सत्यमेव जयते

Indian Telecommunication Security Assurance Requirements (ITSAR)

TRANSMISSION TERMINAL EQUIPMENT

(SDH, MULTIPLEXING EQUIPMENT, DXC AND DWDM)

NCCS

Securing Networks

Release Date: Version: 1.0.0

Enforcement Date:

Security Assurance Standards Facility
National Centre For Communication Security
Department of Telecommunications, Bengaluru-560027

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

Sl. No	ITSAR Reference	Title	Remarks
1			

CONTENTS

A) Outline

This document defines the security requirements of Transmission Terminal Equipments that include SDH equipments, Multiplexing Equipments, Digital Cross connects and DWDM equipments. These equipments are used by Indian TSPs to provide transparent transmission of client traffic between connected client devices by establishing and maintaining point to point or point to multipoint connections between such devices. The networks so constructed by using these equipments and transmission links are called as Transport Networks and they, are basically independent of any higher layer network that may exist between the clients. In addition to client traffic, these transport networks carry traffic to facilitate their own operation that are necessary for connection control, operation, administration, maintenance and provisioning (OAMP) functions, network management systems (NMSs), and protection.

The objective of this document is to present a comprehensive, country specific security requirements for Transmission Terminal Equipments. There are various international standardization bodies/associations like ITU-T, ISO, ETSI, IEEE, IETF OIF, TMF, who are working on the security aspects related to communication products. The specifications produced by these bodies along with the country specific security requirements are the basis for this document.

This document commences with a brief description of each of the Transmission Terminal Equipments and proceeds to address the common and entity specific security requirements of them.

B) Scope

This document targets on the security requirements of Transmission Terminal Equipment that includes SDH, Multiplexing Equipment, DXC & DWDM in a non-virtualized environment. SDN application architecture in transport/transmission networks is not considered here. The regulations regarding Remote Access and Lawful Interceptions are not part of this ITSAR. This document neither covers the security requirements at NOC nor organization’s security policy. The requirements specified here are binding both on operators (aka Telecommunication Service Provider- TSP) and network equipment providers (aka OEMs-Original Equipment Manufacturer).

C) Conventions

1. Must or shall or required denotes absolute requirement of particular clause of ITSAR.
2. Must not or shall not denotes absolute prohibition of 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.

Chapter 1 – Introduction

A transmission system takes as an input the signal to be conveyed, which may be a single channel or a multiplexed composite of channels, converts that signal into a format suitable for the transmission medium, propagates the transmission signal to the far end, where after conversion from the transmission signal a reproduction of the input signal is produced. Nowadays, almost all the transmission systems are based on Digital signals and carry tremendous amount of circuit switched and packet switched traffic.

Digital Transmission relies on multiplexing i.e transmitting several signals on a single shared transmission medium. Depending on the domain, the multiplexing can happen on the basis of time (Time Division Multiplexing), Wavelength (Wavelength Division Multiplexing) and Code (Code Division Multiplexing).

There are many Digital Multiplexing Technologies used in Digital Transmission. They are

a) Plesiochronous digital hierarchy (PDH)
b) Synchronous digital hierarchy (SDH)
c) Coarse/Dense wavelength division Multiplexing (DWDM)
d) Optical transport network (OTN).

PDH multiplexers have tributaries (individual bit streams) that have the same nominal frequency, but they are not synchronized to each other whereas SDH multiplexers have tributaries with the same clock frequency and they are all synchronized to a master clock.

In the PDH Hierarchy, four primary systems(E1) are multiplexed) to form an output having 120 channels (second order of multiplexing, E2, 8.448 Mbps). Similarly, four 120-channel systems can be multiplexed to give an output of 480 channels (third order, E3, 34.368 Mbps). Four 480-channel systems are multiplexed to give an output of 1920 channels (fourth order, E4, 139.264 Mbps).

PDH multiplexers are primarily deployed at customer premises and support various client interfaces like ISDN, 2-Wire, PON, HDSL, E1/E2/E3, Nx64 etc.

SDH's basic rate is 155.52 Mbps (STM-1). STM-4 (622.080 Mbps) is constructed by multiplexing four STM-1 basic rate streams; STM-16(2488 Mbps) is constructed by multiplexing 16 STM-1 streams and so on.

SDH Networking elements include Terminal Multiplexers, Add/Drop Multiplexers (ADM), Regenerators and Digital Cross Connects. Terminal Multiplexer (TM) multiplexes a number of tributary signals into one aggregate signal. ADMs can insert/add or extract/drop data directly into or from the traffic that is passing across them, without demultiplexing/multiplexing the frame.

