Indian CC Certification Scheme (IC3S)

Certification Report

Report Number : IC3S/DEL01/VALIANT/EAL1/0317/0007/CR

Product / system : OAM (Operation, Administration & Management/Maintenance) Module VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer

Dated: 12-12-2018

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:	**Valiant Communications Limited** 71/1 Shivaji Marg, New Delhi-110015, India
TOE evaluation sponsored by:	**Valiant Communications Limited** 71/1 Shivaji Marg, New Delhi-110015, and India
Evaluation facility:	**CCTL – ERTL (North), Delhi** **STQC Directorate,** **Ministry of Electronics & Information Technology,** **S- Block, Okhla Industrial Area Phase – II** **New Delhi – 110020**
Evaluation Personnel:	Mr. M.K. Saxena Mrs. Banani Das Ms. Anjali Jain
Evaluation Reviewer	A K Upadhyay
Evaluation report:	**CCTL-ERTL (N), Delhi/Valiant/OAM/CC/ETR-03/06/2018/103**
Validation Personnel:	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	**Valiant Communications Limited**
Developer	**Valiant Communications Limited**
The Target of Evaluation (TOE)	**OAM (Operation, Administration & Management/Maintenance) Module** VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer
Security Target	Security Target: OAM (Operation, Administration & Management/Maintenance) Module running on VCL-MX Version6 80 E1, 160Mbps Voice & Data Multiplexer, Version 1.4
Brief description of product	The Target of Evaluation (TOE) is an Operation, Administration and Management/ Maintenance Module (OAM Module) which works as authentication, access control operation, user administration and management/maintenance module. The TOE is a software application module used in telecom sector. TOE is used with VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer. The TOE is the OAM Module implemented on Linux Version: 2.6.31 GNU/Linux. VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer acts as the IT system for the OAM Interface Card. The OAM is the entry point to the system for any user attempting to make configuration changes in the system. OAM provide security against intrusion. OAM interface provides a highly secured interface.
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL1
Evaluation Lab	**CCTL - ERTL(N), New Delhi**
Date Authorized	29-03-2017

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: **M/s Valiant Communications Limited**

b) STQC Certification Body **: IC3S (STQC Certification body/ MeitY/Govt. of India**);

c) Common Criteria Testing Laboratories: **CCTL- ERTL (N), New Delhi**

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 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
- 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 (North), S- Block, Okhla Industrial Area Phase – II, New Delhi – 110020, 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.

Valiant Communications Limited 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 28th November 2018 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 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 (North), D S- Block, Okhla Industrial Area Phase – II, New Delhi – 110020, 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 (North), S- Block, Okhla Industrial Area Phase – II, New Delhi – 110020, India]. The evaluation team has evaluated and confirmed that the security target [ST] that is used for evaluation of the product (TOE) 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

The TOE OAM (Operation, Administration & Management/Maintenance) Module consists of

VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer. The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The product version number is 10.00V20180912FS.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.

