Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/KOL01/EAL3/0720/0024/CR

Product / system : C-DOT IP Encryptor software (CEM1_1_1.23_1) running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 processor, Version CEM1_1_1.23_1

Dated: 29th Sept 2025

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

Product developer:	Centre for Development of Telematics (C-DOT) C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030
TOE evaluation sponsored by:	Centre for Development of Telematics (C-DOT) C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030
Evaluation facility:	Common Criteria Test Laboratory, ERTL (East), DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	**Evaluators:** Nishchal, Sumit Jaiswal, Avishek Raychoudhury, Aniruddha Ghosh **Project Manager:** Arpita Datta, Malabika Ghose
Evaluation report:	Report No: IC3S/KOL01/CDOT/EAL3/0720/0024/ETR/066.
Validation Personnel:	Subhendu Das, Scientist G (retired)

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	Centre for Development of Telematics (C-DOT) C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030
Developer	Centre for Development of Telematics (C-DOT) C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030.
The Target of Evaluation (TOE)	The TOE is "**C-DOT IP Encryptor software (CEM1_1_1.23_1) running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 processor**", also identified as 'CEM', responsible for network level encryption that enables the user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. It employs AES algorithms for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as Internet Key Exchange (IKE) protocols for
Security Target	Security Target for IP Encryptor Software running on C-DOT Compact Encryption Module (CEM), Version 07.
Brief description of product	CEM receives the packets from LAN side, encrypts the data using standard symmetric encryption algorithms and sends the packet towards WAN side and receive encrypted data from WAN side, decrypt and send towards LAN side. The same device can also work as L2 encryptor. It provides standard compliant software and hardware interfaces for interoperability.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL 3
PP Claim	Nil
Evaluation Laboratory/facility	**Common Criteria Test Laboratory, ERTL(EAST), Lab Code: KOL01** Government of India, Ministry of Electronics and IT ERTL(E), Block-DN, Sector-V, Salt Lake, Kolkata-700091
Date Authorized	29th Sept 2025

A2. About the Certification Body

The Indian Common Criteria Certification Scheme(IC3S) has been set up by the Ministry of Electronics and Information Technology (MeitY) as part of Cyber Security Assurance initiatives of the Government of India. The purpose of the scheme is to evaluate and certify IT Security Products and Protection Profiles (PP) against the requirements of Common Criteria Standards, at assurance levels EAL 1 through EAL4. The main players in this programme are Developer of IT Security Products or Protection Profiles, Sponsors, Common Criteria Test Laboratory (CCTL) and Certification Body. The scheme provides National Certification, under the International Mutual Recognition Arrangement with the other member countries of CCRA (Common Criteria Recognition Arrangement), acceptable in all the member countries.

Along with other countries, India has already become a member CCRA as a Certificate Authorizing Nation. As per the article 1 of the CCRA, Certificates issued by one member countries are accepted in other countries without re-certification. Only Government Body can be the Certification Body of the country and in our case

MeitY/STQC is the certification body. 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 17065, 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, R5
- Common Evaluation Methodology (CEM) Version 3.1, R5

A.4 Process of Evaluation and Certification

The certification body monitors each individual evaluation project to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at the Certification scheme (IC3S).
The evaluation of the product was conducted by the evaluation facility as mentioned in section A1. The evaluation facility is recognized under Indian Common Criteria Certification Scheme (IC3S).
Centre for Development of Telematics (C-DOT), C-DOT Campus, Mandi Road, Mehrauli, New Delhi 110030, is the developer of the product and as well as is the sponsor of this evaluation and certification project.
The certification process is concluded with the completion of this certification report.
The evaluation team completed all tasks **on 25 August 2025** 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 3) applies in the following conditions:

- All stated conditions 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. However, under 'Assurance Continuity Program' of IC3S, changes in the Certified product can be accommodated within the validity of the present certificate.

A.5 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 on 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 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.