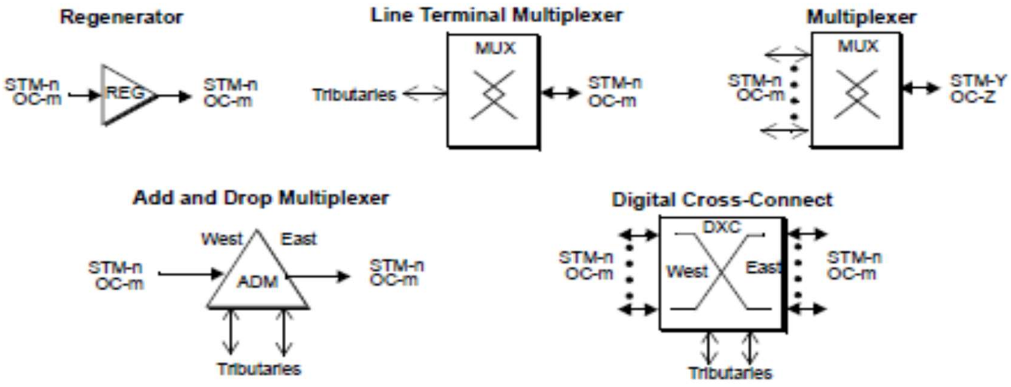

Fig 1.1 SDH Networking Elements

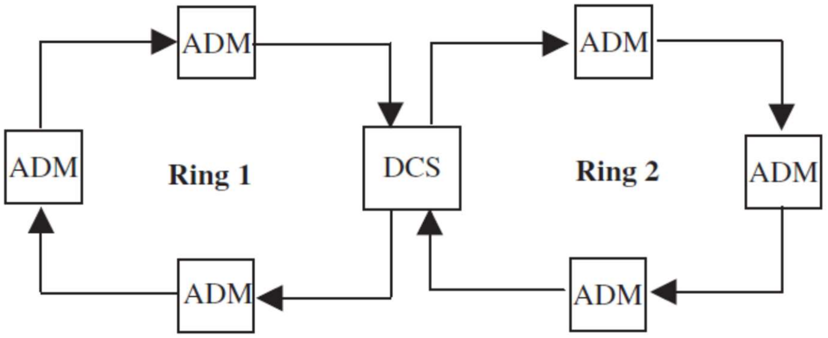

Fig 1.2 A typical SDH Ring

Digital cross-connects (DXCs) configure semipermanent connections to switch traffic between separate networks. The switched traffic can be either SDH streams or selected tributaries. Although it is not common, DXCs can also insert and drop tributaries in transport frames.

The important feature in the DXC is its ability to provision, reconfigure, test, and restore circuits. Provisioning of new circuits and reconfiguration of existing circuits are done electronically via a control terminal. With its ability to be controlled remotely, the DXC facilitates rapid reconfiguration at multiple locations to restore service after transmission facility or equipment failure.

These network elements are mostly deployed in operator network and can support various interfaces like Ethernet, PDH, 2W, NX64, OTU 1/2/3/4, STM-N(electrical/optical) etc

WDM refers to the technology of combining multiple wavelengths onto the same optical fibre. DWDM uses the wavelength spacing proposed in the ITU-T G.692 Standard.

WDM network uses Optical Line Terminals, Transponders, Optical ADMs (OADMs), Optical Cross Connects (OXCs). OADMs and OXCs operate in optical domain. DWDM system can support Ethernet, STM-N and OTU-1/2/3/4 interfaces.

The Optical Transport Networking is defined as the ability to construct WDM networks with advanced services such as optical channel routing and switching, supporting transport of disparate client signals. An optical transport network provides these services to the channels or lightpaths assigned to the higher client layers

The associated transport hierarchy and formats for Optical Transport Network (OTN) are defined with the basic transport frame called the Optical channel Transport Unit (OTU). The nominal bit rates of OTU1, OTU2, OTU3 and OUT 4 are 2.666 Gb/s , 10.709 Gb/s , 43.018 Gb/s, 111.810 Gb/s respectively.

Security of Transmission Terminal Equipments: Network availability is the prime requirement of a transport network.

Security in transmission domain pertains to protection against attacks in 1) Management Plane 2) Control Plane 3) Data/User Plane 4) Synchronisation Plane. Secure hardware/software/firmware define the Node/element level security requirements.

We will collectively call SDH, Multiplexing Equipment, DXC & DWDM as Transmission Terminal Equipment (TTE) and in subsequent chapters address the security requirements.

Chapter 2 – Common Security Requirements

Section 1: Access and Authorization

2.1.1 Management Protocols Mutual Authentication

Requirement:
The protocols used for the TTE 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 TTE management and maintenance.

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

2.1.2 Management Traffic Protection

Requirement:
TTE management traffic shall be protected strictly using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

2.1.3 Role-Based access control

Requirement:
TTE shall support Role Based Access Control (RBAC). A role-based access control system uses a set of controls which determines how users interact with domains and resources. The RBAC system controls how users or groups of users are allowed access to the various domains and what type of operation they can perform i.e. the specific operation command or command group.
TTE supports Role Based Access Control (RBAC) with minimum of 3 user roles, in particular, for OAM privilege management for TTE Management and Maintenance, including authorization of the operation for configuration data and software.

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

2.1.4 User Authentication – Local/Remote

Requirement
The various user and machine accounts on a system shall be protected from misuse. To this end an authentication attribute is typically used, which, when combined with the username, enables unambiguous authentication and identification of the authorized user.
Authentication attributes include
- Cryptographic keys
- Token

- Passwords

This means that authentication based on a parameter that can be spoofed is not permitted. Exceptions are attributes that cannot be faked or spoofed by an attacker.

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

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

2.1.5 Remote login restrictions for privileged users

Requirement:

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

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

2.1.6 Authorization Policy

Requirement:

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

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

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

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

2.1.7 Unambiguous identification of the user & removal of group accounts

Requirement:

Users shall be identified unambiguously by the TTE.

TTE shall support assignment of individual accounts per user, where a user could be a person, or, for Machine Accounts, an application, or a system.

TTE shall not enable the use of group accounts or group credentials, or sharing of the same account between several users.

[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

2.2.1 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) shall be prevented. For machine accounts one authentication attribute will be sufficient. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems.

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

2.2.2 Authentication Support – External

Requirement:
If the TTE supports external authentication mechanism such as AAA server (for authentication, authorisation and accounting services), then the communication between TTE 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.