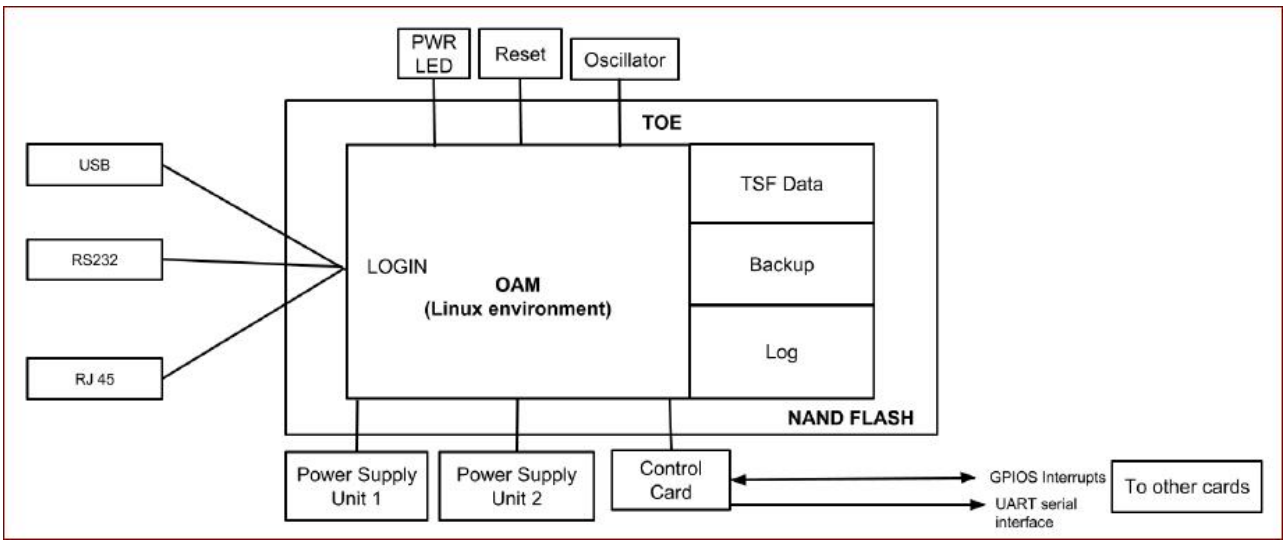

Figure .1- TOE & Its Physical Environments & Boundaries

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 evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. STQC/CC/1617/23 dated 29th March 2017.

The TOE as described in the [ST] is called as Operation, Administration and Management/ Maintenance Module (OAM Module). It works as authentication, access control operation, user administration and management/maintenance module. The TOE is a software application module used in telecom sector. TOE is used with VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer. The TOE is the OAM Module implemented on Linux Version: 2.6.31 GNU/Linux. VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer acts as the IT system for the OAM Interface Card.
The OAM is the entry point to the system for any user attempting to make configuration changes in the system. OAM provide security against intrusion. OAM interface provides a highly secured interface.
TOE was evaluated through evaluation of its documentation (product and process related); Independent testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM].

The evaluation has been carried out under written agreement [dated 29th March 2017] between CCTL, ERTL (N)-New Delhi and the developer/ 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.

B 2 Identification of TOE

The TOE is the OAM (Operation, Administration & Management/Maintenance) Module running on VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer. The TOE version number is 10.00V20180912FS.It is a unique product and is used with E1, 160Mbps Voice and Data Multiplexer.

B 3 Security policy

There is no Organizational security policies that the TOE must meet.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 1: Assumptions

ASSUMPTION CODE	DESCRIPTION
A.NO_HOSTILE	The administrators are not careless or willfully negligent and will abide by the administrator guidance.
A.LOCATE	The resources of the TOE will always be located within controlled access facility, which will prevent unauthorized physical access.
A.TRAIN_AUDIT	The auditor is trained to review logs regularly and identify sources of concern.
A.LOG_OUT	The user connected through physical ports are expected to exit the session before he leaves the system unattended.

B.5 Evaluated configuration

The Target of Evaluation (TOE) is an Operation, Administration and Management/ Maintenance Module (OAM Module) which works as authentication, access control operation, user administration and management/maintenance module. TOE, the software, is used with VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer to access and set the OAM card configuration and other non-TOE card (Core [Control Card, E1 Card, PSU], Ringer Card, FXS Card/ Hotline Card, FXO Card, E&M Card, 64IF Card, NX64 Card, RIO Card, G.703 Card, RS-232 Card, C37.94 TP Card, TP4C Card, Ethernet + Optical Card & Ethernet Card) configuration. The TOE is the OAM Module implemented on Linux operating system Version: 2.6.31GNU/Linux. The TOE (OAM product.tar.bz2) along with other files (rootfs.tar.bz2, rwfs.tar.bz2 & linux.sb) is loaded in flash memory. The TOE is used for authentication of users (superuser, systemuser and adituser) and provides access to the systems resources in controlled LAN environment.

The RTC stored in control card provides a source of date and time information for the TOE, which is used in audit timestamps. When the system is powered ON the time stored in the RTC is brought into the OAM oscillator. The oscillator of the OAM maintains the time of the system thus giving the necessary time stamps for logging purposes. The date and time can be set in the Control Card by using help/rtc/ Command. After a power failure, RTC maintains its date and time using Lithium Ion battery of control card.

The OAM Interface provides two serial ports (RS232 and USB) and one Ethernet port (RJ45) to login OAM. The OAM communicates with the other cards through control card. The superuser accesses OAM locally through serial port. System user and adituser access through Ethernet port (RJ45) through SSH and systemuser additionally access through serial port.