The evaluation activities have been performed by the CC Evaluators of Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India, hence forward, is termed as 'evaluation facility or 'evaluation laboratory' in this report. The information, presented in this report, are derived from the [ST] submitted by the developer and the Evaluation Technical Report [ETR] issued by the evaluation facility. The evaluation team determined the product is conformant to CC Version 3.1, R5 Part 2 and Part 3 and concluded that it meets requirements for Evaluation Assurance Level (**EAL 3**) of Common Criteria Standard, ver. 3.1. R5.

B.1.2 Evaluated product and TOE

"C-DOT IP Encryptor software (CEM1_1_1.23_1) running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 processor" is the heart of Target of Evaluation. The device is responsible for network level encryption. It receives the packets from LAN side, encrypts the data using standard symmetric encryption algorithms and sends the packet towards WAN side. Conversely, the encrypted data received from WAN side gets decrypted by the device and those decrypted data are made available at its' LAN side. The same device can also work as L2 encryptor. It provides standard compliant software and hardware interfaces for interoperability.

The evaluated version of the product, with its guidance documents, has been described as the Target of Evaluation (TOE) in this report. The Evaluated Configuration of the product, its security functions, and the assumed environment are given below (Refer B.2 to B.5).

B.1.3 Security Claims

The [ST] specifies the security objectives of the TOE (sec. 4.1 of the [ST]) and the threats that they counter (sec. 3.3 of [ST]). Most of the Security Functional Requirements (SFRs), listed in 6.2 of the [ST], are taken from CC Part 2. However, there are some security features of the TOE, which could not be defined by the catalog of SFRs of CC Part 2. For those features, a group of 'Extended Security Functional components' have been brought under in the [ST], under section 5 of the [ST].

The developer considered the following **threats**, which are relevant to the TOE:

Threat code	Description
T.UNAUTHORIZED_PEER	An unauthorized IT entity may impersonate as a legitimate communicating peer to establish a VPN communication channel with the TOE which leads to disclosure of User Data. An unauthorized user may get access to TOE security functions and data to disrupt the security function of TOE by changing the configuration data.
T.EAVESDROP	An attacker eavesdrops on communication channel between parties over an untrusted network (e.g. Internet) which leads to unauthorized disclosure of User Data
	An unauthorized process or application may get access to TOE security functions and data to disrupt the security function of TOE

Threat code	Description
T.UNAUTH_APPL	by changing the configuration data.
T.MALFUNCTION	An attacker may use a malfunction of the TOE to deactivate, modify, or circumvent security functions of the TOE to enable attacks against the integrity or confidentiality of User Data or TSF Data.
T.UNIDENTIFIED_ACTIONS	An attacker may change the TOE configuration or management data which may not get detected.
T.UNAUTHORISED_ADMINISTRATOR_ACCESS	An attacker may attempt to gain administrator access to the TOE by various means such as masquerading as an administrator to the device, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session.
T.INTERCEPT	An attacker may intercept and change the network traffic specific to the management and configuration of TOE that may be going to TOE.

B.1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/CB/2019/0011 dated 15.07.2020.

The TOE has been evaluated through the following activities, using methodology stated in Common Evaluation Methodology [CEM] of CC Standards and Operating Procedure, OP-07 of Common Criteria Test Laboratory, ERTL (E), Kolkata.

a. Assessment of its Security Target document, TOE Architecture description, TOE design document, User's guidance document, installation/configuration procedure, document and records of TOE development lifecycle, including developer's test logs'
b. Performing independent Testing of TOE Security functions, and its interface behaviors
c. Assessment security vulnerabilities and performing penetration testing for those security vulnerabilities which could possibly be exploited with "Basic" attack potential.

The TOE was evaluated through assessment of its Architecture description, design and Development documentation, Testing of Security functions, Review of source codes responsible for rendering Security Functions and Focused 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 activities have been carried out under written agreement [dated **31st July 2020**] between Common Criteria Test Laboratory, ERTL (E), Kolkata and Center for Telematics (C-DOT), New Delhi.

B.1.5 Independence of the Certifier

The certifier/validator has not rendered any consulting or other services for the developer, aspiring for CC certification of his product. No relationship exists between the Developer/Sponsor and the certifier/validator, 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. This report is 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.

