Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : **IC3S/KOL01/ECI_Lightsoft/EAL2/1218/0014/CR**

Product / system : **Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes as mentioned in Annex A; EMS-NPT Software Version 7.6 (build 229) along with required fixes as mentioned in Annex A; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)**

Dated: 6th September 2021
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 20 pages. In case it needs to be reproduced, all the pages must be included.

Product developer: ECI Telecom Ltd. 30 Hasivim Street Petach Tikvah, 4959388 ISRAEL

TOE evaluation sponsored by: ECI Telecom Ltd. 30 Hasivim Street Petach Tikvah, 4959388 ISRAEL

Evaluation facility: Common Criteria Test Laboratory, ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.

Evaluation Personnel: **Evaluators:** Malabika Ghose, Sc. F & Avishek Raychoudhury, Scientific Assistant
Test engineers: Madhumita Chakraborty, Sc ‘C’

Evaluation report: **STQC IT (KOL)/IC3S/KOL01/ECI_Lightsoft/EAL2/1218/0014/ETR/0028**

Validation Personnel: Subhendu Das, Scientist G

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product 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	ECI Telecom Ltd. 30 Hasivim Street Petach Tikvah, 4959388 ISRAEL
Developer	ECI Telecom Ltd. 30 Hasivim Street Petach Tikvah, 4959388 ISRAEL
The Target of Evaluation (TOE)	TOE is composite system, comprised of Network Management Systems (NMS), Element Management System (EMS-APT) and Network Elements (NPTs). The TOE components provide control and monitoring functions for the Network Elements [NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 components] which provide packet transport services. These systems are intended for use in Service Provider (SP) environments. (i) **NMS** is ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes (ii) **EM**S is EMS-NPT Software Version 7.6 (build 229) along with required fixes (iii)**NPTs** are NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269) & NPT-1800 Software Version 7.6 (build 269)].
Security Target	*ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Security Target, Version 1.3*
Brief description of product	LightSOFT is a Network Management System (NMS) providing the control and monitoring of all ECI products deployed by an SP. LightSOFT, when integrated with an Element Management System (EMS), enables SPs to manage multiple technologies (SDH/SONET, DWDM-based optical, ROADM, Carrier Ethernet, and MPLS) independently of the physical layer. LightSOFT simultaneously provisions, monitors, and controls many network layers with multiple transmission technologies. The EMS-NPT is designed to manage the Native Packet Transport (NPT) products. It has an architecture which supports multiple operating systems for integrated management, either standalone or with the NMS. For this evaluation, the EMS-NPT is always integrated with the NMS which is only used to manage the following NPTs: NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800. The NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 are NE appliances that provide Native Packet Transport (NPT) services within the SP network.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL 2
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata
Date Authorized	29th November 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, the then, Department of Information Technology (now MeitY), STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. 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 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 (CCTLs).

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
- 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 of the product was conducted by the evaluation body, Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, West Bengal, India. Hereafter this is referred as '**ERTL (E)-CCTL**'. The evaluation facility is recognized under Indian Common Criteria Certification Scheme (the IC3S), operated by STQC Dte. , Min. of Electronics and Information Technology, Govt. of India.

M/S ECI Telecom Ltd. 30 Hasivim Street Petach Tikvah, 4959388 ISRAEL is the developer of the product and as well as is the sponsor of the TOE evaluation.

The certification process is concluded with the completion of this certification report.

The evaluation team completed all task on 10th August 2021 and handed over the Evaluation Technical Report [ETR] to the validator (on behalf of the certification body).

The confirmation of the evaluation assurance level (EAL) applies on the following conditions:

- 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 of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the developer /sponsor of the product applies for re-certification for 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 https://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 certification Report 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 'Security Target' [ST] of the product, which specifies the functional, environmental and assurance requirements, those the product has addressed.

The evaluation was performed by the CC Evaluators of Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information, presented in this report, are derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] issued by Common Criteria Test Laboratory [ERTL (E)-CCTL], ERTL (EAST), Block-DN Sector-V, Kolkata. The evaluation team determined the product is conformant to CC Version 3.1, Part 2 and Part 3 and concluded that it meets requirements for Evaluation Assurance Level (**EAL 2**) of Common Criteria Standard, ver. 3.1.