2.2.3 Protection against brute force and dictionary attacks

Requirement:
A protection against brute force and dictionary attacks that hinder authentication attribute guessing shall be implemented in TTE.
Brute force and dictionary attacks aim to use automated guessing to ascertain authentication attribute for user and machine accounts.
Various measures or a combination of the following measures can be taken to prevent this:
(a) Using the timer delay (this delay could be the same or increased depending the operator's policy for each attempt) for each newly entered password input following an incorrect entry ("tar pit").
(b) Blocking an account following a specified number of incorrect attempts. However, it has to be taken into account that this solution needs a process for unlocking and an attacker can force this to deactivate accounts and make them unusable.
(c) Using an authentication attribute blacklist to prevent vulnerable passwords.
(d) Using CAPTCHA to prevent automated attempts (often used for Web applications).
In order to achieve higher security, two or more of the measures indicated above shall be mandatorily supported by TTE. An exception to this requirement is machine accounts.

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

2.2.4 Enforce Strong Password

Requirement:
(a) The configuration setting shall be such that a TTE 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 TTE). 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 TTE.
e) When a user is changing a password or entering a new password, TTE /central system checks and ensures that it meets the password requirements. Above requirements shall be applicable for all passwords used (e.g. application-level, OS-level, etc.).
Password shall not be stored in clear text in the system; passwords shall be salted and hashed.

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

2.2.5 Inactive Session Timeout

Requirement:
An OAM user interactive session shall be terminated automatically after a specified period of inactivity. It shall be possible to configure an inactivity time-out period.
TTE shall monitor inactive sessions of administrative login users and initiate session locking mechanism based on user configurable timers. Unlocking the session shall be permissible only by authentication. If the inactivity period further continues for a defined period, Session /user ID time out must occur after this inactivity. The timer values can be admin configurable as per requirement, normally set between 2 to 5 minutes.

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

2.2.6 Password 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 should be possible to implement this function on this system.
Password change shall be enforced after initial login.
TTE shall enforce password change based on password management policy.

In particular, the system shall enforce password expiry. TTE 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 TTE shall store at least the three previously set passwords. The maximum number of passwords that the TTE 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.

TTE 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 TTE.

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

2.2.7 Protected Authentication feedback

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

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

2.2.8 Removal of predefined or default authentication attributes

Requirement:
Predefined or default authentication attributes shall be deleted or disabled.
Normally, authentication attributes such as password or cryptographic keys will be preconfigured from producer, OEM or developer of a system. Such authentication attributes shall be changed by automatically forcing a user to change it on 1st time login to the system or the OEM provides instructions on how to manually change it.

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

Section 3: Software Security

2.3.1 Secure Update

Requirement:
For software updates, TTE shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only. To this end, the TTE has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.

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

2.3.2 Secure Upgrade

Requirement:
(a) TTE Software package integrity shall be validated in the installation /upgrade stage.

(b) TTE shall support software package integrity validation via cryptographic means, e.g. digital signature, code signing certificate (valid and not time expired) and using Secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only. To this end, the TTE has a list of public keys or certificates of authorised software sources, and uses the keys to verify that the software update is originated from only these sources.

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

(d) A security mechanism is required to guarantee that only authorized individuals can initiate and deploy a software upgrade and modify the list mentioned in (b) above.

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

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 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 TTE Software which includes OEM developed code, third party software and open-source code libraries used/embedded in the TTE.
(ii)TTE software shall be free from CWE top 25 and OWASP top10 security weaknesses on the date of offer of product to designated TTSL for testing. For other security weaknesses, OEM shall give mitigation plan.

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

2.3.4 Known Malware and backdoor Check

Requirement:
OEM shall submit an undertaking stating that TTE is free from all known malware and backdoors as on the date of offer of TTE to designated TSTL for testing and shall submit their internal Malware Test Document (MTD) of the TTE 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 TTE shall not be present.
Orphaned software components /packages shall not be present in TTE.
OEM shall provide the list of software that are necessary for TTE's operation
In addition, OEM shall furnish an undertaking as "TTE does not contain Software that is not used in the functionality of TTE"

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

2.3.6 Unnecessary Services Removal

Requirement:
TTE shall only run protocol handlers and services which are needed for its operation and which do not have any known security vulnerabilities. By default, all other ports and services will be permanently disabled. TTE Shall not support following services

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

- IP Identification Service (Identd)
- PAD
- MOP

Any other protocols, services that are vulnerable are also to be permanently disabled.
Full documentation of required protocols and services (communication matrix) of the TTE 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]

2.3.7 Restricting System Boot Source

Requirement:
TTE shall boot only from memory devices intended for this purpose.

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

2.3.8 Secure Time Synchronization

Requirement:
TTE shall provide reliable time and date information provided through NTP/PTP server. TTE shall establish secure communication channel with the NTP/PTP server.
TTE shall establish secure communication channel strictly using Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) " with NTP/PTP server.

TTE shall generate audit logs for all changes to time settings.

2.3.9 Restricted reachability of services

Requirement:
The TTE shall restrict the reachability of services such that they can be reached only on interfaces meant for the purpose. On interfaces where services are active, the reachability should be limited to legitimate communication peers.
Administrative services (e.g. SSH, HTTPS, RDP) shall be restricted to interfaces in the management plane for separation of management traffic from user traffic.

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

2.3.10 Self Testing

Requirement:
TTE shall perform self-tests (integrity of the firmware and software as well as correct operation of cryptographic Module as per security requirement area of "self-test" of FIPS-140-2 or Later version etc.,) to identify failures in its security Mechanisms during i) power on

ii) when Administrator Instructs iii) Periodic, with period configurable and iv) at the time of restart.

