SECURITY TARGET

OAM (Operation, Administration & Management/Maintenance) Module

VCL-MX Version 6

80 E1, 160Mbps Voice & Data Multiplexer

ST Version 1.4

16th October 2018

PREPARED BY:

Abhishek Anand
Sagar Gupta
AshutoshVaish

Aditi Jha

(Valiant Communications Limited)

71/1 Shivaji Marg, New Delhi-110015, India

www.valiantcom.com

ABSTRACT:

This document provides the basis for the evaluation of a specific Target of Evaluation (TOE), OAM Module (Operational, Administration & Management/Maintenance Module) a part of VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, security requirements and the IT security functions provided by the TOE which meet the set of requirements.

DOCUMENT MANAGEMENT

Document ID	ASE Version 1.4
Document Title	Security Target
Release Authority	Abhishek Anand

DOCUMENT HISTORY

Version	Date	Description	Author
1.0	16th March 2017	Initial Draft	AshutoshVaish Sagar Gupta
1.1	20th July 2017	Revised Draft	AshutoshVaish Sagar Gupta
1.2	14thOctober 2017	Revised Draft	Sagar Gupta AshutoshVaish
1.3	12thDecember 2017	Revised Draft	Sagar Gupta AshutoshVaish
1.4	16th October 2018	Final Draft	Aditi Jha

CONTENTS

DOCUMENT MANAGEMENT 3
DOCUMENT HISTORY 3
CONTENTS 4
1. INTRODUCTION 6
1.1 ST REFERENCE 6
1.2 TOE REFERENCE 6
1.3 ST OVERVIEW 6
1.4 TOE OVERVIEW 7
1.5 TOE DESCRIPTION 8
1.5.1 PHYSICAL BOUNDARY 8
1.5.2 LOGICAL BOUNDARY 9
1.5.3 Non TOE CARDS 11
2. CC CONFORMANCE CLAIMS 12
2.1 COMMON CRITERIA CLAIMS 12
3. SECURITY PROBLEM DEFINITION 13
3.1 THREATS 13
3.2 ENVIRONMENTAL THREATS 13
3.3 ORGANIZATIONAL SECURITY POLICIES 14
3.4 ASSUMPTIONS 14
4. SECURITY OBJECTIVES 16
4.1 SECURITY OBJECTIVES FOR TOE 16
4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT 17
5. EXTENDED COMPONENT DEFINITION 18
6. SECURITY REQUIREMENTS 19
6.1 SECURITY FUNCTIONAL REQUIREMENTS 19
6.1.1 CLASS FAU: SECURITY AUDIT 19
6.1.2 CLASS FIA: IDENTIFICATION AND AUTHENTICATION 22
6.1.3 CLASS FMT: SECURITY MANAGEMENT 24
6.1.4 CLASS FPT: PROTECTION OF THE TSF 27
6.1.5 CLASS FTA: TOE ACCESS 28
6.1.6 CLASS FTP: TRUSTED PATH/CHANNELS 28
6.1.7 CLASS FCS: CRYPTOGRAPHIC SUPPORT 29
7. TOE SUMMARY SPECIFICATION 31
7.1 SECURITY AUDIT 31
7.1.1 AUDIT EVENTS 31
7.1.2 AUDIT RECORDS 32

7.1.3 AUDIT STORAGE 32
7.1.4 AUDIT VIEW 32
7.2 IDENTIFICATION AND AUTHENTICATION 33
7.2.1 USERNAME AND PASSWORD 33
7.2.2 IDENTIFICATION AND AUTHENTICATION FAILURE 34
7.3 SECURITY MANAGEMENT 35
7.3.1 MANAGEMENT ROLES 35
7.3.2 TSF DATA 36
7.4 PROTECTION OF TSF 37
7.4.1 RTC (REAL TIME CLOCK) 37
7.4.2 SECURE STATE IN CASE OF FAILURE 37
7.5 TOE ACCESS 37
7.6 TRUSTED PATH/CHANNELS 38
7.7 CRYPTOGRAPHIC SUPPORT 38
8. CORRESPONDENCE AND RATIONALE 39
8.1 TOE SECURITY OBJECTIVES RATIONALE 39
8.2 ENVIRONMENTAL SECURITY OBJECTIVES RATIONALE 40
8.3 DEPENDENCY RATIONALE 41
8.4 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE 43