B 1.2 Evaluated product and TOE

The evaluated product is a *"**Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes as mentioned in Annex A; EMS-NPT Software Version 7.6 (build 229) along with required fixes as mentioned in Annex A; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)**"*.

"LightSOFT", the Network Management System (NMS) component of the TOE, when integrated with an Element Management System (EMS), enables SPs to manage multiple technologies (SDH/SONET, DWDM-based optical, ROADM, Carrier Ethernet, and MPLS) independently of the physical layer. LightSOFT simultaneously provisions, monitors, and controls many network layers with multiple transmission technologies.

"EMS-NPT", the Element Management System is designed to manage the Native Packet Transport (NPT) products.

"NPTs", the Network Elements (NEs) provide Native Packet Transport (NPT) services within the SP network. For this evaluation, the EMS-NPT is always integrated with the NMS and is only used to manage the following NPTs: NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800.

The **NPT family members** included in the evaluation are:

1. **NPT-1022** - Designed to provide packet throughput ranging from 10 Gbps to 60 Gbps.
2. **NPT-1050** – Designed to provide packet throughput ranging from 72 Gbps to 120 Gbps.
3. **NPT-1200** – Designed to provide packet throughput ranging from 70 Gbps to 240 Gbps.
4. **NPT-1300** – Designed to provide packet throughput up to 920 Gbps.
5. **NPT-1800** – Designed to provide packet throughput up to 2 Tbps.

The evaluated version of the product, with its guidance documents, have been described as the Target of Evaluation (TOE) in this report. The Evaluated Configuration of the product, its security functions, assumed environment are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 3.2 and 4.1 of ST). All the

Security Functional Requirements (SFRs), listed in 6.2 of [ST] are taken from CC Part 2. **The threats** considered by the developer are as below:

i. An unauthorized person may attempt to compromise the integrity of TOE data by bypassing a security mechanism.

ii. The Network systems communicating via the TOE, may attempt to access unauthorized remote network systems by transmitting packets through the TOE with misleading source MAC addresses.

iii. An unauthorized person may attempt to remove or destroy data from the TOE.

iv. An unauthorized person may attempt to compromise the continuity of the TOE's functionality by halting execution of the TOE.

v. An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.

vi. Network systems communicating via the TOE may gain unauthorized access to remote network systems by transmitting packets through the TOE to unauthorized destination MAC addresses.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/KOL01/ECI Lightsoft/EAL2/1218/0014 dated 8th January 2019.

The TOE as described in the [ST] is "***Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes as mentioned in Annex A; EMS-NPT Software Version 7.6 (build 229) along with required fixes as mentioned in Annex A; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)***".

The TOE components LightSOFT and EMS-NPT provide control and monitoring functions for the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments.

The TOE was evaluated through assessment of its Architecture, design and Development documentation, Testing of Security functions, and Vulnerability Assessment, using methodology stated in Common Evaluation Methodology [CEM] of CC Standards and Operating Procedure, OP-07 of Common Criteria Test Laboratory, ERTL (E), Kolkata.

The evaluation has been carried out under written agreement [**29th January 2019**] between Common Criteria Test Laboratory, ERTL (E), Kolkata and the sponsor.

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.

B2 Identification of TOE

The TOE is a "*Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) ; EMS-NPT Software Version 7.6 (build 229) ; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)*".

The TOE components LightSOFT (NMS) and EMS-NPT (EMS) provide control and monitoring functions for the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 components (executing on supported appliances) that provide packet transport services. These systems are intended for use in Service Provider (SP) environments.

