# Indian CC Certification Scheme (IC3S)

## Certification Report

| | | |
|---|---|---|
| **Report Number** | **:** | **IC3S/KOL01/TEJAS/EAL1/1018/0011/CR** |
| **Product / system** | **:** | **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270** |

**Dated: 15-11-19**

**Version: 1.0**

**Government of India**
**Ministry of Electronics & Information Technology**
**Standardization, Testing and Quality Certification Directorate**
**6. CGO Complex, Lodi Road, New Delhi – 110003**
**India**

*This report contains a total of 16 pages. In case it needs to be reproduced, all the pages must be included.*

**Product developer:**

**Tejas Networks Limited Plot no 25, J. P. Software Park,**
**Electronic City, Phase I, Hosur Road, Bangalore 560100,**
**India**

**TOE evaluation sponsored by**:

**Tejas Networks Limited Plot no 25, J. P. Software Park,**
**Electronic City, Phase I, Hosur Road, Bangalore 560100,**
**India**

**Evaluation facility**:

**CCTL, ERTL(East), Kolkata**
**STQC Directorate, Govt. of India**
**Ministry of Electronics & Information Technology,**
**63 DN Block, Sector V Salt Lake City, Kolkata**
**700091, India**

**Evaluation Personnel:**

1. Smt. Malabika Ghosh (Project Manager)
2. Sri Manikanta Das
3. Sri Anirudhha Ghosh
4. Sri Sumit Jaiswal

**Evaluation report:** **IC3S/KOL01/TEJAS/EAL1/1018/0011/ETR/0010**

**Validation Personnel:** **Sri Tapas Bandyopadhyay**

# Table of Contents

## Contents

# PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

## A1 Certification Statement

| **The product (TOE) below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.** | |
|---|---|
| Sponsor | **Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India** |
| Developer | **Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India** |
| The Target of Evaluation (TOE) | **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270** |
| Security Target | **Security Target TejNOS EN software version 5.3 running in Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270 , Version 1.6** |
| Brief description of product | **TOE is a software package running on the TJ1270 system hardware. Without TJ1270 TOE won't work alone and vice versa. The appliance TOE hardware platform is completely self-contained, housing the software and hardware necessary to perform all functions. TejNOS EN software has the two basic components data and control & management plane. The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic and control plane & management plane is used for administration and configuration and serve the data plane. TJ1270 shall be installed and managed only in private network and not in public network. It can be managed through NMS/EMS.** |
| CC Part 2 [CC-II] | **Conformant to CC Part 2 Version 3.1 Rev 5** |
| CC Part 3 [CC-III] | **Conformant CC Part 3 Version 3.1 Rev 5** |
| EAL | **EAL1** |
| Evaluation Lab | **Common Criteria Test Laboratory, ERTL( East) , Kolkata** |
| Date Authorized | **08-01-2019 ( Ref IC3S letter IC3S/KOL01/TEJAS/EAL2/1018/0011 dated 08/01/2019 )** |

## A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are-

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/MeitY'/Govt. of India);
c) Common Criteria Testing Laboratories (CCTL, ETDC (Bangalore).

## A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1 Rev 5
- Common Evaluation Methodology (CEM) Version 3.1.

## A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation body **Common Criteria Test Laboratory (CCTL, ERTL(East), Kolkata STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology,63 DN Block, Sector V Salt Lake City, Kolkata ,700091, India has** conducted the evaluation of the product. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

**M/s Tejas Networks Limited Plot no 25, J. P. Software Park, Electronic City, Phase I, Hosur Road, Bangalore 560100, India** is the developer and sponsor of the TOE under certification.

The certification process is concluded with the completion of this certification report. This evaluation was completed on 13-11-2019 after submission of [ETR] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the environment described.

This certification report applies only to the version and release/build of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant apply for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

## A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

# PART B: CERTIFICATION RESULTS

## B.1 Executive Summary

### B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

Common Criteria Test Laboratory (CCTL, ERTL(East), Kolkata STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology,63 DN Block, Sector V Salt Lake City, Kolkata ,700091, India has performed the evaluation. The information in the Certification Report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [CCTL, ERTL(East), Kolkata STQC Directorate, Govt. of India, Ministry of Electronics & Information Technology,63 DN Block, Sector V Salt Lake City, Kolkata ,700091, India The evaluation team has evaluated and confirmed that the security target [ST] that is used for evaluation of the product is CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL1) have been met.