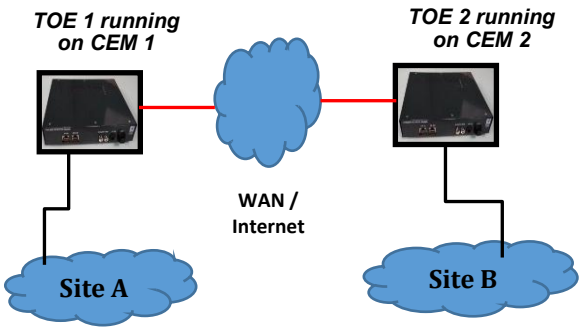
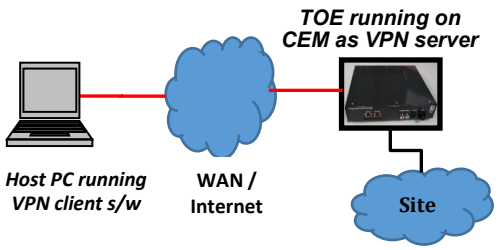
B.1.7 Recommendations and conclusions

- 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 identified as "C-DOT IP Encryptor software (CEM1_1_1.23_1) running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 processor", along with its guidance documents.

The TOE is purposed for realization of Site-to-Site VPN or Remote access VPN.

Site-to-Site VPN deployment scenario for the TOE	Remote Access VPN deployment scenario for TOE
	

B.2.1 TOE environment:

The assumptions made about the TOE environment are:

- The device (CEM) must be protected from any physical attack.
- The IT network of the TOE environment shall protect the management interface of CEM.
- External authentication services to CEM must be available via a RADIUS server operating within internal trusted network.
- CEM uses the timing services from the NTP server to provide accurate/synchronized time services to its own security functions and data; the NTP Server must be available within internal trusted network.
- Authorized users of CEM must be trained and follow all administrator guidance.

B.2.2 Following are the parts/items that shall be delivered to the TOE user

Software:

Sl. No.	List of Item	Quantity	Delivery method
1.	IP Encryptor Software package (Release CD/USB) • Release Tar ball: CEM1_1_1.23_1.tar • Certificate Generation utility v1.0 (for Site-to-Site and Remote-access Site VPN deployment setup): CEM_CERT_GEN_IPSEC_1.1.tar • Software Release Note: CEM-SW-REL-NOTE-CEML1_1_1.23_1	One	Inside CD/USB and shipped by post

	• Installation Manual: CDOT-FT-MAN-INSTALL-IPES_CEM-v02 • User Manual: CDOT-FT-MAN-USR-CEM-v03		
2.	Pre-installation Release Verification file *"md5sum_pre_REL1.23_1.txt"*	One	Through email
3.	Post-installation Release Verification file *"md5sum_post_REL1.23_1.txt"*	One	Through email

Hardware:

Sl. No.	List of Item	Quantity	Delivery method
1.	CEM Hardware: Model: QSCCEM01 Serial Number:	One	shipped by post
2.	Power Adaptor (AC to DC)	One	shipped by post
3.	Serial / Minicom Cable	One	shipped by post
4.	Hardware Release Note: CEM-HW-REL-NOTE-CEMv01	One	shipped by post
5.	CEM User Registration Form: User-Registration-Form-v01	One	shipped by post

B.3 Security policy

There are no Organizational security policies or rules with which the TOE must comply.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Physical Assumptions

Assumption (Physical)	Assumption Description
A.ACCESS	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access to TOE.

Personnel Assumptions

Assumption (Personnel)	Assumption Description
A.COMP_NOEVIL	The authorized users of TOE will be trained and competent to use TOE. He/she will not be careless, willfully negligent, or hostile and will follow and abide by the instructions provided in the TOE documentations.