1. INTRODUCTION

This chapter presents Security Target (ST) and TOE identification information and a general overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. An ST principally defines:

A security problem expressed as a set of assumptions about the security aspects of the environment, a list of threats that the TOE is intended to counter, and any known rules with which the TOE must comply (chapter 3, Security Problem Definition).

A set of security objectives and a set of security requirements to address the security problem (chapters 4 and 6, Security Objectives and IT Security Requirements, respectively).

The IT security functions provided by the TOE that meet the set of requirements (chapter 7, TOE Summary Specification).

1.1 ST REFERENCE

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

ST Revision: 1.4

ST Draft Date: **16th October 2018**

Author: Sagar Gupta

AshutoshVaish

Abhishek Anand

Aditi Jha

1.2 TOE REFERENCE

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

1.3 ST OVERVIEW

The security target follows the following format:

S.No.	Title	Description
1	ST Introduction	This section provides the TOE overview. It defines the hardware and software that makes up the target of evaluation as well as physical and logical

		boundaries of the TOE.
2	CC Conformance Claims	This section lists evaluation conformance to CC versions, Protection Profile or Packages where applicable.
3	Security Problem Definition	It illustrates the threats, organizational security policies and assumptions by which the TOE is affected.
4	Security Objectives	This section defines the security objectives for TOE and provides the rationale to prove that security objective satisfies the threat.
5	Extended Security Requirements Components Definition	This section defines the extended Security Functional Requirements (SFRs).
6	Security Requirements	It contains the functional and assurance requirement for the TOE.
7	TOE Summary Specification	It identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.
8	Rationale	It demonstrates traceability and internal consistency.

Table 1.1- ST Organization and Section Descriptions

1.4 TOE OVERVIEW

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.

OAM is used for creating systemusers for system configuration. These systemusers can further configure and manage the Non-TOE cards such as E1 interface card.

There are three categories of users: superuser (administrator), systemusers (users for system maintenance and management) and audituser (to view and review audit records). Systemusers have limited access to the TOE security functions. User roles are described in subsequent chapters.

The OAM (TOE) is used along with a control card, Power supply units and other cards (ex E1 interface card). The power supply units provide power to the system for operation. There is a provision of redundant power supply available. The control card provides a real time clock for system timing, powered through its internal battery. It also provides alarm extensions. Other non-TOE cards are available as per the functionality expected of the VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer.

The non-TOE hardware required by the TOE includes:

- VCL-MX Version 6 Chassis along with its power supply unit and connection cables.

- Ethernet wire, USB cable, RS232/DB9 cable.
- Non-TOE cards

The non-TOE software required by the TOE includes:

- A third party software to communicate with OAM ex. TeraTerm or PuTTY on windows 7 and 8.

NOTE 1: The TOE will be pre-installed software. Considering the possibilities of product corruption, if the user requires any subsequent installations of the product for resolving the issues, the product needs to be sent to the developers only. It will be ensured by the developer that the installed version on the product is only the evaluated version.

NOTE 2: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*

1.5 TOE DESCRIPTION

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. OAM works as an authentication, access control operation, administration, management and maintenance gateway to the multiplexer (VCL-MX Version 6 80 E1, 160Mbps Voice & Data Multiplexer).

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 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.

1.5.1 PHYSICAL BOUNDARY

The OAM Interface provides two serial ports (RS232 and USB) and one Ethernet port(RJ45) to connect the unit to the external world. The user may use either of the above ports to access, maintain and manage the system, either locally or remotely over a secure IP link.