TOE environment: Version of the OS: Solaris x86 11.4 on ORACLE machine

(*The TOE components, LightSOFT software and EMS-NPT software are executing on one or more dedicated Solaris servers, (optionally) the LightSOFT client-side application executing on Solaris or Linux workstations, and the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 software executing on supported appliances. The Solaris server that hosts the server side of the LightSOFT NMS and EMS-NPT software components of the TOE is supplied by ECI. The Oracle DB is in a dedicated zone on the Solaris server.)*

Non-TOE Environment:

Table 1: LightSOFT / EMS-NPT Server Minimum requirements

Item	Requirements
Base Hardware	7 virtual CPUs
Memory	48 GB
Hard Disk	85 GB
Operating System	Hardened Solaris x86 11.3 Rev 10
Desktop	CDE 5.10, X11 Version 1.0.3
CORBA	Orbix 6.3.7

Table 2: LightSOFT Client-Side Application Minimum Requirements

Item	Requirements
Base Hardware	< 1 virtual CPU
Memory	1 GB
Hard Disk	2 GB
Operating System	Solaris x86 11.3 Rev 10
CORBA	Orbix 6.3.7

Table 3: The TOE and its guidance document

TOE Component	Description
The Product	Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes as mentioned in Annex A; EMS-NPT Software Version 7.6 (build 229) along with required fixes as mentioned in Annex A; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)
Users' Manual	1. LightSOFT Version 14.91 Getting Started & Administration Guide 2. LightSOFT Version 14.91 Fault Management and Performance Monitoring Guide 3. LightSOFT V14.91 – SW Installation, Update and Configuration Procedure 4. EMS-NPT Version 7.6 Installation Guide (Solaris) 5. EMS-NPT Version 7.6 User Guide 6. EMS-NPT Version 7.6 Service Management Guide 7. EMS-NPT Version 7.6 Performance Management Guide 8. EMS-NPT Version 7.6 Network Management Guide 9. EMS-NPT Version 7.6 Supporting Information 10. Neptune (Packet) Version 7.6 Reference Manual 11. Common Phase 11.3 Activities for Preparation, Installation and Upgrade of Management Systems Infrastructure 12. Common Management HW Preparation and Configuration Activities 13. ECILoracle v12 – SW Installation and Upgrade Procedure 14. Preparative Procedures titled as "ECI LightSOFT v14.91, EMS-NPT v7.6, NPT-1022 v7.6, NPT-1050 v7.6, NPT-1200 v7.6, NPT-1300 v7.6 and NPT-1800 v7.6 Software Common Criteria Supplement", V1.6

B3 Security policy

There are following organizational security policy (ies) that the TOE must meet.

Table 4: Organizational Security Policies

P.Type	Description
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of activities.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 5: Assumptions

A.ECI	Administrators perform installation of the TOE in conjunction with ECI personnel.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.MGMTNETWORK	The TOE components will be interconnected by a private, segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users, and limits traffic from entering the management network.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.NOTRST	The TOE can only be accessed by authorized users.

A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.ORBIX	Orbix provides reliable communication for TSF data transmitted between LightSOFT and EMS-NPT.
A.SOLARIS	Solaris provides separation between LightSOFT, EMS-NPT and Oracle zones on a single physical server.