IT Environment Assumptions

Assumption (Operations)	Assumption Description
A.EXTAUTH	External authentication services will be available via RADIUS server.
A.TIME	External NTP services will be available for synchronization of date and time.
A.NWCOMP	The network components that access the management interface of the TOE will be located within a controlled and secure environment. The authorized users of the components will not be willfully negligent or hostile.
A.LIMITED_FUNCTIONALITY	The TOE is assumed to provide IP encryptor functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide computing platforms for general purpose applications (unrelated to IP encryptor functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. Traffic that is traversing the TOE, destined for another network entity, is not covered by this ST. It is assumed that this protection will be covered by particular types of network devices.

B.5 Evaluated configuration

TOE Hardware Configurations and associated documentation

Sl. No.	List of Item
1.	**CEM Hardware**: Model: QSCCEM01 Serial Number: XXXXXXX
2.	Power Adaptor (AC to DC)

3.	Serial / Minicom Cable
4.	Hardware Release Note: CEM-HW-REL-NOTE-CEMv01
5.	CEM User Registration Form: User-Registration-Form-v01

Identification of the evaluated software files

Sl. No.	Software/Component	Release No.	MD5 Checksum
1	CEM1_1_1.23_1 (includes components mentioned in Sl. No. **2** to **6 of this table**)	1_1_1.23_1	b37ecec92a553949eb6621cf93620281
2	CemPsRel.tar	1_1_1.23_1	d33140f69603a2c72576257b394ccb65
3	cemenv.tar	1_1_1.23_1	32589890948ad5d1071ad96b94b868b4
4	cemrel.tar	1_1_1.23_1	94cbaa666e7276c360284764f4cf10dc
5	auto_rel_upgrade.sh	1_1_1.23_1	473e69de7ef33568e2b0d8443454cfa3
6	ip_list.txt	1_1_1.23_1	5388b1076dd157a72f102edad966beda

B.6 Document Evaluation

B.6.1 Documentation

The list of documents presented as evaluation evidence to the evaluation team is given below:

1. **Security Target**: Security Target for IP Encryptor Software running on C-DOT Compact Encryption Module (CEM), version 07, date of release: 30.07.2025 (Doc. ID: CDOT-FT-ST-IPES_CEM-v06)
2. **TOE Architecture:** Security Architecture for IP Encryptor software running on C-DOT Compact Encryption Module (CEM), version 02, Released on: 18.01.2024 (doc. ID: -CDOT-FT-ARC-IPES_CEM)
3. **TOE Functional Specification:** Functional Specification for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), version 04, Released on: 30-Jul-2025 (Doc. ID: CDOT-FT-FSP-IPES_CEM)
4. **TOE Design description**: TOE Security Design for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), version 03, Released on: 30.07.2025 (Doc. ID: CDOT-FT-TDS-IPES_CEM)
5. **TOE Preparative Guidance**:
   Installation Manual for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), Version 02, Released on:30.07.2025-CDOT-FT-MAN-INSTALL-IPES_CEM.
6. **TOE Operational Guidance**:
   User Manual for C-DOT's Compact Encryption Module (CEM), version 03, Released on: 30.07.2025-CDOT-FT-MAN-USR-CEM
7. **TOE Configuration Management Capability:** Configuration Management Plan for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), version 02, Released on: 30.07.2025-CDOT-FT-CMP-IPES_CEM
8. **TOE Configuration Management Scope:** CI List for TOE Security Function (Document, Source and TOE release)-CDOT-FT-CILIST-CEM
9. **TOE delivery Procedure:** Configuration Management Plan for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), version 02, Released on: 30.07.2025-CDOT-FT-CMP-IPES_CEM
10. **TOE development and maintenance life-cycle model:** Configuration Management Plan for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), version 02, Released on: 30.07.2025-CDOT-FT-CMP-IPES_CEM.
11. **Test cases, logs and coverage**:
    Test Case Document for IP Encryptor Software Running on C-DOT Compact Encryption Module (CEM), Version 04, Released on: 30.07.2025 - CDOT-FT-FTC-IPES_CEM.

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 R5 [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 R5 and internally consistent for EAL 3.

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

Functional Specification:

The evaluation team analyzed the Functional specification of the TOE in consultation with TOE Design and TOE Architecture description and arrived at the conclusion that the TOE Security Function Interfaces are described clearly and unambiguously.