Network interface	RJ45 Ethernet 10 BaseT (MDI-X)
Compatibility	Ethernet Version 2.0 IEEE802.3

Protocols supported	UDP/IP, TCP/IP, SSH, ICMP, SNMP
LEDs	10Base-T connection and activity.
EMI Compliance	• Radiated and conducted emissions - complies with Class B limits of EN55022:1998 • Direct and Indirect ESD - complies with EN55024:1998 • Electrical Fast Transient/Burst Immunity complies with EN55024:1998 • Power Frequency Magnetic Field Immunity complies with EN55024:1998 • RF Common Mode Conducted Susceptibility complies with EN55024:1998

Table 1. – TOE Physical Boundary

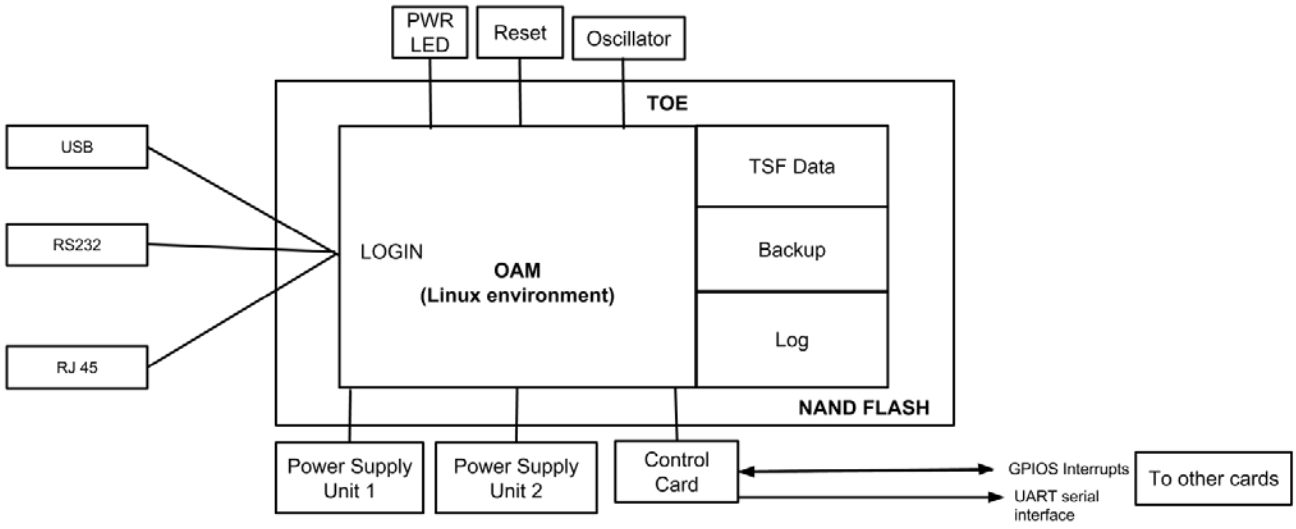

Figure .1- TOE & Its Physical Environments & Boundaries

The Login interface is used for logging in to the OAM. There are three physical ports through which the User connects to the OAM. The OAM operating system is based on the Linux environment. The TSF data, itsbackup and Logs are stored in the NAND flash memory of the system. 100 KB Log data is stored in a FIFO manner. An RTC is available in the control card. When the system is started for the first time, the time from the RTC is brought into the OAM oscillator. The oscillator of the OAM is now used for time stamping the events. The OAM communicates with the other cards through UART interface at 9600 baud rate. The GPIOS interrupts are brought in/sent to other cards via the control card.

1.5.2 LOGICAL BOUNDARY

This section outlines the boundaries of the security functionality of the TOE. The logical boundary of the TOE includes the security functionality described in the following sections.

The OAM Interface provides access to 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 access to all settings and configurations of OAM.

- **Systemuser**

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

- **Audituser**

An 'audituser' is a user who 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. Only 'superuser' can change audituser’s password.However on first login, audituser is forced to change the default password set by the superuser.