B.5 Evaluated configuration

Description	Software Version and Release	The image files	File size in bytes	Hash values (MD5)of the image files
Lightsoft NMS Server	Version 14.9	NMSsrv_v1491.01307.Sol_vol1.X93607.iso	2954200 KB	MD5: 1e80cd5c71eb3748edda74948e4ea9ef SHA2: 86d6a2fce440139646e4c057f57889f386a642f578f382894772f19ca9e81a96
		NMSsrv_v1491.01307.Sol_vol2.X93607.iso	2249534 KB	MD5: 950e699fb3a8bd93af43b345e1f559a3 SHA2: 51e8b87e0f3c58a1ba634ffa84e3c3658b1a2731095d7a7904fc73d485877d67
Lightsoft NMS Client	Version 14.9	NMScli_v1491.01307.Sol.X93608.iso	980724 KB	MD5: 20d8b80fe7d5aaa3cdb29e9be940c62d SHA2: 19de428a0a78b9975e7d7c92a964ebbfa382c3c96488258af86a7c705a67e849
EMS APT	Version 7.6.229	emsbgf_sol_x86_7.6.229.iso	1633678 KB	MD5: bda3debebbbf73725a1ebc7215bc2a61 SHA2: 08f22214647413ffd900c52fe1580851d3b1134b65eaba920bdc6bd693321ae8
NPT 1022	Version 7.6.269	NPT1022_Emb_76269.bin	287873 KB	MD5: df5af8566fb42417643902b1042b9ff1 SHA2: 6422e710ea3dce5a46eee24ace96c34f10e7721117134fe846de89360640b74b
NPT 1050	Version 7.6.269	NPT1050i_Emb_76269.bin	327710 KB	MD5: d74fbf7b9b10d1f33798a66488b0b854 SHA2: ca82a03045fe15603307dbc298c7fb86a0ee2d76a366dc47f6de3787d0184866
NPT 1200	Version 7.6.269	NPT1200i_Emb_76269.bin	323550 KB	MD5: 15114321a46f27efbbd49559674ecb1f SHA2: 44e42590bf2ad6e3865fd4be45243f0680260dfdb1fa9a34842d76c15da465fa
NPT 1300	Version 7.6.269	NPT1300_Emb_76269.bin	324031 KB	MD5: 44e8f513d5d4cc11088c851459bccbf1 SHA2: 352e861018cf246817c12f4825b14b852957bba0a8539467df35e52799b5a1a4
NPT 1800	Version 7.6.269	NPT1800_Emb_76269.bin	457921 KB	MD5: 9141fb88631121ec6511e25f7bd99d06 SHA2: 89d87bca00819f9c4c7560a585cd1014d2fdf66f1f1a2e232b43455bdebbf335
Oracle Server	Version 12.08	OraSrv_12.083_Sol-X93816.iso	12215612 KB	MD5: d715fdccb01d03c25ab2492349605d0f SHA2: 87743a6238e5879bd276df49edd0d97147016b50ecfb94361e9e58b3483a0b0a

B6 Document Evaluation

B.6.1 Documentation

The list of documents, presented, as evaluation evidences to the evaluation team are given below:

1. **Security Target**: ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Security Target, version 1.3, date of release: 26.07.2021
2. **TOE Architecture:** ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Development Document, Version 1.0, December 28, 2018
3. **TOE Functional Specification:** ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Development Document, Version 1.0, December 28, 2018
4. **TOE Design description**: ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Development Document, Version 1.0, December 28, 2018
5. **TOE Preparative Guidance**: ECI LightSOFT v14.91, EMS-NPT v7.6, NPT-1022 v7.6, NPT-1050 v7.6, NPT-1200 v7.6, NPT-1300 v7.6 and NPT-1800 v7.6 Software Common Criteria Supplement, Version 1.6 , April 14, 2021

6. **TOE Operational Guidance**:
   1. LightSOFT Version 14.91 Getting Started & Administration Guide
   2. LightSOFT Version 14.91 Fault Management and Performance Monitoring Guide
   3. LightSOFT V14.91 – SW Installation, Update and Configuration Procedure
   4. EMS-NPT Version 7.6 Installation Guide (Solaris)
   5. EMS-NPT Version 7.6 User Guide
   6. EMS-NPT Version 7.6 Service Management Guide
   7. EMS-NPT Version 7.6 Performance Management Guide
   8. EMS-NPT Version 7.6 Network Management Guide
   9. EMS-NPT Version 7.6 Supporting Information
   10. Neptune (Packet) Version 7.6 Reference Manual
   11. ECI LightSOFT, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Common Criteria Supplement Version 1.6
   12. Common Phase 11.3 Activities for Preparation, Installation and Upgrade of Management Systems Infrastructure
   13. Common Management HW Preparation and Configuration Activities ECILoracle v12 – SW Installation and Upgrade Procedure

7. **TOE Configuration Management Capability :** ECI LightSoft, EMS-NPT, NPT-1022,NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Configuration Management Plan version 1.0 June 30, 2019
8. **TOE Configuration Management Scope:** ECI LightSoft, EMS-NPT, NPT-1022,NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Configuration Item List Version 1.2 May 10, 2021
9. **TOE delivery Procedure:** ECI LightSoft, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Delivery Document Version 1.0 June 30, 2019
10. **Test cases, logs and coverage**:
    1. ECI LightSoft, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Test Plan and Procedures Version 1.0 January 31, 2020
    2. ECI LightSoft, EMS-NPT, NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 Software Test Results Version 1.0 January 20, 2020

B.6.2 Analysis of document

The documents related to the following areas were analyzed following the guidance stated in respective Work Units of Common Evaluation Methodology, ver. 3.1[CEM]. The summary of analysis is as below:

The ST:

The evaluation team checked, analyzed the ST document, presented for the TOE and confirmed that ST complies all requirements of the Common Criteria Standards, ver. 3.1 and internally consistent.