Security Architecture description:

Domain separation

CEM maintains four '**Security Domains'**, architecturally realized through software. Its four software planes are 'Control Plane', Data Plane, Management Plane' and 'System Software plane'. These four planes are separated from each other according to their functionalities. The domains have been created in such a manner that they interact with each other with well-defined interfaces. During the boot-up, the System Software plane initializes the TOE and synchronize clock. The Management Plane perform all the management related tasks and provide CLI to configure the TOE configuration and to configure the IPSec parameters. Control plane helps for establishment of IPSec Tunnel between two instances of the TOE, using IKEv2 protocol and in accordance with the configuration parameters. The Data plane of the TOE takes care of encrypted communication in accordance with the VPN parameters, configured.

Secure start-up

The software planes of the TOE, coupled with the security functions, follow well-defined start-up procedure. On power-on or on re-boot, the TOE performs Self-Test. During self-test, it checks the integrity of Data Plane, Control Plane and Management Plane software. If self-test is passed, it loads the CEM application software (which includes Management Plane, Data Plane, Control Plane and Fault Management Plane). Then it initializes itself with the last active configuration or with the factory default settings. On completion of start-up procedure, the TOE becomes ready for the intended operation.

Self-protection

The TOE protects its security functions through various mechanisms. It first performs self-test to verify the integrity of the system software and ensures that the system software is not tampered with before it is loaded. During integrity check, it calculates the md5 HASH value of the system software file and compares it with the respective stored md5 HASH value. If this integrity check is passed, it loads the CEM system software. After loading the system software, TOE also checks the integrity of the cryptographic operations by checking the correctness of supported AES-CBC algorithm.

Non-bypassibility

All user inputs to the TOE through the CLI are validated at the time of entry itself, ensuring entered input does not corrupt the TOE or cause any unintended consequences. It is also ensured that the user runs and enters inputs according to the privileges it has been granted.

The TOE is accessible to its users only when all the software planes of the CEM are executed properly and in the well-defined order as configured in the design. None of the functionality of the TOE is accessible until all the planes are up and running. All security functions are invoked properly when the TOE boots up successfully. Users can only access the CEM through its ETH-IN port by logging in, using SSH. Once authenticated, user gets access to Command Line Interface (CLI) and can run the commands, as per his authorization. Access to the CEM without authentication is not permitted.

Design Description:

The TOE comprises of 7 subsystems, those are (1) TOE Initialization subsystem (2) TOE Access subsystem (3) Cryptographic Support subsystem (4) Identification & Authentication subsystem (5) IPSec subsystem (6) Audit subsystem and (7) Configuration Data subsystem. These subsystems are responsible for implementing the intended TOE Security Functions.

The evaluator presented the mapping of the subsystems to the TOE Security Functions. The behavior of the subsystem described in the TOE design document is in line with the purpose of the TSFI identified in FSP document. The TOE design document covers all SFRs accurately. This analysis has been presented by the evaluator.

TOE Guidance

Guidance Documents: The evaluator analysed guidance documents (preparative procedure and operational user guidance) and confirms that preparative procedure is clear and unambiguous. Clear steps to bring the TOE to its secure state have been defined. The information is operational user guidance are clear and unambiguous.

TOE Development environment

Life-cycle support documents: The document on TOE development Life cycle support, containing information on Configuration Management processes and Delivery Procedure etc. and the related records reflect the TOE development discipline that the developer follows. Those documents are evaluated found 'Complied' with the requirements of the Standards. During site visit, the evaluator evidenced those documented processes are being followed by the development team.

Configuration management scope: The evaluator analyzed configuration management documentation (Configuration Management Plan and scope; it is confirmed that for the documented method of uniquely identifying the configuration items is followed. The evaluator has arrived at a conclusion that the TOE and its associated documents are properly brought under configuration management process. The evaluators also analyzed access control measures on CM system, as defined in the CM documentation and found them satisfactory for "ALC_CMC.3: Authorization controls" requirements.