Section 4: System Secure Execution Environment

2.4.1 No unused functions

Requirement:

Unused functions i.e the software and hardware functions which are not needed for operation or functionality of the TTE shall be deactivated in the TTE's software and/or hardware.
The list of hardware and software functions installed in the system shall match with
the ones that have been mentioned and deemed necessary for the operation of the TTE.

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

2.4.2 No unsupported components

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

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

2.4.3 Avoidance of Unspecified mode of Access

Requirement:
TTE shall not contain any wireless access mechanism which is unspecified or not declared.
An undertaking shall be given by the OEM as follows:

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

Section 5: User Audit

2.5.1 Audit trail storage and protection

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

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

2.5.2 Audit Event Generation

Requirement:

The TTE shall log all important Security events with unique System Reference details as given in the Table below.

TTE shall record within each audit record at least information pertaining to Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event. Additional audit record information, depending on the audit event, shall also be provided as given in the Table below:

Event Types (Mandatory or optional)	**Description**	**Event data to be logged**
Incorrect login attempts (Mandatory)	Records any user incorrect login attempts to the TTE.	Username Source (IP address) if remote access Outcome of event (Success or failure) Timestamp
Administrator access (Mandatory)	Records any access attempts to accounts that have system privileges.	Username, Timestamp, Length of session Outcome of event (Success or failure) Source (IP address) if remote access
Account administration (Mandatory)	Records all account administration activity, i.e. configure, delete, copy, enable, and disable.	Administrator username, Administered account, Activity performed (configure, delete, enable and disable) Outcome of event (Success or failure) Timestamp
Resource Usage (Mandatory)	Records events that have been triggered when system parameter values such as disk space, CPU load over a longer period have exceeded their defined thresholds.	Value exceeded, Value reached (Here suitable threshold values shall be defined depending on the individual system.) Outcome of event (Threshold Exceeded) Timestamp
Configuration change (Mandatory)	Changes to configuration of the network device	Change made Timestamp

		Outcome of event (Success or failure) Username
Reboot/shutdown/crash (Mandatory)	This event records any action on the network device/TTE that forces a reboot or shutdown OR where the network device/TTE has crashed.	Action performed (boot, reboot, shutdown, etc.) Username (for intentional actions) Outcome of event (Success or failure) Timestamp
Interface status change (Mandatory)	Change to the status of interfaces on the network device/TTE (e.g. shutdown)	Interface name and type Status (shutdown, down missing link, etc.) Outcome of event (Success or failure) Timestamp
Change of group membership or accounts (Optional)	Any change of group membership for accounts	Administrator username, Administered account, Activity performed (group added or removed) Outcome of event (Success or failure) Timestamp.
Resetting Passwords (Optional)	Resetting of user account passwords by the Administrator	Administrator username Administered account Activity performed (configure, delete, enable and disable) Outcome of event (Success or failure) Timestamp
Services (Optional)	Starting and Stopping of Services (if applicable)	Service identity Activity performed (start, stop, etc.) Timestamp Outcome of event (Success or failure)
X.509 Certificate Validation (Optional)	Unsuccessful attempt to validate a certificate	Timestamp Reason for failure Subject identity Type of event
Secure Update (Optional)		User identity

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

		Details of data deleted or modified
Port Scan attempts	Any attempt to scan the network interface shall lead to triggering of logging of the appropriate parameters	Date
		Time Stamp
		Source IP address
		Destination Port address
User Login (Mandatory)	All use of Identification and authentication mechanisms.	User identity
		Origin of attempt (IP address)
		Outcome of event (Success or failure)
		Timestamp

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

2.5.3 Secure Log Export

Requirement:
(a) (i) The TTE shall support forwarding of security event logging data to an external system by push or pull mechanism.
(ii) Log functions should support secure uploading of log files to a central location or to a system external for the TTE.
(b) TTE shall be able to store the generated audit data itself may be with limitations.
(c)TTE shall alert administrator when its security log buffer reaches configured threshold limit.
(d) In the absence of external system (due to loss of connectivity or due to node failure or due to any other reasons), TTE shall have mechanism to store audit data locally. TTE shall have sufficient memory (minimum 100 MB) allocated for this purpose. OEM shall submit justification document for sufficiency of local storage requirement.
(e) Secure Log export shall comply the 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 4.2.3.6.2]

Section 6: Data Protection

2.6.1 Cryptographic Based Secure Communication

Requirement:
TTE shall Communicate with the connected entities strictly using the secure cryptographic controls prescribed in Table1 of the latest document “Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)” only.

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

2.6.2 Cryptographic Module Security Assurance

Requirement:
Cryptographic module embedded inside the TTE (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards.

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic module embedded inside the TTE (in the form of hardware, software or firmware) that provides all the necessary security services such as authentication, integrity and confidentiality is designed and implemented in compliance with FIPS 140-2 or later as prescribed by NIST standards".

OEM shall also submit cryptographic module testing document and the detailed self / Lab test report along with test results for scrutiny.

2.6.3. Cryptographic Algorithms implementation Security Assurance

Requirement:
Cryptographic algorithm implemented inside the Crypto module of TTE shall be in compliance with the respective FIPS standards (for the specific crypto algorithm).

Till further instructions, this clause will be considered 'complied' by submission of an undertaking by the OEM in specified format along with self-certified test reports.