TOE Development (Functional Specification, Architecture, and Design):

Functional Specification:

The evaluation team analyzed the functional specification of the TOE in consultation with TOE Design, Guidance document, TOE implementation document and found that the TOE security function interfaces are described clearly and unambiguously.

Security Architecture description:

The evaluation team analyzed the descriptions of the Security architecture of Lightsoft NMS, EMS-NPT and NPT

The evaluator also confirmed that the TSFs are getting initialized securely as below:

- *Initialization of NPT software in separate zone*
- *Initialization of Oracle Database*
- *Followed by initialization of LightSOFT EMS-NPT and LightSOFT Application*

➢ *During NPT initialization no incoming network connections are accepted.*

➢ *No incoming VNC connections are accepted during initialization of LightSoft Application*

➢ *Processing of messages from the NPT Software subsystem is not performed until the LightSoft and EMS-NPT subsystem initialization is complete.*

➢ *Once the initialization is complete the TOE is accessible by authorized user through TSFI*

TSFs are architecturally protected from tampering, through the following means:

1. *Non availability of general purpose processing*
2. *Operating system is hardened. Unnecessary services in the components are disabled.*
3. *Communication to the Oracle Database is limited to the NMS Server zone*
4. *Validation of GUI requests and abortion of the process, if input validation fails*
5. *Limited functionality at UI & NI as "User Interfaces as user input for forwarding only" and "Network Interfaces as user data for delivery via a User Interface only".*

Message is processed by the LightSOFT & EMS-NPT from known entities only.

Bypass of SFR-enforcing functionalities are prevented architecturally:

➢ *LightSOFT & EMS-NPT interfaces require the user to successfully complete the login process before any further access to functions or data.*

➢ *NPTs process incoming data as per configuration for forwarding.*

➢ *No other access to the TOE is available which can bypass the security mechanism.*

➢ *The underlying OS & Database is protected from unauthorized access through hardened server, limited functionality, Secure installation process (OE.INSTALL) & protected physical environment (OE.PHYSICAL)*

Design description:

The description of the TOE has been made in terms of sub-systems:

The TOE is a "**Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) , EMS-NPT Software Version 7.6 (build 229) , NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)**". The TOE components LightSOFT and EMS-NPT provide control and monitoring functions for the NPT-1022, NPT-1050, NPT-1200, NPT-1300 and NPT-1800 components (executing on supported appliances) that provide packet transport services.

The TOE subsystems are as follows:

Subsystem	Description
1. LightSOFT Application	The LightSOFT application provides the GUI interfaces to the administrative users of the TOE. This subsystem may execute on a Solaris/Fedora workstation and be accessed from a user on the same workstation, or execute on the same Solaris server (and zone) as the LightSOFT subsystem and be accessed by remote users via the VNC Server software

Subsystem	Description
2. LightSOFT	The LightSOFT subsystem is a collection of services and applications executing within a zone on the Solaris server. It provides the management functionality for the enterprise-level of the TOE, as well as the pass-through interface used for user access to the EMS-NPT subsystem.
3. EMS-NPT	The EMS-NPT subsystem is a collection of services and applications executing within a zone on the Solaris server. It provides the management functionality for the NPT instances.
4. NPT Software	The NPT Software subsystem is the software executing on NPT appliances. It provides packet transport and filtering functionality.

Guidance Documents: The evaluators 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 were also clear and unambiguous.

Life-cycle support documents: The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.

Configuration management: The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory**.**

Delivery procedure: The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences are found to comply with the requirements of CCv3.1 for **EAL 2**.

B7 Product Testing

Testing at **EAL 2** consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analysed the developer’s test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design was complete.