Delivery procedure: The evaluator analyzed the TOE delivery document with an objective of ascertaining whether it covers secure delivery of the TOE to the end-users and found the same satisfactory. The secure delivery procedure has been further audited by the evaluators during their visit to the development site. TOE delivery process enables the customer/end-users of the TOE to check integrity of the instance of TOE, received.

The respective evaluation evidence is found to comply with the requirements of CCv3.1 R5 for EAL3.

B.7 Product Testing

Assurance through Testing of the TOE for EAL 3 consists of the three prongs testing efforts, those are (1) Testing by developer, (2) Independent Testing by Evaluation Team, and (3) Penetration testing on potential vulnerabilities of the TOE, hypothesised through analysis of the TOE related documents.

B.7.1 IT Product Testing by Developer

The evaluators analysed the developer's test report to assess coverage and depth of their testing effort and found satisfactory. The test procedures are comprehensive enough for repeatability and reproducibility. The result of evaluator's analysis of test evidences has been reported in Evaluation Technical Report [ETR], IC3S/KOL01/CDOT/EAL3/0720/0024/ETR/066.

B.7.2 IT Product Independent Testing by Evaluation Team

The evaluator prepared the TOE following the preparative procedure to achieve the sated configuration of the TOE as claimed in the Security Target document. Independent tests are carried out under isolated and controlled environment at CCTL which complied with the stated operational environment. The test cases are developed based on the information available in Security Target, Functional Specification and design description of the TOE. Manual tests are carried out using the interfaces of the TOE.

The evaluators' independent functional testing effort is summarized below.

- Evaluator planned for 22 test cases, covering ALL the TSFIs and the SFRs (Security Functional Requirements) stated in Functional Specification and Security Target documents. The tests are conducted in an environment, which is consistent with the Operational Environment of the TOE, declared in the ST.
- All tests are planned and documented in detail, so that those are repeatable and reproducible.
- The evaluator verified the TOE configuration steps as given in TOE preparative guidance document and found

that the TOE is configurable as per the guidance and the evaluated configuration of the TOE can be successfully arrived.

- The evaluator has repeated the developer's tests at CCTL, Kolkata to confirm the test results. [report no.: IC3S/KOL01/CDOT/EAL3/0720/0024/IND/0064]
- The results of Independent testing(ATE_IND) confirm correct implementation of the stated security functionalities.

B.7.3 Vulnerability Analysis and Penetration testing

The evaluator used vulnerability scanning tools, primarily, Nessus' to identify publicly known vulnerabilities. The tool 'Nessus' includes attack scripts to verify the presence of technology specific vulnerabilities the TOE. 'Nessus' plugin set '*202507070008 dated: Jul 7, 2025*' is used for this purpose.

The evaluator has analyzed the ST, Functional Specification, Design description, Security Architecture Description, the Guidance Documents to find out possible security vulnerabilities, considering '**Bypassing**', '**Tampering**', '**Direct Attacks**', '**Monitoring**' and '**Misuse**' of the TOE and arrived at following Attack scenarios.

Category Bypass:

AT3: An adversary exploits a bypass by accessing the TOE through any hidden backdoor user account, circumventing normal authentication controls.

AT9: An adversary exploits a bypass by accessing the TOE's management interface through the external ETH OUT port, circumventing network isolation controls

Category Direct Attack:

AT2: An adversary performs a direct attack by exploiting known CVE vulnerabilities in the TOE's outdated OpenSSH to compromise system security.

AT6: An adversary performs a direct attack by exploiting flawed SSH authentication that accepts passwords matching only the first 8 characters, ignoring extra characters (e.g., Root@123 is accepted, and Root@1234, Root@123XXX also succeed).

Category Monitoring:

AT5: An adversary conducts monitoring by probing open external interfaces (SSH, serial console) before the TOE completes self-tests and exits the Fail Secure State

Category Misuse:

AT 1: An adversary misuses the audit log mechanism to extract sensitive data like VPN EAP passwords, PSKs, and RADIUS secrets logged insecurely.

AT 4: An adversary exploits misuse by accessing the ipsec.secrets file due to excessive permissions exposing sensitive IPSec credentials.