An undertaking is to be submitted by the OEM mentioning that "Cryptographic algorithm implemented inside the Crypto module of TTE is in compliance with the respective FIPS standards(for the specific crypto algorithm embedded inside the TTE)"

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

2.6.4. Protecting data and information – Confidential System Internal Data

Requirement:
a) When TTE is in normal operational mode (i.e., not in maintenance mode) there shall be no system function that reveals confidential system internal data in the clear text to users and administrators.

b) 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.]

2.6.5. 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 TTE system that are needed for the functionality shall be protected against manipulation strictly using the Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" with appropriate non-repudiation controls.

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 in the clear. Such systems shall hash this sensitive data strictly using the cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.
(iii)Stored files in the TTE: Shall be protected against manipulation strictly using the NCCS approved Secure cryptographic controls prescribed in Table1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR)" only.

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

2.6.6 Protection against Copy of Data

Requirement:
a) Without authentication, TTE shall not create a copy of data in use or data in transit.
b) Protective measures should exist against use of available system functions / software residing in TTE to create copy of data for illegal transmission.
c) The software functions, components in the TTE for creation of data copy are to be disabled or sufficiently secured to prevent illegal copy of data.

2.6.7 Protection against Data Exfiltration - Overt Channel

Requirement**:**
a) TTE shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound overt channels such as, HTTPS, IM, P2P, Email etc. are to be forbidden if they are auto-initiated by / auto-originated from the TTE.
Session logs shall be generated for establishment of any session initiated by either user or TTE.

2.6.8 Protection against Data Exfiltration - Covert Channel

Requirement:
a) TTE shall have mechanisms to prevent data exfiltration attacks for theft of data in use and data in transit.
b) Establishment of outbound covert channels and tunnels such as DNS Tunnel, HTTPS Tunnel, ICMP Tunnel, TLS, SSL, SSH, IPSEC VPN, RTP Encapsulation etc. are to be forbidden if they are auto-initiated by / auto-originated from the TTE.
c) Session logs shall be generated for establishment of any session initiated by either user or TTE system.

Section 7: Network Services

2.7.1: Traffic Filtering – Network Level

Requirement:
TTE 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 source IP, destination IP and port addresses of protocol header.
(v) To reset the accounting.
(vi) The TTE shall provide a mechanism to disable/enable each defined rule.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.2.6.2.1]

2.7.2: Traffic Separation

Requirement:
TTE shall support physical or logical separation of Operation & management traffic and control plane traffic. See RFC 3871 for further information.

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

2.7.3: Traffic Protection –Anti-Spoofing: TTE shall not process IP Packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.

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

Section 8: Attack Prevention Mechanisms

2.8.1 Network Level and application level DDoS

Requirement:
TTE shall have protection mechanism against Network level and application level DDoS attacks.

TTE shall provide security measures to deal with overload situations which may occur as a result of a denial of service attack or during periods of increased traffic. In particular, partial or complete impairment of system availability shall be avoided.

Potential protective measures include:
- Restricting of available RAM per application
- Restricting of maximum sessions for a Web application
- Defining the maximum size of a dataset
- Restricting CPU resources per process
- Prioritizing processes
- Limiting of amount or size of transactions of an user or from an IP address in a specific time range
- Limiting of amount or size of transactions to an IP address/Port Address in a specific time range

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

2. 8.2 Excessive Overload Protection

Requirement:
TTE shall act in a predictable way if an overload situation cannot be prevented. TTE shall be built in this way that it can react on an overload situation in a controlled way.
However, it is possible that a situation happens where the security measures are no longer sufficient. In such case it shall be ensured that TTE cannot reach an undefined and thus potentially insecure, state.

[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

2.9.1 Fuzzing – Network and Application Level

Requirement:
It shall be ensured that externally reachable services of TTE 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]

2.9.2 Port Scanning

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

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

2.9.3 Vulnerability Scanning

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

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

Section 10: Operating System

2.10.1 Growing Content Handling

Requirements:
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 TTE from operating properly. Therefore, countermeasures shall be taken to ensure that this scenario is avoided.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. Section 4.2.4.1.1.1]

2.10.2 Handling of ICMP

Requirement:
Processing of ICMPv4 and ICMPv6 packets which are not required for operation shall be disabled on the TTE.
TTE shall not send certain ICMP types by default but it may support the option to enable utilization of these types which are marked as "Optional" in below table:

Type (IPv4)	Type (IPv6)	Description	Send	Respond to
0	129	Echo Reply	Optional (i.e. as automatic reply to "Echo Request")	N/A
3	1	Destination Unreachable	Permitted	N/A
8	128	Echo Request	Permitted	Optional
11	3	Time Exceeded	Optional	N/A
12	4	Parameter Problem	Permitted	N/A
N/A	2	Packet Too Big	Permitted	N/A
N/A	135	Neighbour Solicitation	Permitted	Permitted
N/A	136	Neighbour Advertisement	Permitted	N/A

TTE shall not respond to, or process (i.e. do changes to configuration), under any circumstances certain ICMP message types as marked in below table.

Type (IPv4)	Type (IPv6)	Description	Send	Respond to	Process (i.e. do changes to configuration)
5	137	Redirect	N/A	N/A	Not Permitted
13	N/A	Timestamp Request	N/A	Not Permitted	N/A
14	N/A	Timestamp Reply	Not Permitted (i.e. as automatic reply to "Timestamp")	N/A	N/A
N/A	133	Router Solicitation	N/A	Not Permitted	Not Permitted
N/A	134	Router Advertisement	N/A	N/A	Not Permitted

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

2.10.3 Authenticated Privilege Escalation only

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

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

2.10.4 System account identification

Requirement:
Each system account in TTE 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]

2.10.5 OS Hardening

Requirement:
Appropriate OS hardening procedures including security measures required to ensure the kernel miniaturization etc. shall be implemented in TTE.