### B 1.2 Evaluated product and TOE

**TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270,** the evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The TOE version no. is 5.3 and build no. is txc8-ppc-REL_5_3_19_a10_2.squash.img. The Evaluated Configuration, its security functions, assumed operational environment, architectural information and evaluated configuration are given below (Refer B2 to B5). The TOE & Its Physical Environments & Boundaries are depicted in Figure 1 and Figure 2.

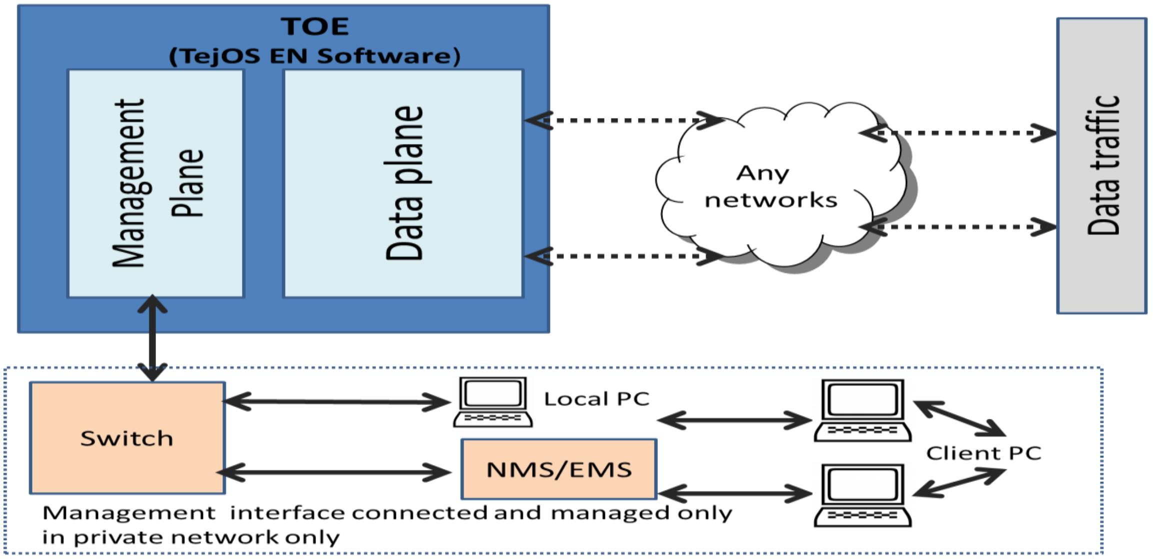

**Figure 1: TOE Boundary**

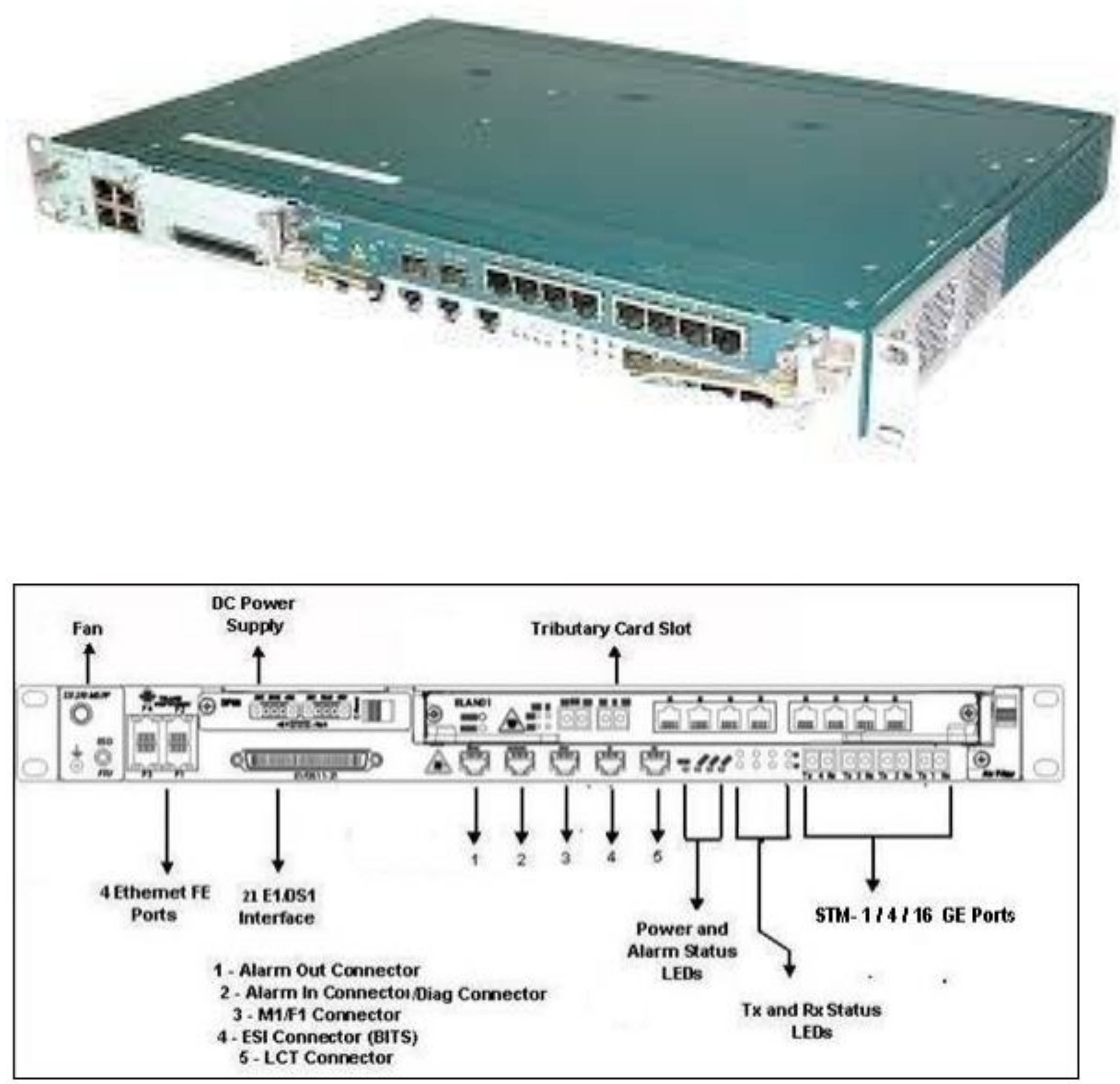

**Figure 2: Networking Equipment TJ1270,**

## B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter. The Security Functional Requirements (SFRs) are taken from CC Part 2.

## B 1.4 Conduct of Evaluation

The common criteria evaluation of the TOE was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. **IC3S/KOL01/TEJAS/EAL2/1018/0011** dated 08/01/2019 later amended as **IC3S/KOL01/TEJAS/EAL1/1018/0011** dated 13th November 2019.

The Target of Evaluation (TOE) is **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270.** TOE is a software package running on the TJ1270 system hardware. Without TJ1270 hardware platform TOE won't work alone and vice versa. The appliance TOE hardware platform is completely self-contained, housing the software and hardware necessary to perform all functions. TejNOS EN software has the two basic components data and control & management plane. The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic and control plane & management plane is used for administration and configuration and serve the data plane. TJ1270 shall be installed and managed only in private network and not in public network. It can be managed through NMS/EMS.

TOE was evaluated through evaluation of its documentation; independent testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM]. The Evaluation Assurance Level is **EAL 1 as per Common Criteria Version 3.1 Rev 5.**

The evaluation has been carried out under written agreement [05-12-2018] between CCTL, ERTL(East), Kolkata and the developer/ sponsor M/s Tejas Networks Limited, Bengaluru.

### B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

### B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

### B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

## B 2 Identification of TOE

The TOE is the **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270.**

**The TOE has the following identification details:**

| | |
|---|---|
| **Product (TOE):** | **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270** |
| **TOE Version:** | **5.3** |

**TOE build and corresponding MD5 Hash values of the software and firmware**

**Software build no.: txc8-ppc-REL_5_3_19_a10_2.squash.img; hash: 8f117ae296cb1cb4e46b00323d7c2ad0**

**Firmware build no.: fw_txc8_r1hw_rel_2_6.tgz: hash: b917964c2f694a0fa2930989b210ff84**

## B 3 Security policy

Following is the list of security features available in the TOE:

- Audit Data Generation
- Audit Review
- Protected Audit Trail Storage
- Cryptographic Key Generation
- Cryptographic Key Distribution
- Cryptographic Key Destruction
- Cryptographic Operation
- Subset Information Flow Control
- Simple Security Attributes
- Subset Residual Information Protection
- User attribute definition
- Verification of secrets
- User authentication before any action
- User identification before any action
- Management of Security Functions Behavior
- Management of Security Attributes
- Secure Security Attributes
- Static Attribute Initialization
- Management of TSF Data
- Specification of Management Functions
- Security Roles
- Reliable Time Stamps
- TSF-initiated termination
- Trusted Path

## B.4 Assumptions

**There are following assumptions exist in the TOE environment.**

**Table 1: Assumptions**

| Item | Assumption ID | Assumption Description |
|---|---|---|
| 1 | A.GENPUR | There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE. |
| 2 | A.NOEVIL | Authorized administrators are non-hostile and follow all administrator guidance. |

| | | |
|---|---|---|
| 3 | A.PHYSEC | The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. |
| 4 | A.PUBLIC | The TOE does not host public data. |
| 5 | A.SINGEN | Information cannot flow among the internal and external networks unless it passes through the TOE. |

## B.5 Evaluated configuration

The **Target of Evaluation (TOE**) is **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270.**

**TOE description**

The TOE is identified as **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270.**

| | |
|---|---|
| **Product (TOE):** | **TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270** |
| **TOE Version:** | **5.3** |

**TOE build and corresponding MD5 Hash values of the software and firmware**

**Software build no.: txc8-ppc-REL_5_3_19_a10_2.squash.img; hash: 8f117ae296cb1cb4e46b00323d7c2ad0**

**Firmware build no.: fw_txc8_r1hw_rel_2_6.tgz: hash: b917964c2f694a0fa2930989b210ff84**

The TOE is the TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270, a software package running on the TJ1270 system hardware. Without TJ1270 hardware platform TOE won't work alone and vice versa. The appliance TOE component is completely self-contained, housing the software and hardware necessary to perform all functions. TejNOS EN software has the two basic components data and control and management plane. The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic and control plane and management plane serve the data plane, which bears the traffic that the network exists to carry.TJ1270 shall be installed and managed only in private network and not in public network. TOE components along with users' manuals are detailed in Table 2.

Table 2: TOE components along with users' manuals

| S/N | Part Number | Description |
|---|---|---|
| 1 | 1127-SW0000015-S | TejNOS EN software version 5.3 running in Tejas Networks SDH / SONET based Optical Networking Equipment TJ1270 |
| 2 | 127-SKU000016-P | TJ1270 System |
| 3 | 127-DOC000023-E | TJ1270 Operation Manual document, Version 0.1 |
| 4 | 127-DOC000024-E | TJ1270 Preparatory Procedure document, Version 0.2 |

## TOE Environment:

The TOE has two logical interfaces: end user and management interface. The management interface to the TOE includes a terminal console, and a Web- Based administrative interface. The TOE includes a proprietary web server developed by Tejas, which provides the main interface for management interface of the TOE. The web server provides users an interface to submit connection requests via an HTTPS encrypted tunnel. The web server provides administrators an interface to administrate the TOE using a web browser. The web server component is included as part of the TOE.

The TOE utilize a Linux operating system that includes the Kernel Versions 2.6.26 The operating system is relied upon for all access to the physical hardware devices connected to the TOE and for providing reliable time stamping. The TOE communicates with various software clients like NMS/EMS etc. These clients open and manage a secure connection to the appliance for user connections

## TOE features under evaluation are:

- Manages users and their profiles
- User Identification and Authentication
- Audit log generation and verification
- User Session Management
- Password complexity and usage settings configuration
- Cryptographic Support
- Trusted Path/Channels
- Cross connect management

## TOE features not under evaluation are:

- Alarms/Fault: Filtering and managing alarms
- Configuration: MSP groups, overhead tunnel, Environment alarm input and SNMP traps.
- Node facility management
- Timing block to Node Synchronization
- License enabling
- Performance monitoring
- Maintenance
- Communication of TOE with IT entities like Radius or AAA server
- Synchronize Node element clock times in a network like NTP server

The hardware on which the TOE runs is not under evaluation.

## Users of the TOE

The ST specifies the four roles as below:

- USER: Read-only access to all the management information including configuration, faults, limited security access for modification of own password and performance.

- OPERATOR: Can perform certain configuration operations such as port and acknowledgment of faults, resetting performance statistics and limited security access for modification of own password etc.

