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

## 11.2 Webserver logging

**Requirement:**

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

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

These logs should be exportable to external syslog server using secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)".

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

## 11.3 HTTPS input validation

**Requirement:**

The ONU/ONT shall have a mechanism in place to ensure that web application inputs are not vulnerable to command injection or cross-site scripting attacks. The ONU/ONT shall validate, filter, escape, and encode user-controllable input before it is placed in output that is used as a web page that is served to other users.

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

## 11.4 No unused HTTPS methods



**Requirement:**

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

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

## 11.5 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.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 . section 4.3.4.4]

## 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).

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

## 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 be used for uploads.

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

## 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.

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

## 11.9 Access rights for web server configuration (Not there in Wi-Fi)

**Requirement:**

Access rights for ONU/ONT webserver configuration files shall only be granted to the owner of the webserver processor to a user with system privileges.

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

## 11.10 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]

## 11.11 No directory listings

**Requirement:**

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

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

## 11.12 Web server information in HTTPS headers

**Requirement:**

The HTTPS header shall not include information on the version of the ONU/ONT webserver and the modules/add-ons used.

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

## 11.13 Web server information in error pages

**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 4.3.4.12]

## 11.14 Minimized file type mappings (not there in WiFi)

**Requirement:**

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

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

## 11.15 Restricted file access

**Requirement:**

Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the ONU/ONT webserver's document directory.

In particular, the ONU/ONT webserver shall not be able to access files which are not meant to be delivered.

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

## 11.16 Execute rights exclusive for CGI/Scripting directory

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 4.3.4.15]

# Section 12: Other Security requirements

## 12.1 No System / Root Password Recovery

**Requirement:**

No provision shall exist for ONT/ONU System / Root password recovery.

In the event of system password reset (e.g., through press of Hard-reset button), the entire configuration of the ONT/ONU shall be irretrievably deleted

## 12.2 Secure System Software Revocation

**Requirement:**

Once the ONU/ONT 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.

ONU/ONT shall support a well-established control mechanism for rolling back to previous software image.

## 12.3 Software Integrity Check – Boot

**Requirement:**

The ONU/ONT 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 "Cryptographic Controls for Indian Telecom Security Assurance Requirements (ITSAR)" only to the expected reference value.

## 12.4 Unused Physical and Logical Interfaces Disabling

**Requirement:**

The ONU/ONT 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.

## 12.5 No Default Profile

**Requirement:**

No pre-defined user accounts other than Admin / Root user account would be available.

---

# Section 13 Specific Requirement

The present document contains Indian Telecom Security Assurance Requirements (ITSAR) specific to the stand alone ONU/ONT passive optical network end user devices with a dedicated hardware and dedicated software, which includes system software as well as application software.

---

## 13.1 Registration with ONT

**Requirement:**

The ONT must support transmitting serial No, registration ID, logical ONU ID, credentials for mutual authenticating with OLT

OLT should support this mutual authentication

a) Pre-shared secret

A compliant G-PON system shall support a pre-shared secret key (PSK) that is associated with a particular ONU and is stored at that ONU and in the operator infrastructure. On the operator side, the pre-shared secret for a particular ONU might be stored in the physically-connected OLT, or at a central server that the OLT accesses during authentication. The PSK is a 128-bit value. It may be provisioned into the ONU and into the operator infrastructure in any manner that satisfies these requirements.

b) Master session key

OLT and ONU may execute a mutual authentication procedure, in the course of which both the OLT and the ONU compute the 128-bit master session key (MSK), a session-specific shared secret.

Whenever the ONU is successfully authenticated MSK is used to encrypt data encryption keys that are transmitted upstream.

For the duration of the execution of the secure mutual authentication procedure, the OLT refrains from initiating data encryption key exchanges.

OLT and ONT mutually authenticate based on Pre-shared key or master session key.