Kernel based network functions not needed for the operation of the TTE shall be deactivated.

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

2.10.6 No automatic launch of removable media

Requirement:
TTE shall not automatically launch any application when removable media device is connected.

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

2.10.7 Protection from buffer overflows

Requirement:
TTE 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 the OEM.

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

2.10.8 External file system mount restrictions

Requirement:
If normal users are allowed to mount external file systems (attached locally or via the network), OS-level restrictions shall be set properly in TTE in order to prevent privilege escalation or extended access permissions due to the contents of the mounted file systems.
OS-level restrictions shall apply to normal users against mount / use of removable media devices (e.g. USB drive, CD ROM etc.) for data transfer.

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

2.10.9 File-system Authorization privileges

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

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

2.10.10 Restrictions on running Scripts / Batch-processes

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

2.10.11 Restrictions on Soft-Restart

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

Section 11: Web Servers

This entire section of the security requirements is applicable if the TTE supports **web management interface.**

2.11.1 HTTPS

Requirement:
The communication between Web client and Web server 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.

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

2.11.2 Webserver logging

Requirement:
Access to the TTE webserver (for both successful as well as failed attempts) shall be logged by TTE.
The web server log shall contain the following information:

- Access timestamp
- Source (IP address)
- Account (if known)
- Attempted login name (if the associated account does not exist)
- Relevant fields in http request. The URL should be included whenever possible.
- Status code of web server response

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

2.11.3 HTTPS input validation

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

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

2.11.4 No system privileges

Requirement:
No TTE web server processes shall run with system privileges.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.2]

2.11.5 No unused HTTPS methods

Requirement:
HTTPS methods that are not required for TTE operation shall be deactivated.

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

2.11.6 No unused add-ons

Requirement:
All optional add-ons and components of the web server shall be deactivated if they are not required for TTE operation.
In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.

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

2.11.7 No compiler, interpreter, or shell via CGI or other server-side scripting

Requirement:
If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory or other corresponding scripting directory shall not include compilers or interpreters.

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

2.11.8 No CGI or other scripting for uploads

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

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

2.11.9 No execution of system commands with SSI

Requirement:
If Server Side Includes (SSI) is active, the execution of system commands shall be deactivated.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.7]

2.11.10 Access rights for web server configuration

Requirement:
Access rights for TTE web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges.

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

2.11.11 No default content

Requirement:
Default content that is provided with the standard installation of the TTE web server shall be removed.

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

2.11.12 No directory listings

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

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

2.11.13 Web server information in HTTPS headers

Requirement:
The HTTPS header shall not include information on the version of the TTE web server and the modules/add-ons used.

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

2.11.14 Web server information in error pages

Requirement:
User-defined error pages and Error messages shall not include version information and other internal information about the TTE web server and the modules/add-ons used.
Default error pages of the TTE web server shall be replaced by error pages defined by the OEM.

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

2.11.15 Minimized file type mappings

Requirement:
File type or script-mappings that are not required for TTE operation shall be deleted.

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

2.11.16 Restricted file access

Requirement:
Restrictive access rights shall be assigned to all files which are directly or indirectly reside in the TTE web server's document directory.
In particular, the TTE web server shall not be able to access files which are not meant to be delivered.
[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0 section 4.3.4.14]

2.11.17 Execute rights exclusive for CGI/Scripting directory

Requirement:
If CGI or other scripting technology is used, only the CGI/Scripting directory is configured with execute rights. Other directories used or meant for web content do not have execute rights.

[Reference: TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0. section 4.3.4.15]

Section 12: Other Security requirements

2.12.1 Remote Diagnostic Procedure – Verification

Requirement:
If the TTE is providing Remote access for troubleshooting purposes/alarm maintenance then it shall be allowed only for authorized users, other than the root user.

All activities performed by the remote user are to be logged with the following parameters:

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

2.12.2 No System Password Recovery

Requirement:
No provision shall exist for TTE System / Root password recovery.

2.12.3 Secure System Software Revocation

Requirement:
Once the TTE software image is legally updated/upgraded with New Software Image, it should 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.
TTE shall support a well-established control mechanism for rolling back to previous software image.

2.12.4 Software Integrity Check –Installation

Requirement:

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

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

2.12.5 Software Integrity Check – Boot

Requirement:

The TTE shall verify the integrity of a software component by comparing the result of a measurement of the component, typically 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)" to the expected reference value.

2.12. 6 Unused Physical and Logical Interfaces Disabling

Requirement:

TTE shall support the mechanism to verify both the physical and logical interfaces exist in the product.

Physical and logical accessible interfaces (except console interface) which are not under use shall be disabled so that they remain inactive even in the event of reboot.

2.12.7 No Default Profile

Requirement:

Predefined or default user accounts (other than Admin/Root) in TTE shall be deleted or disabled.

2.12.8 Security Algorithm/Protocol Downgrade attack

Requirement:

It shall not be possible to downgrade security algorithms/protocols supported by TTE to other than those listed in Table 1 of the latest document "Cryptographic Controls For Indian Telecom Security Assurance Requirements (ITSAR) version 1.0.0"

Chapter 3 Specific Security Requirements

3.1.1 S-Plane Security (Only for SDH equipments): S plane security is crucial for proper realisation of cryptographic services. A slip may cause the loss of the encryption key which forces the key to be resent, resulting in adverse impact on security.