- OPERATOR2: Can configure node name, configure Router ID and Ethernet IP, perform maintenance operations such as software or configuration backup and restore, limited security access for modification of own password and all other operations similar to operator.

- ADMIN: Can create, modify and delete login user on the network element. Can configure Location, Contact, security parameters and as well as management parameters such as Ethernet/Router IP Address/Masks.

Users must log on by Web Session with a user account and password to gain access to the TOE.

## B.6 Document evaluation

### B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility by the developer, are given below:

1. **Security Target: Security Target TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270, Version 1.6**
2. **TOE Functional Specification document**: Functional Specifications (ADV_FSP.2) TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270, version 1.2
3. **Preparative procedures**: TJ1270 Preparatory Procedure version 0.2
4. **Operational User guidance**: TJ1270 Operation Manual Version 0.1
5. **Configuration Management, Capability and scope: Life-cycle Support process TejNOS EN software version 5.3 running in Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270, version 1.3**

### B.6.2 Analysis of document

The developer's documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

**Development process:** The evaluators have analyzed the functional specification of the TOE and found that the TOE security function interfaces [TSFI} are described clearly and unambiguously.

**Guidance Documents:** The evaluators have analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information was also clear and unambiguous.

**Configuration management:** The evaluators have analyzed configuration management documentation and determined that the TOE and its associated components and documents are clearly identified as configurable items (CI).

## B 7 Product Testing

Testing effort required for EAL1 consists of the following two steps: Independent Testing by Evaluation team, Vulnerability analysis and Penetration testing by Evaluation team.

### B 7.1 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of test results. The evaluators have examined the TOE and it is found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. Highlights of Independent testing are given below:

The TOE has been installed properly as per the preparative procedure document. While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements. Independent testing is designed to verify the correct implementation of security functionalities available to different categories of users and to check whether audit record is being generated for auditable events, also checked for the privilege escalation is prevented.

The tests were designed to cover following TSFs and associated TSFIs of the TOE:

a. **Security Audit**

The TOE's auditing capabilities generates audit records for security events. The administrator is the only role with access to the audit trail and has the ability to view the audit trail.

b. **Cryptographic Operations**

TOE supports secure communications between users and the TOE and between TOE components. This encrypted traffic prevents Modification and disclosure of user information.

c. **User Data Protection and Protection of the TSF**

TOE provides an information flow security policy. The security policy limits traffic to specified ports.

d. **Identification and authentication**

Each user must be successfully identified and authenticated with a username and password by the TSF. The TOE provides a password-based authentication mechanism to users. Access to security functions and data is prohibited until a user is identified and authenticated.

e. **Security management**

The TOE allows only authorized users with appropriate privileges to administer and manage the TOE. Only authorized administrators with appropriate privileges may modify the TSF data related to the TSF, security attributes, and authentication data. The TOE maintains 4 default roles (authorities):

**ADMIN**: Can create, modify and delete login user on the network element. Can configure Location, Contact, security parameters and as well as management parameters such as Ethernet/Router IP Address/Masks.

**OPERATOR2:** Can configure node name, configure Router ID and Ethernet IP, perform maintenance operations such as software or configuration backup and restore, limited security access for modification of own password and all other operations similar to operator.

**OPERATOR:** Can perform certain configuration operations such as port and acknowledgment of faults, resetting performance statistics and limited security access for modification of own password etc.

**USER:** Read-only access to all the management information including configuration, faults, limited security access for modification of own password and performance.

f. **TOE Access**

TOE provides time initiated termination of any inactive session that is open for a more than specified duration.

g. **Time Stamps**

TOE provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware.

h. **Trusted Path/Channels**

Connection to and from the TOE are protected using the protocols mentioned within the Cryptographic Support section. Trusted paths are used to secure all user sessions through HTTPS. All connections for the TOE are protected using the HTTPS cryptographic mechanism.

The tests were carried out under isolated and controlled environment which complied with the operational environment, as specified in ST. Test cases were developed using information available in the ST and FSP containing information on TOE interfaces. The manual tests were carried out using the interfaces of the TOE.

### B 7.2 Vulnerability Analysis and Penetration testing

The evaluators have considered the threats identified in ST and conducted vulnerability search from the information available in the public domain in search of potential vulnerabilities from public domain, scanning tools are used. Nmap tools was used for scanning to find out open ports. After configuring close ports, it is found that only 443 TCP port is open. Nessus scanning tool were used with the latest plug in to find out hypothesized potential vulnerabilities present in the TOE.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

Subsequent to the independent review of public domain vulnerability databases and all evaluation evidences, potential vulnerabilities were identified with their attack potentials. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing.