TSF	DESCRIPTION
Security Audit (FAU)	OAM’s auditable events are stored in the LOG memory maintained over the NAND Flash. It can be viewed through command line interface by the audituser when the system is accessed through SSH and can be viewed over serial ports(RS232 and USB) by the superuser.
Identification and Authentication(FIA)	The TOE requires • The superuser to access the system only through the serial ports (RS232 and USB). Superuser is required to provide username and password before any access to the system is granted. • The ‘systemusers’ (Users) to provide username and password before any access to the system is granted. • Audituser can only view and review the log data using SSH after providing correct username and password. No access is granted without authentication.
Security management (FMT)	OAM allows three types of users (Superuser, systemusers, audituser) with different roles. These users can access TOE through predefined ports of access only and then are allowed to make configuration changes as per their role. The TOE allows capability to manage TSF data and to perform management and maintenance functions.
Protection of the TSF (FPT)	The TOE provides reliable time stamps on audit logs maintained and a secure state (d) is observed in case of power failure and resetting.
TOE Access (FTA)	The TOE terminates the user access if an incorrect login or password is entered in a row and if a user tries to open multiple concurrent sessions.

Trusted path/Channels (FTP)	A trusted path is maintained by means of SSH which allows secure exchange of data between user and the TOE.
Cryptographic Support (FCS)	All passwords are stored in the system in hashed format using salted MD5 algorithm. An encrypted path is maintained between user and TOE using SSH making communication secure.

Table 1. - TOE Logical Boundaries

1.5.3 Non TOE CARDS

The OAM is also responsible for configuration management of some 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

2. CC CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CLAIMS

The following conformance claims are made for the TOE and ST:

CCv3.1 conformant. The TOE and ST are Common Criteria conformant to Common Criteria version 3.1.

Part 2 conformant. The ST is Common Criteria Part 2 conformant.

Part 3 conformant. The ST is Common Criteria Part 3 conformant.

Package conformant. The ST package is conformant to Evaluation Assurance Level (EAL) 1.

The TOE and ST does not conform to Protection Profiles.

3. SECURITY PROBLEM DEFINITION

The security problem to be addressed by the TOE is described by threats and policies that are common to OAM Module.

This chapter comprises of threats as T.threat, environmental threats as TE.environmental_threat, security objectives as O.objective, environmental security objectives as OE.environmental_objective, assumptions as A.assumption and policies as P.policy.

Note that the assumptions, threats, objectives, and policies are such that this TOE serves to address the Security Problems.

3.1 THREATS

The following threats are addressed by the TOE:

THREAT CODE	DESCRIPTION
T.PHYSICAL_ACCESS	The loss or theft of the device may give rise to loss of confidentiality of user data including credentials. These physical access threats involve attacks which attempt to access the device through external hardware ports.
T.REMOTE_ACCESS	An attacker is positioned on a remote communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the device or alter communications between the device and other endpoints in order to compromise the device.
T.TIME_STAMP	An authorized user will not be able to determine the sequence of events in the audit trail because the audit records are not correctly time-stamped.
T.MGMT_FLAWS	The users are not able to manage the security functions of the TOE, resulting in the potential security compromise of the TOE configuration.
T. DATA	An unauthorized user modifies or destroys TSF data on the TOE, which may cause the TOE to be inappropriately configured and user may gain inappropriate access to the TOE.
T.AUDIT	Actions performed by users may not be known to the audit reviewers due to actions not being recorded. The stored audit records may be modified or deleted by unauthorized users. Audit record making is stopped.

Table 3.1- Threats Addressed by the TOE

3.2 ENVIRONMENTAL THREATS

The following environmental threats are addressed by the TOE:

OBJECTIVE	DESCRIPTION
TE.LOCATE	Security critical parts of the TOE may be subject to physical attack which may compromise security.
TE.NO_HOSTILE	Compromise of IT assets may occur as a result of actions taken by careless, wilfully negligent or hostile administrators or other privileged users.

Table 3.2- Environmental Threats

3.3 ORGANIZATIONAL SECURITY POLICIES

These are the security policies followed by the organization:

POLICY	DESCRIPTION
P.PASS_STRENGTH	When the user changes the existing password he must follow following rules. Password Strength for acceptance >=14 Password strength for rejection <14 Calculating the Password strength Password strength = {Total length of the characters + 2 point for at least one lower case + 2 points for at least one upper case + 2 points for at least one number + 2 points for at least one special character}

Table 3.3- List of Organizational Security Policies

3.4 ASSUMPTIONS

This section contains assumptions regarding the security environment and the intended usage of the TOE:

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.