The User connects to the OAM through login interface. There are three types of users:

- Superuser: The “Superuser”, who is also the system administrator, creates “users” and assigns the password for each such user. Superuser has the access to the OAM settings and its configuration (specifically it can change network settings of OAM and can create and delete systemuser). Superuser can access OAM through serial port (RS232 and USB)

- Systemuser: A “Systemuser” is any normal user of the system that is 'created' by 'superuser'. While the “systemuser” are provided with an access to the system, they only have a limited access to the OAM settings and its configuration.

- Audituser: An 'audituser' is a user who shall be able to view and download the LOG files by accessing the system on Ethernet port using SSH protocol and shall not have access to anything else in the system. Only 'superuser' can change audituser’s password.

TOE Software Identification- OAM (Operation, Administration & Management/Maintenance) Module running on VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer. The version number was 10.00V20180912FS.

Table 2: Details of evaluated instantiations of the TOE: Unique reference of evaluated Software

(Version no. 10.00V20180912FS)

File name	File Size	MD5 hash
linux.sb	2197776	00a0d9243f915c589d78fa460e41f148
product.tar.bz2	83594	dce8854ec2b507cd3a69e07e0d5bfe83
rootfs.tar.bz2	31916564	b2ac2706eea30dfdefc2a28a176953f6
rwfs.tar.bz2	560117	bbf3b8e8abc3b3c21cf5ba68384c9f35

The non-TOE hardware required by the TOE:

- VCL-MX Version 6 Chassis along with its power supply unit and connection cables.
- Ethernet wire, USB cable, RS-232.
- Non-TOE cards: Core(Control Card, E1 Card, PSU), Ringer Card, FXS Card/ Hotline Card, FXO Card E&M Card, 64IF Card, NX64 Card, RIO Card, G.703 Card, RS-232 Card, C37.94 TP Card, TP4C Card Ethernet + Optical Card, Ethernet Card

The non-TOE software required by the TOE includes:

- A third party software to communicate with OAM ex. TeraTerm or PuTTY.

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**: OAM (Operation, Administration & Management/Maintenance) Module running on VCL-MX Version6 80 E1, 160Mbps Voice & Data Multiplexer.
2. **TOE Functional Specification document**: OAM Functional specification.
3. **Preparative procedures**: Preparatory Guidance Document
4. **Operational User guidance**: Operational User Guidance, AGD_OPE:
5. **Configuration Management, Capability /scope**

B.6.2 Analysis of document

The developers 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.

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

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 and Vulnerability analysis & Penetration testing.

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 results as per the Test Plan: STQC-IT Delhi/CC/TP02/OAM.

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. The 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, considerations were 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 were designed to verify the correct implementation of security functionalities available to different types of users and to check whether audit 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 OAM Module creates and stores audit records for the f user activities. Audit records are stored in 100KB files locally on NAND Flash. The overall memory allocated on NAND Flash for audit storage is 10 MB. When a 100 KB audit file is exhausted, a new file is created for audit storage and the process continues until whole 10 MB audit storage exhausts. After the whole 10 MB storage is exhausted, the LOG files are deleted in FIFO manner for further audit storage. In a LOG file, LOGS of events are written in sequence of occurrence. This ensures that even if someone tries to vary the clock of the system, the login attempt and introduced changes are logged as latest entries irrespective of system clock time stamp. "Audituser" shall be able to view and review the logs by accessing the system through SSH and shall not have access to anything else in the system. Other than audituser, only superuser can view filtered LOGS through CLI interface

b. Identification and authentication

The TOE requires users to provide unique authentication information before any access to the system is granted. The TSF enforces binding between users and TOE. User accounts in the TOE have

the following attributes: user identity (username), authentication data (password) and user role ("Superuser", "Systemuser" "Audituser"). Every user has an entry in the database, which includes username, password (hashed) and user role. The passwords are stored in hashed format in accordance with salted MD5 algorithm. Superuser assigns default passwords during Systemuser creation and these passwords do not fulfill password strength requirements. Systemuser is forced to change this default password to a secure password of strength >=14. The TSF detects when unsuccessful authentication attempts occur related to wrong user names or passwords

c. Security management

The Authorized Administrator (Superuser) is responsible for managing (creation, deletion) user accounts. The TOE provides systemuser access either through the physical serial port (USB/RS232) or remotely over the Trusted Path using the SSH2 protocol. Superuser/System can view the system settings, Change the network configuration i.e. IP Address, Subnet Mask, Gateway and DNS Addresses and control the system.