B 7.2 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 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. The evaluators have repeated the developer’s test at CCTL, Kolkata to confirm the reproducibility of the test results. 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, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

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

a. Security Audit :

The LightSOFT and EMS-NPT servers generate audit records for actions taken by their users and maintain a separate audit trail. The audit trail consists of Security Logs and Activity/Action Logs; audit records for start-up of the audit function are stored in the designated file. The client-side GUI application provide authorized users with the LightSOFT Role of Admin or Security Administrator with the ability to review audit records in a human readable form in LightSOFT. Users with the EMS Role of Admin or Security Admin may review audit records in a human readable form in LightSOFT. Users that do not have those capabilities or roles do not have access to any audit record information.

b. User data protection

ACLs may be configured for Ethernet ports of the NPTs. Each ACL specifies a list of source and destination MAC addresses that may be permitted or denied through the interface. If the flow is permitted, received packets are forwarded; if denied, received packets are silently dropped. If no ACL is associated with a port, all packets are forwarded.

c. Identification and authentication

The TOE requires all users of the client-side GUI application to successfully identify and authenticate themselves before access is granted to any TSF data or functions. User credentials are collected via the GUI and validated by the TOE. When a password is supplied, the TOE echoes a single dot for each supplied character to obscure the user input. If an invalid password is supplied, the count of unsuccessful login attempts for the User Account is incremented. If the supplied password is valid, the count is reset to 0.

d. Security Management

LightSOFT and EMS-NPT provide functionality for authorized users to manage the following items:

- Security configuration (including User Accounts)
- Log management
- NEs
- Services
- Alarms

LightSOFT provides default Roles, and customized Roles may also be configured (via customized Profiles and User Groups). The EMS-NPT Role is also configured via the capabilities. For EMS-NPT, only the default Roles are supported.

B 7.3 Vulnerability Analysis and Penetration testing

The evaluator used scanning tools to identify publicly known vulnerabilities as these standard tools include attack scripts covering type of the TOE, technology and OS used. Port scanning was conducted for CKDS, NKDS and KA. Nessus scanning tool is used with the plugin set ‘202107132056’. Moreover, it is analyzed whether any technology specific vulnerability is present.

The evaluation team has analyzed the evaluation evidences like, **the ST**, **the Functional Specification**, the TOE Design, the Security Architecture Description, the Guidance Documentation and Implementation Representation and then hypothesized the security vulnerabilities considering ‘Bypassing’, ‘Tampering’, ‘Direct Attacks’, ‘Monitoring’ and ‘Misuse’ of the TOE and arrived at Five Attack scenarios**.** Evaluator hypothesized five **Attack Scenarios** and calculated respective Attack **Potentials.**

Sl. No.	Hypothesized potential vulnerabilities/ Areas of Concern identified	Attack scenarios hypothesized with estimated attack potential	PT devised

1	By-pass	**AT1.** Administrator Role of LS Server for GUI based login can access and manage the ECI NPT system through GCT. However, he is not authorized to login as super user in LS Server via SSH and access sensitive files. Application user with highest privilege tries to access sensitive TOE files using SSH to the TOE environment bypassing security mechanism of the application. **Estimated attack potentials:** 6 (within Basic)	**PT1:** The SSH login attempt to access the TOE environment, containing LS Server and LS client.
2	By-pass	**AT2.** Accessing NPTs directly and all its data bypassing EMS-NPT interface to access NPTs. **Estimated attack potentials:** **7** (within Basic)	**PT2:** The SSH login attempt to access the NPT**.**
3	By-pass	**AT3.** Accessing Sensitive Data of Oracle Database bypassing access control mechanism of database using blank credential or default credential**.** **Estimated attack potentials:** 8 (within Basic)	**PT3:** Attacking possible loopholes available during the booting process of the TOE and access sensitive data
4	Tampering	**AT4.** Accessing Sensitive data of TOE during booting process by tampering security mechanism when security functions are not fully invoked. **Estimated attack potentials:** 8 (within Basic)	**PT4:** Try to access sensitive data in Oracle Database with default credential as an attacker
5	Mis-use	**AT5.** Attacker takes the role of Admin and changes any other user's password after creation of account and before first login without knowledge of the user. **Estimated attack potentials:** **11** (beyond Enhanced-basic)	NA

As the target assurance level is **EAL 2**, the evaluation team has restricted their Penetration Testing activities to the attack scenarios for which the estimated attack potential is **less than 10**.