The penetration testing could not exploit any vulnerability in the intended operational environment of the TOE. However, these vulnerabilities may be exploited with higher attack potential.

**Residual Vulnerabilities**

Considering the attack potential as 'Basic', no identified vulnerabilities could be exploited by the evaluators. Hence the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'. However, these vulnerabilities may be exploited with higher attack potential.

The identified vulnerabilities, having attack potential more than 'Basic' were not considered for penetration testing. Hence, these vulnerabilities may be considered as residual vulnerabilities. The residual vulnerabilities are given below.

AT1: Encrypted channel may be intercepted if attacker becomes successful to decrypt algorithms used to encrypt the channel.

AT2: The password is passing in clear text from the client to the TOE and stored there. Though the transmission of password is happening inside the encrypted channel, this vulnerability remains as residual vulnerability as the attack potential to decrypt algorithms used to encrypt the channel is beyond 'Basic'.

## B 8 Evaluation Results

The evaluation team has documented the evaluation results in the Evaluation Technical Report [ETR].

The TOE was evaluated through evaluation of its evaluation evidences, documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedures.

**Documentation evaluation results:**

The documents for TOE and its development life cycle have been analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CC Version 3.1 Revision 5 for Evaluation level EAL1.

**Testing:**

The independent functional tests yielded the expected results, giving assurance that '**TejNOS EN**

**software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270**’ behaves as specified in its [ST].

**Vulnerability assessment and penetration testing:**

The penetration testing with ‘**Basic**’ attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

**Table 3: Assurance classes and components wise verdict**

| Assurance classes and components | | | Verdict |
|---|---|---|---|
| Security target document evaluation | | ASE | PASS |
| 1 | ST introduction | ASE_INT.1 | PASS |
| 2 | Conformance claims | ASE_CCL.1 | PASS |
| 3 | Security problem definition | ASE_SPD.1 | PASS |
| 4 | Security objectives | ASE_OBJ.1 | PASS |
| 5 | Extended components definition | ASE_ECD.1 | PASS |
| 6 | IT Security requirements | ASE_REQ.1 | PASS |
| 7 | TOE Summary Specification | ASE_TSS.1 | PASS |
| TOE Development evaluation | | ADV | PASS |
| 2 | Basic functional specification | ADV_FSP.1 | PASS |
| TOE Guidance document evaluation | | AGD | PASS |
| 1 | Operational user guidance | AGD_OPE.1 | PASS |
| 2 | Preparative procedure | AGD_PRE.1 | PASS |
| TOE Life cycle support evaluation | | ALC | PASS |
| 1 | Labelling of the TOE | ALC_CMC.1 | PASS |
| 2 | TOE CM coverage | ALC_CMS.1 | PASS |
| Testing of the TOE | | ATE | PASS |
| 3 | Independent Testing - conformance | ATE_IND.1 | PASS |
| Vulnerability assessment of the TOE | | AVA | PASS |
| 1 | Vulnerability survey | AVA_VAN.1 | PASS |

## B 9 Validator Comments

The Validator has reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, worksheets, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that ‘TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270 ”satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL1 Certification as per Common Criteria standard version 3.1 Revision 5.**

However, it should be noted that there are no **Protection Profile** compliance claims.

## B 10 List of Acronyms

ACL: Access Control List

CC: Common Criteria

CCTL: Common Criteria Test Laboratory

CEM: Common Evaluation Methodology

EAL: Evaluation Assurance Level

ETR: Evaluation Technical Report

FSP: Functional Specification

IC3S: Indian Common Criteria Certification Scheme

IT: Information Technology

PP: Protection Profile

ST: Security Target

TOE: Target of Evaluation

TDS: TOE Design Specification

TSF: TOE Security Function

TSFI: TOE Security Function Interface

SDH: synchronous digital hierarchy

SONET: Synchronous optical networking

## B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1
4. [CEM]: Common Methodology for Information Methodology: Version 3.1
5. [ST] : Security Target TejNOS EN software version 5.3 running on Tejas Networks SDH / SONET Based Optical Networking Equipment TJ1270
6. [ETR]: Evaluation Technical Report No. IC3S/KOL01/TEJAS/EAL1/1018/0011/ETR/0010