AT 7: An adversary exploits misuse due to audit logs having excessive 'execute' permissions, exposing security risks from improper file access controls

AT 8: An adversary leverages misuse by using a legitimate command to view the RADIUS PSK exposed to the Root system user in plaintext

AT10: Adversary leverages misuse by attempting USB-based certificate configuration without proper privilege or valid certificate package

Additional effort by the evaluator:

During the evaluation process, CEM got modified several times based on the continuous feedback from the evaluation results and finally achieved requisite compliance. The final vulnerability assessment conducted with 'Nessus' plugin set '*202507070008 dated: Jul 7, 2025*'.

Areas of concern and hypothesized attack scenarios with estimated attack potential.

Sl. No.	Hypothesized potential vulnerabilities/ Areas of Concern (AoC) identified	Attack scenarios hypothesized with estimated attack potential	PT devised
1	An attacker may exploit hidden back door of the underlying OS of the TOE and bypass its authentication mechanism /access control /interface restriction.	**AT3**: An adversary exploits a bypass by accessing the TOE through any hidden backdoor user account, circumventing normal authentication controls. **Estimated attack potential:** 8 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack **AT9**: An adversary exploits a bypass by accessing the TOE's management interface through the external ETH OUT port, circumventing network isolation controls. **Estimated attack potential:** 7 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack	**PT 3** **PT 9**
2	An adversary can directly exploit vulnerabilities in the TOE—such as weaknesses in software components, protocol implementations, or configurations—to compromise its security functions.	**AT2**: An adversary performs a direct attack by exploiting known CVE vulnerabilities in the TOE's outdated OpenSSH to compromise system security. **Estimated attack potential:** 4 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack **AT6:** An adversary performs a direct attack by exploiting flawed SSH authentication that accepts passwords matching only the first 8 characters, ignoring extra characters (e.g., Root@123 is accepted, and Root@1234, Root@123XXX also succeed). **Estimated attack potential:** 7 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack.	**PT 2** **PT 6**
3	An attacker can monitor security mechanisms for unauthorized access.	**AT5:** An adversary conducts monitoring by probing for open external interfaces (SSH, serial console) before the TOE completes self-tests and exits the Fail Secure state **Estimated attack potential:** 7 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack.	**PT 3**
4	An adversary can **misuse legitimate functions or excessive permissions** to gain unauthorized access to security-relevant information or configurations	**AT1:** An adversary misuses the audit log mechanism to extract sensitive data like VPN EAP passwords, PSKs, and RADIUS secrets logged insecurely**.** **Estimated attack potential:** 8 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack	**PT 1**

Sl. No.	Hypothesized potential vulnerabilities/ Areas of Concern (AoC) identified	Attack scenarios hypothesized with estimated attack potential	PT devised
		AT4: An adversary exploits misuse by accessing the ipsec.secrets file due to excessive permissions exposing sensitive IPSec credentials. **Estimated attack potential:** 8 (<Basic) Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack	**PT 4**
		AT7: An adversary exploits misuse due to audit logs having excessive 'execute' permissions, exposing security risks from improper file access controls. **Estimated attack potential:** 7 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack.	**PT 7**
		AT8: An adversary leverages misuse by using a legitimate command to view the RADIUS PSK exposed to the Root system user in plaintext. **Estimated attack potential:** 8 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack.	**PT 8**
		AT10: An Adversary leverages misuse by attempting USB-based certificate configuration without proper privilege or valid certificate package **Estimated attack potential:** 7 (<Basic). Therefore, for EAL 3, the TOE must be tested to confirm that it is resistant to this hypothesized attack	**PT 10**

The relevant attack potentials, corresponding to the identified vulnerabilities, have been estimated considering various factors like the '**time to identify & exploit'**, '**expertise required'**, '**knowledge of the TOE'**, '**windows of opportunity'** and **'equipment required'**. The Evaluator also estimated the spent attack potential of AT1 as AT10 (more than '**Basic**' Attack Potential), following the guidance of CEMv3.1.