[Reference Annex B Enhanced security capabilities 9.13.11 of ITU-T G.988]

---

## 13.2. Secure data Communication on wireless media (Ex: Wi-Fi) for ONT

**Requirement:**

ONU/ONT should support, WPA2- PSK or later version with AES standard in wireless networks which has strong encryption for Wi-Fi standard.

## 13.3 MAC address filtering

**Requirement:**

ONT/ONU should have capability for MAC address filtering, access is granted to matched address only.

## 13.4 Configuration and management of ONTs (Using OMCI/TR69 protocols)

**Requirement:**

Remote configuration management, fault management, performance management & security management of ONT/ONU shall comply mutual authentication & encryption of the management traffic using Secure cryptographic controls prescribed in Table1 of the latest document of "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)".

## 13.5 IGMP Filter

**Requirement:**

The ONT must be able to filter upstream IGMP requests based on white and black lists of multicast groups (defined by both source and destination IP address and placed by the OLT through appropriate OMCI messages) that will allow subscribers to request only multicast streams from the white list or any multicast stream except from the black list.

Reference clause 134 of ETSI TS 102 973 V1.1.1 (2008-09)

## 13.6 SSID Scanning

**Requirement:**

The ONT/ONU 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.

## 13.7 Password Change for User facility

**Requirement:**

1st Installation /Factory Reset ONT/ONU shall 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 ONT shall provide a function that facilitates the user to change his password at any time. However, the ONT shall not allow the previously used passwords up to a certain number (Password History).

## 13.8 Key exchange mechanism

**Requirement:**

The data encryption between the OLT and ONT shall use Secure cryptographic controls prescribed in Table1 of the latest document of “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR).

The keys generated during this process must be unpredictable.

## 13.9 Rogue detection

**Requirement:**

The ONU should have the capability to monitor its own behaviour and autonomously turn off the laser if a fault condition is detected. This capability would serve as a secondary measure in the event that the primary method to turn off the laser via the OLT is not possible. 1) The ONU should turn its laser off if it detects rogue behaviour in order to prevent possible harm to the PON. 2) The ONU should attempt to send a message to the OLT to indicate why the ONU is going out of service.

The ONU transmitter default state (e.g., at installation) should be in the "off" position. This is a precaution to prevent, for example, cases where there is a failure to prevent the transmitter from being shut off, resulting in potential rogue behaviour.

Reference: ITU-T Rec, Series G Supplement 49 (02/2011) Rouge Optical Network unit (ONU)

## Annexure-I

### Acronyms

| | |
|---|---|
| AES | Advanced Encryption Standard |
| CVE | Common Vulnerabilities and Exposures |
| CWE | Common Weakness Enumeration |
| DDOS | Distributed Denial of Service |
| FIPS | Federal Information Processing Standards |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IPSec VPN | Internet Protocol Security Virtual Private Network |
| NIST | National Institute of Standards and Technology |
| NTP | Network Time Protocol |
| OS | Operating System |
| PTP | Precision Time protocol |
| SFTP | Secure File Transfer Protocol |
| AUTN | Authentication token |
| DoS | Denial of Service |
| NCCS | National Centre for Communication Security |
| NTP | Network Time Protocol |
| OS | Operating System |
| PTP | Precision Time Protocol |
| ONT | Optical Network Terminal |
| ONU | Optical Network Unit |
| OLT | Optical Line Terminal |
| PON | Passive Optical Network |
| GPON | Gigabit Passive Optical Network |

## Annexure-II

### List of Undertakings to be Furnished by the OEM for OLT (PON Family BB Equipment) Security Testing

1. Source Code Security Assurance (against test case 3.3)
2. Known Malware and backdoor Check (against test case 3.4)
3. Undertaking that ONT/ONU does not contain Software that is not used in the functionality of ONT/ONU (against test case 3.5)
4. Avoidance of Unspecified Wireless Access (against test case 3.10)
5. Cryptographic Module Security Assurance (against test case 6.2)
6. Cryptographic Algorithms implementation Security Assurance (against test case 6.3)