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 vulnerability, having attack potential more than 'Basic' was not considered for penetration testing. Hence, this vulnerability may be considered as residual vulnerabilities. The residual vulnerabilities given below.

AT5 Attacker takes the role of Admin and changes any other user's password after creation of account and before first login without knowledge of the user.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].

The TOE was evaluated through evaluation of its documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07].

Documentation evaluation results:

The documents for TOE and its development life cycle were 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 CCv3.1 for **EAL 2**.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that '**Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) ,EMS-NPT Software Version 7.6 (build 229) , NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269'**, behaves as specified in its [ST], functional specification and TOE design.

Vulnerability assessment and penetration testing:

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

B 9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, 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 '"Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307 & fixes) , EMS-NPT Software Version 7.6 (build 229 & fixes), NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269)", satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, **the TOE is recommended for EAL 2 Certification**.

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
DVS: Development security
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

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]: IACCS Security Framework for Additional IACCS Node and associated systems Security Target, ver. 2.4
6. [ETR]: Evaluation Technical Report No. Report No: Report No: STQC/CC/16-17/19/ETR/0006
7. [OP-07]: CCTL operating procedure

Annexure – A: Configuration of the TOE

Composite system comprised of ECI LightSOFT Software Version 14.91 (build 1307) along with required fixes as mentioned below; EMS-NPT Software Version 7.6 (build 229) along with required fixes as mentioned below; NPT-1022 Software Version 7.6 (build 269), NPT-1050 Software Version 7.6 (build 269); NPT-1200 Software Version 7.6 (build 269); NPT-1300 Software Version 7.6 (build 269); and NPT-1800 Software Version 7.6 (build 269).
At the time of the evaluation, the following updates are available for LightSOFT and EMS-NPT:

LightSoft updates	EMS-NPT updates
• NA1491_1307-100 27 • NG1491_1307-100 27 • NG1491_1307-200 8 • NG1491_1307-300 12 • NSx1491_1307-100 27 • NSx1491_1307-200 8 • NSx1491_1307-300 12 • NT1491_1307-100 27 • OR0600-01 4 • PMx1491_1307-100 27 • WL0213-001 1	• BC0760-01 1 • BS0760-01 1 • BS0760-02 1 • BS0760-03 1

At the time of the evaluation, the following patch is available for Oracle:
10_x86_Recommended_CPU_2021-04.zip

Hash values of fixes and patches:

Name of fix/ patch	MD5 Hash value of fix/ patch
LightSOFT SERVER	
NG1491_1307-100.tar	ab622be29dfe09653377c495de2a5e48
NG1491_1307-200.tar	3305145644bd99c2d73e371f6c4ec8b5
NA1491_1307-100.tar	0390a09c2a23063b11e6e08740267fd7
NG1491_1307-300.tar	f74537237cf0c3983ae4bd76e9fee21a
NSx1491_1307-100.tar	f3c33798530bdf96efbc3314c50d9c69
WL0213-001.tar	3494f8f64632ee685ee5ad95d559d211
PMx1491_1307-100.tar	bb3a70cd871d5a9ece2090fdd0f1682e
NSx1491_1307-300.tar	570750540252b15e3e7cdfa35894a6a6
NT1491_1307-100.tar	e53660893c5829693235ae7a2400bee3
NSx1491_1307-200.tar	d672812977363d87ac3956bad8fb34e2
OR0600-01.tar	54ad3125f7fca9b5b10403c4072266a1
EMS-NPT	
BS0760-01 .tar	03633db724e6790bf8288ed297ec7786
BS0760-03.tar	196d099458c30124161d5ce41ab7024e
BC0760-01.tar	a8e45a91c261914e66ec1e820eaaca5b
BS0760-02.tar	88a0d982803f9884d5dd48d667fbe6ea
Oracle	
10_x86_Recommended_CPU_2021-04.zip	b843d2c47da1e91948740922171bf05e

-------------- o ----------------