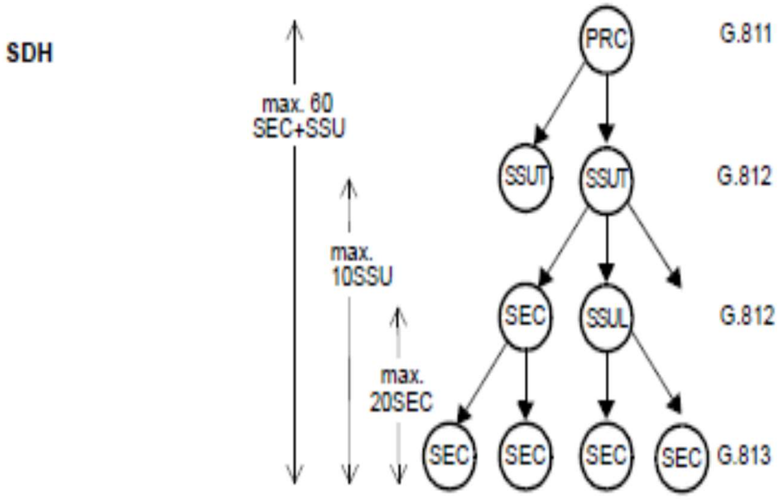

Fig 3.1 SDH Synchronization Network Hierarchy

a) Access to synchronization network management should be secured by different enabling levels from the mere reading of event logs to network and equipment configuration.

b) Synchronisation network topology shall allow Network Element to trace more than one master clock(redundant). The purpose is to avoid depending on only one clock in case of failure.

c)Synchronisation network 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.

3.1.2 Node/Element Level Security Requirements: The hardware over which transmission terminal equipment is running shall be free of known vulnerability at the date of product release. The OEM shall furnish an undertaking in this regard.

Annexure-I (Definition)

1. Administration involves keeping track of resources in the networks and how they are assigned so as to meet service quality objectives. It deals with all the "housekeeping" that is necessary to keep things under control.
2. ASON: An automatically switched transport network (ASTN) that is applied to connection oriented circuit or packet transport networks as defined in ITU-T G.8080.
3. ASTN: An ASTN is a transport network where configuration connection management is implemented by means of a control plane.
4. Control Security Plane (C-Plane): The control plane performs the call control and connection control functions. Through signaling, the control plane sets up and releases connections, and may restore a connection in case of a failure. The control plane also performs other functions in support of call and connection control, such as routing information dissemination.

   The control security plane is concerned with protection of the activities that enable the efficient delivery of information, services and applications across the network. It typically involves machine-to-machine communications of information that allows the machines (e.g., switches or routers) to determine how best to route or switch traffic across the underlying transport network. This type of information is sometimes referred to as control or signalling information. The network carrying these types of messages may be in-band or out-of-band with respect to the service provider's user traffic. A control plane typically functions in a distributed way.
5. Data Plane/User Plane: The data or user plane, that is, bearer plane, is meant to carry the traffic of the terminals of the end-users. The data can be of any information, including voice, files, audio, video and other type of contents.
6. End User Security Plane: The end-user security plane addresses security of access and use of the service provider's network by customers. This plane also represents actual end-user data flows. End-users may use a network that only provides connectivity, they may use it for value-added services such as VPNs, or they may use it to access network-based applications.
7. Firmware refers to the programs and data components of an ICT product that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) and cannot be dynamically written or modified during execution. It is said to be hard-wired and a hybrid between hardware and software.
8. Hardware refers to the physical objects, components, circuits and sub-assemblies that are physically and electronically coupled to process programs and data.
9. Local access: The access from Console interface, from local Console network, from LMT (Local Maintenance Terminal interface) or from TTE's local hardware interface.
10. Machine Accounts: These will be used for authentication and authorization from system to system or between applications on a system and cannot be assigned to a single person or a group of persons.
11. Maintenance refers to activities, such as tests, measurements, replacements, adjustments, and repairs, upgrades/updates necessary to restore or maintain a network resource in a specified state so that the resource can perform its required functions. It also involves corrective and preventive proactive measures.

12. Management security Plane(M-Plane): The management plane performs management functions for the transport plane, the control plane and the system as a whole. It also provides coordination between all the planes. The management plane is usually operating in a centralized way .

    The management functional areas performed in the management plane are: performance management; fault management; configuration management; accounting management and security management.

    The management security plane is concerned with the protection of OAM&P functions of the network elements, transmission facilities, back-office systems (operations support systems, business support systems, customer care systems, etc.), and data centres. The management plane supports the fault, capacity, administration, provisioning, and security (FCAPS) functions. It should be noted that the network carrying the traffic for these activities may be in-band or out-of-band with respect to the service provider's user traffic.

13. NG SDH: Next Generation SDH enables the delivery of TDM and packet-based services over SDH.
14. NMS: A Network Management System is a network management layer (ITU-T M.3010) operations system.
15. Network Management: It refers to activities, methods, procedures and tools that pertains to operation, administration, maintenance and provision of networked systems (OAMP).
16. Network Operations Centre (NOC): NOC handles the operation and maintenance at network levels. The functions of network operations like fault management/service restoration, configuration management, performance management/traffic management, security management, accounting management, report management and inventory management are administered at NOC. A network will generally have only one NOC. NOC is focused on network management functions such as network monitoring traffic management and signalling management. NOC is also responsible for gathering statistics and generating reports for management, system support, and users.
17. Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot the problems as soon as possible, ideally before service is affected. In short, it refers to the processes and procedures used to manage and control telecommunications network devices and telecommunications management
    Network (TMN)-related devices.