Table 3.1- Assumptions

4. SECURITY OBJECTIVES

4.1 SECURITY OBJECTIVES FOR TOE

Security Objectives of the system are listed below:

SECURITY OBJECTIVE CODE	DESCRIPTION
O.ACCESS_CONTROL	The TOE will restrict access to the users based on their roles (Superuser, Systemuser, Adituser) through correct mode of access.
O.AUDIT	Users must be accountable for their administrative actions on the TOE. Appropriate audit event logs are maintained. Audit log cannot be deleted or modified by anyone including superuser.
O.CFG_MANAGE	The TOE must provide services that allow effective management of its TSF and TSF-data.
O.ID_AUTH	The TOE must uniquely identify and authenticate the claimed identity of all administrative users before granting access.
O.SELF_PRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions. The protection involves TSF data protection.
O.SYS_MON	The TOE will provide capability to review audit data and make this data available for Adituser and Superuser.
O.TOE_ADMIN	The TOE will make sure that only the Superuser is able to configure critical functionalities (Modify Network settings, management of users) of the TOE.
O.LOGIN_EXPIRE	The TOE will terminate existing session if it is interrupted due to reasons such as time-out, power failure, resetting and link disconnection. It will also terminate existing SSH session after 6minutes of inactivity.
O.TIME	Time Stamps are provided for the TOE events and are recorded in Audit.

Table 4.1- Security Objectives of the TOE

4.2 SECURITY OBJECTIVES FOR OPERATIONAL ENVIRONMENT

Security objectives of the TOE are listed in the following points:

OBJECTIVE	DESCRIPTION
OE.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
OE.NO_HOSTILE	The administrators are not careless or willfully negligent and will abide by the administrator guidance.

Table 4.2- Security Objectives for Environment

5. EXTENDED COMPONENT DEFINITION

No extended components are required for this ST as all requirements are drawn from Common Criteria Parts 2 and 3.

6. SECURITY REQUIREMENTS

This section provides security functional and assurance requirements that must be satisfied by the TOE. These requirements consist of components from the CC Part 2 and Part 3.

6.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the security functional requirements (SFRs) for the TOE, organized by CC class as specified in CC part 2.

The following table identifies all the SFR's implemented by the TOE.

SECURITY FUNCTIONAL CLASS	SECURITY FUNCTIONAL COMPONENTS	DESCRIPTIONS
SECURITY AUDIT	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_STG.2	Guarantees of Audit Data Availability
	FAU_STG.4	Prevention of Audit Data Loss
IDENTIFICATION AND AUTHENTICATION	FIA_AFL.1	Authentication Failure Handling
	FIA_ATD.1	User Attribute Definition
	FIA_SOS.1	Verification of Secrets
	FIA_UAU.2	User Authentication Before Any Action
	FIA_UID.2	User Identification Before Any Action
SECURITY MANAGEMENT	FMT_MOF.1	Management of Security Functions Behavior
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
PROTECTION OF THE TSF	FPT_FLS.1	Failure with Preservation of Secure State
	FPT_STM.1	Reliable Timestamps
TOE ACCESS	FTA_MCS.1	Basic Limitation on Multiple Concurrent Sessions
	FTA_TSE.1	TOE Session Establishment
TRUSTED PATH/CHANNELS	FTP_TRP.1	Trusted Path
CRYPTOGRAPHIC SUPPORT	FCS_COP.1	Cryptographic Operations
	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.4	Cryptographic Key Destruction

Table 6.1 - Security Functional Requirements

6.1.1 CLASS FAU: SECURITY AUDIT

6.1.1.1 Security Audit Data Generation (FAU_GEN)

FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
Dependencies:	FPT_STM.1 Reliable time stamps

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: • Start-up and shutdown of the audit functions; • All auditable events for the **[not specified]** level of audit; and • **[Each login attempt by superuser, systemuserand adduser(both successful and unsuccessful), add of user, deletion of user, password change, exit].**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: • Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and • For each audit event type, based on the auditable event definitions of the functional components included in the ST, **in the section 7.1**].