d. TOE Access function

The TSF shall be able to deny session establishment based on 1. Incorrect login credentials i.e. username and password 2. Incompatible mode (like Ethernet, serial port) of access.
Following are correct ports of access as per the user role:
Audituser – using Ethernet port (RJ45) through SSH protocol
Superuser – using serial port (USB/RS232)
Systemuser – using serial port (USB/RS232) and Ethernet port (RJ45)
All access attempts to the TOE require passing through an authentication mechanism. Users can terminate user sessions. The sessions through SSH expire after 6 minutes. The TSF enforces, by default, a limit of 1 session per user. The system closes the existing sessions immediately if it is interrupted due to reasons such as time-out, power failure, and resetting and link disconnection.

e. Protection of Security Functions

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that users must authenticate before any administrative operations can be performed on the system, whether those functions are related to the management of user accounts or the configuration of access control. The RTC stored in control card provides a source of date and time information for the TOE, which is used in audit timestamps. When the system is powered ON the time stored in the RTC is brought into the OAM oscillator. The oscillator of the OAM maintains the time of the system thus giving the necessary time stamps for LOG purposes. In the event of either the failure or the removal of the OAM Card from the chassis, the session terminates. The previous configurations in the other cards continue as long as power failure does not occur. It will remain in secure state.

f. TRUSTED PATH/CHANNELS

The TOE supports and enforces Trusted Channels that protect the communications between the TOE and Users from unauthorized disclosure or modification of data. The TOE achieves Trusted Path by use of the SSH protocol which ensures the confidentiality and integrity of communication with the users (systemusers).

g. CRYPTOGRAPHIC SUPPORT

The TOE uses salted MD5 Hashing technique to store passwords. MD5 is used to verify through the creation of a 128-bit message digest from data input that is claimed to be unique. The SSH protocol is

followed for establishing a trusted channel between the user and the OAM system through exchange of keys as per SSH File transfer protocol.

B 7.3 Vulnerability Analysis and Penetration testing

The possible security vulnerabilities were searched from public domain considering the reported vulnerabilities of similar products/technology. In search of potential vulnerabilities from public domain, scanning tools are used by the Evaluation facility. Vulnerability scanning was conducted to find out open ports, services and their associated vulnerabilities. OpenVAS scanning tool is used with the latest feeds 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 potential vulnerabilities with higher than 'Basic' attack potential are treated as residual vulnerabilities.

Penetration testing scenarios are summarized as below:

- TSF behavior in case of TCP flooding on the TOE
- Inheriting privileges or other capabilities that should otherwise be denied; i.e., whether users of different roles can escalate their privileges beyond their defined privileges as given in ST, bypassing implemented mechanism in TOE. Mis-use of privilege escalation by lower level users / Vulnerability through specified interfaces
- Attempt to crack the salted MD5 through which the user password is hashed and stored in the TOE.
- Improper input validation of string format in the username and host argument. If specific usernames including "%" symbols can be created on a system then an attacker could run arbitrary code as root when connecting to Dropbear server.

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.

B 8 Evaluation Results

The evaluation team has documented the evaluation results in the [ETR].
The TOE was evaluated through evaluation of its evaluation evidences, documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [QA/EP-10].

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 CCv3.1 for EAL1.

Testing:

The independent functional tests yielded the expected results, giving assurance that '(Operation, Administration & Management/Maintenance) Module running on VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer', the TOE version number is 10.00V20180912FS,)' behaves as specified in its [ST], functional specification.

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 Validator has 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 for EAL1 evaluation.**
- **The results of evaluation of product and process documentation, independent testing and vulnerability assessment confirm that the TOE 'OAM (Operation, Administration & Management/Maintenance) Module running on VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer', the TOE version number 10.00V20180912FS, satisfies all the security functional requirements and assurance requirements as defined in the [ST].**

  Hence, the TOE is recommended for EAL1 Certification as per CC version 3.1.

However, it should be noted that there are no **Protection Profile** compliance claims, it is evaluated based on the Security target [ST].

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

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: OAM (Operation, Administration & Management/Maintenance) Module running on VCL-MX Version6 80 E1, 160Mbps Voice & Data Multiplexer

6. [ETR]: Evaluation Technical Report No. CCTL-ERTL (N)/Valiant/OAM/CC/ETR-04/11/2018/172
7. [QA/EP-10]: CCTL operating procedure