18. Operations Support System (OSS) is a server that hosts the implementation of the OSS Application layer in the form of one or more specific OSS applications; the applications might be implemented by Enterprise Java Beans, CORBA objects or Web Services. While eMS and NMS are responsible for managing the network and network resources, OSS supports the operation of network and service management systems.
19. Operator/Telecommunication Service Provider: an entity who has been granted with the license to provide telecommunication services in the country.

20. Original Equipment Manufacturer (OEM): manufacturer of communication and its related products under whose brand, the products are sold or proposed to be sold to operators in the country.
21. Provisioning is concerned with configuring resources in the network to support a given service to users. The act of specifying parameters necessary when assigning/deassigning network resources to/from the control plane or to invoke/remove services provided by a control plane instance. These parameters are specific to a resource or service request, causing changes to these parameters to only impact a specific resource or service request. Therefore, provisioning is allowed in the initialization and operations phases of control plane lifecycle.
22. 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.
23. SDH Equipment Clock (SEC): The logical function representing the equipment clock of a SDH network element having the timing characteristics given in EN 300 462-5-1.
24. SDN: Software Defined Networking is a network architecture approach that enables the network to be intelligently and centrally controlled or programmed using software applications. This enables the operators to manage the entire network consistently and holistically, regardless of underlying network technology.
25. Sensitive Data: data that may be used for authentication or may help to identify the user, such as user names, passwords, PINs, cryptographic keys, IMSIs, IMEIs, MSISDNs, or IP addresses of the UE, as well as files of a system that are needed for the functionality such as firmware images, patches, drivers or kernel modules.
26. Slip: The repetition or deletion of a block of bits in a synchronous or plesiochronous bit stream due to a discrepancy in the read and write rates at a buffer.
27. Software refers to the programs and data components which are usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution. Two general categories of software are system software and application software.
28. Synchronization network: A network to provide reference timing signals. In general, the structure of a synchronization network comprises synchronization nodes connected by synchronization links.
29. Synchronisation plane(S-plane): S-plane is for the frequency and time/phase synchronization information dissemination.
30. System Internal Data: 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).
31. Transmission or Transport is the transfer of information from one entity (transmitter) to another (receiver) via a communication path.
32. Transport Plane: The transport plane provides bidirectional or unidirectional transfer of user information from one location to another. It can also provide transfer of some control and network management information. The transport plane is layered.
33. 10/100/1000 Base-T: Ethernet connection method which operates at 10, 100,1000 Mbps and uses twister pair cables. Base here denotes that base band transmission is used.

Annexure-II(Acronyms)

ASON: Automatically Switched Optical Network

ASTN: Automatically Switched Transport Network

BITS: Building Integrated Timing Supply

BRA: Basic Rate Access

CVSS: Common Vulnerability Scoring System

CWE: Common Weakness Enumeration

CVE: Common Vulnerabilities and Exposures

DWDM: Dense Wavelength Division Multiplexing

DXC: Digital Cross Connect system, also called as DCS

ETSI: European Telecommunications Standards Institute

GMPLS: Generalized Multiprotocol Label Switching

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

ISDN: Integrated System Digital Network

ITU-T: International Telecommunication Union-Telecommunication Standardization

LCT: Local Craft Terminal

MUX: Multiplexer/Demultiplexer Equipment

NG SDH: Next Generation SDH

OIF: Optical Internetworking Forum

OTN: Optical Transport Network

OTU: Optical Transport Unit

PDH: Plesiochronous Digital Hierarchy

PON: Passive Optical Network

PRC: Primary Reference Clock

PRI: Primary Rate Access

SDH: Synchronous Digital Hierarchy

SEC: SDH Equipment Clock

SHDSL: Symmetric/single pair High-speed Digital Subscriber Line

SDN: Software Defined Networking

SSU: Synchronization Supply Unit

STM: Synchronous Transport Module

TDM: Time Division Multiplexing

TEC: Telecommunication Engineering Centre

TMF: Tele Management Forum

Annexure-III (List of Submissions)

1. Source Code Security Assurance (against test case 2.3.3)
2. Known Malware and backdoor Check (against test case 2.3.4)
3. Communication Matrix (against test case 2.3.6)
4. Avoidance of Unspecified Wireless Access (against test case 2.4.3)
5. Cryptographic Based Secure Communication (against test case 2.6.1)
6. Cryptographic Module Security Assurance (against test case2.6.2)
7. Cryptographic Algorithms implementation Security Assurance (against test case 2.6.3)
8. Hardware - Absence of known vulnerability/security weakness (against test case 3.1.2)

Annexure-IV (References)

1. ETSI EN 300 462-2-1 V1.2.1 (2002-06) based on SDH networks Transmission and Multiplexing (TM); Generic requirements for synchronization networks; Part 2-1: Synchronization network architecture.
2. ETSI EN 300 462-1-1 V1.1.1 (1998-05) Transmission and Multiplexing (TM); Generic requirements for synchronization networks; Part 1-1: Definitions and terminology for synchronization networks.
3. ITU-T Recommendation X.805 Security architecture for systems providing end-to-end communications
4. TEC ER TEC78831911 Transmission Terminal Equipment
5. TSDSI STD T1.3GPP 33.117-14.2.0 V.1.0.0: "Catalogue of General Security Assurance Requirements".
6. ETSI EN 300 462-2-1 V1.2.1 (2002-06) Transmission and Multiplexing (TM);
   Generic requirements for synchronization networks; Part 2-1: Synchronization network architecture based on SDH networks

-End of Document-