FAU_GEN.2 User identity association

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification

FAU_GEN.2 User identity association

FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.2 Security Audit Review (FAU_SAR)

FAU_SAR.1 Audit review

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation

FAU_SAR.1.1	The TSF shall provide **["Superuser", "Adituser"]** with the capability to read **[following audit records :** **Superuser: User authentication related audit records (successful and unsuccessful login attempts by superuser and systemuser).** **Adituser: Complete logs with all audit records (successful and unsuccessful login attempts by superuser,systemuserand adituser,addition of user, deletion of user, password change, exit)]** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.3 Security Audit Event Storage (FAU_STG)

FAU_STG.2 Guarantees of audit data availability

Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation

FAU_STG.2.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.2.2	The TSF shall be able to **[prevent]** unauthorized modifications to the stored audit records in the audit trail.
FAU_STG.2.3	The TSF shall ensure that **[audit record in 100 KB files making a total of 10 MB]** stored audit records will be maintained when the following conditions occur: **[audit storage exhaustion]**.

FAU_STG.4 Prevention of audit data loss

Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage

FAU_STG.4.1	The TSF shall **[overwrite the oldest stored audit records]** and **[the oldest log file is deleted in FIFO manner]** if the audit trail is full.

6.1.2 CLASS FIA: IDENTIFICATION AND AUTHENTICATION

6.1.2.1 Authentication failures (FIA_AFL)

FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication

FIA_AFL.1.1	The TSF shall detect when **[[3/5 or 10]]** unsuccessful authentication attempts occur related to **[wrong user name or passwordthrough serial port(USB/RS232) / incorrect username or correct username and incorrect password through RJ45]**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been **[met]**, the TSF shall: **[In case of USB or RS232:** • **Terminate the login screen.** • **Brings superuser/systemuser back to the home screen.** **In case of RJ45** • **Terminate the systemuser's active session.** • **Terminate the audit user's active session.]**

6.1.2.2 User attribute definition (FIA_ATD)

FIA_ATD.1 User attribute definition

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: **[User-name, Passwords]**.

6.1.2.3 Specification of secrets (FIA_SOS)

FIA_SOS.1 Verification of secrets

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet **[the password quality]**.

6.1.2.4 USER AUTHENTICATION (FIA_UAU)

FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies:	FIA_UID.1 Timing of identification

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF - mediated actions on behalf of that user.

6.1.2.5 USER IDENTIFICATION (FIA_UID)

FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification

Dependencies:	No dependencies.

FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 CLASS FMT: SECURITY MANAGEMENT

6.1.3.1 Management of functions in TSF (FMT_MOF)

FMT_MOF.1 Management of security functions behavior

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

-FMT_MOF.1.1	The TSF shall restrict the ability to **[modify the behavior of]**the functions **[listed below:** **1. For systemuser:** • **Log-in in the system through Ethernet port over SSH and through USB/RS232 port.** • **View system settings.** • **Change the SNMP Configuration i.e. Target IP Address, Target Port and Target Community.** • **Change self-password only after verifying its old password.** **2.For adituser:** • **View and review the logs by accessing the system through SSH.** • **Change self password (Only on first time login).** **3. For superuser:** • **Log-in in the system through USB/RS232 port** • **View system settings.** • **Change the network configuration i.e. IP Address, Subnet Mask, Gateway and DNS Addresses.** • **Enable / Disable SNMP traps** • **Change the SNMP Configuration, i.e., SNMP Read**

	Community, SNMP Write Community,Target IP Address, Target Port and Target Community • **See the users registered in the system except Adituser.** • **Change self-password** • **Change the password of 'adituser'.** • **Add a systemuser, delete a systemuser** • **View Audit Records stored in the system's non-volatile memory.** • **Initiate Ping command to check network connectivity]** to**[1. Systemuser, 2. Adituser, 3. Superuser]**