The evaluator conducted Penetration Testing PT1 to PT10 for attack scenarios AT1 to AT10 and established that the TOE is unexploitable by the attack with 'Basic' Attack Potential **(≤ 9**).

As the target assurance level is EAL 3, the evaluation team has restricted their Penetration Testing activities to the attack scenarios for which the estimated attack potential is 8 which is within 'Basic Attack Potential'.

Considering the attack potential as **'Basic'**, no identified vulnerabilities/areas of concern could be exploited by the evaluators.

As any security measure can be compromised by an attack with very high attack potential and with unlimited resources of the attacker; the security functions of this product are also breakable. Hence, the TOE may have some security weakness which can be exploited with the attacks having higher attack potential than 'Basic'.

The Evaluator identified such vulnerabilities and declared those as residual vulnerabilities for this Security Evaluation project. The reported residual vulnerabilities are as follows:

- An adversary performs a monitoring attack by intercepting IKEv2 message flows during key negotiation over an insecure intermediate network path. While the messages are encrypted, metadata like packet timing and volume may leak behavioral patterns.

- An adversary exploits a direct attack by targeting side-channel leakages (e.g., timing or power consumption) during AES encryption operations on the ARMv7 CPU, attempting to recover cryptographic keys using differential analysis techniques.
- An adversary conducts a bypass by emulating a remote peer in a site-to-site VPN setup, attempting to exploit misconfigured or weak IKEv2 authentication policies to establish unauthorized secure tunnels.
- An adversary misuses legitimate TOE CLI commands (available to Root-System) to view cryptographic parameters or logs that reveal operational secrets such as key lifetimes or negotiation logs, which may aid in future attacks.
- An adversary tampers with stored configuration files or IKE security policies on the TOE if filesystem permissions or integrity verification mechanisms are inadequately enforced post-boot, aiming to downgrade the cryptographic strength or inject malicious peers.

  [Vulnerability Assessment planning and execution for the TOE IP Encryptor Software running on C-DOT Compact Encryption Module (CEM) Version CEM1_1_1.23_1, Dt: 18.08.2025 (Report No.: IC3S/KOL01/CDOT/EAL3/0720/0024/AVA/065]

B.8 Site visit

To assess the implementation of all security control measures taken by the developer for the development environment, the evaluation team visited the development site on 5th-6th June 2024. The specific objectives of site visit are as below:

- To observe usage of the CM system as described in the CM documentation
- To ensure that the integrity of the TOE is preserved throughout its life cycle by using Configuration Management System
- To evidence measures, procedures, and standards concerned with secure delivery of the TOE, ensuring that the security protection offered by the TOE is not compromised during the transfer to the user.
- To observe the practical application of delivery procedures as described in the delivery documentation.
- To witness the security measures implemented by the developer during development and maintenance of the TOE and its consistency with that described in the development security documentation.

The Evaluation team has drawn their conclusion as satisfactory, after the site visit and confirmed that the specific requirements for EAL 3 are met in respect of ALC_CMC.3, ALC_DEL.1 and ALC_DVS.1
The evaluator presented the site visit report as, Report No: IC3S/KOL01/CDOT/EAL3/0720/0024/SiteVisit/063 dated 18-Aug-2025.

B.9 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].

A. 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 R5 for EAL3.

B. Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that '**C-DOT IP Encryptor software (CEM1_1_1.23_1) running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 processor**', behaves as specified in its [ST], functional specification and TOE design.

B. Vulnerability assessment and penetration testing:

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

B.10 Validator Comments

The Validator has reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation results, evidence, documents, records, etc. shared by the evaluator and agrees with the conclusion made by the evaluator for each evaluation work-unit of Common Evaluation Methodology (CEM). The consolidated comments are as follows:

- 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 'C-DOT IP Encryptor software (CEM1_1_1.23_1) running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 processor', satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL 3 Certification.

B.11 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.12 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 for IP Encryptor Software running on C-DOT Compact Encryption Module (CEM), Version 07
6. [ETR]: Evaluation Technical Report No. Report No: IC3S/KOL01/CDOT/EAL3/0720/0024/ETR/066
7. [OP-07]: CCTL operating procedure