6.1.3.2 Management of TSF data (FMT_MTD)

FMT_MTD.1 Management of TSF data

Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1	The TSF shall restrict the ability to **[change_default, modify, delete,query, [create]]** the **[TSF data listed below:** **1. For systemuser** • **Self-password (change_default,modify)** • **SNMP Target IP Address (change_default, modify,query)** • **SNMP Target Port (change_default, modify,query)** • **SNMP Target Community (change_default, modify,query)** • **Version (query)** • **SNMP Read Community (query)** • **SNMP Write Community (query)** **2. For superuser** • **Self-password (change_default, modify)** • **Adituser password (change_default, modify)** • **Systemuser password (create, delete)** • **Systemuser username (create, query, delete)** • **Superuser username (query)** • **Network IP Address (change_default, modify,**

	query) • **Subnet Mask (change_default, modify, query)** • **Gateway (change_default, modify, query)** • **DNS Addresses (change_default, modify, query)** • **SNMP Status(Enable/Disable) (change_default, modify, query)** • **SNMP Read Community (change_default, modify, query)** • **SNMP Write Community (change_default, modify, query)** • **SNMP Target IP Address (change_default, modify, query)** • **SNMP Target Port (change_default, modify, query)** • **SNMP Target Community (change_default, modify, query)** • **Version (query)** • **Audit data(query)** **3. For Audit User** • **Audit data(query)** • **Change Self-password (Only on first time login)]** to**[1. Systemuser, 2. Superuser, 3. Audituser]**

6.1.3.3 Specification of Management Functions (FMT_SMF)

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1	The TSF shall be capable of performing the following managementfunctions: **[** • **Create and delete systemusers.** • **Change passwords of superusers, systemusers, auditusers.** • **Change the network configuration i.e. IP Address, Subnet Mask, Gateway and DNS Addresses.** • **Enable / Disable SNMP traps.** • **Change the SNMP Configuration, i.e., SNMP Read Community, SNMP Write Community,Target IP Address, Target Port and Target Community** • **See the all users (except Audituser) registered in the**

	system. • **View system settings.** • **View Audit Records stored in the system's non-volatile memory.** • **Initiate Ping command to check network connectivity** **]**

6.1.3.4 Security management roles (FMT_SMR)

FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FMT_SMR.1.1	The TSF shall maintain the roles **[Superuser, Systemuser, Adduituser]**
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.4 CLASS FPT: PROTECTION OF THE TSF

6.1.4.1 Fail secure (FPT_FLS)

FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: **[power failure, resetting module]** as it continues to run in the same state.

6.1.4.4 Time stamps (FPT_STM)

FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

6.1.5 CLASS FTA: TOE ACCESS

6.1.5.1 Limitation on multiple concurrent sessions (FTA_MCS)

FTA_MCS.1 Basic limitation on multiple concurrent sessions

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FTA_MCS.1.1	The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.
FTA_MCS.1.2	The TSF shall enforce, by default, a limit of **[one]** session per user.

6.1.5.2 TOE session establishment (FTA_TSE)

FTA_TSE.1 TOE session establishment

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [**1. incorrect login credentials :(username and password) 2. Incompatible mode (like Ethernet, serial port) of access]**.

6.1.6 CLASS FTP: TRUSTED PATH/CHANNELS

6.1.6.1 Trusted path (FTP_TRP)

FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FTP_TRP.1.1	The TSF shall provide a communication path between itself and **[local and remote]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[Disclosing].**
FTP_TRP.1.2	The TSF shall permit **[local users(USB and RS232 ports) &remote users(Ethernet port using SSH)]** to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for **[initial user authentication, and all further communications between user to OAM]**.

6.1.7 CLASS FCS: CRYPTOGRAPHIC SUPPORT

6.1.7.1 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1 FCS_CKM.4

FCS_COP.1.1 **MD5**	The TSF shall perform **[hashing]** in accordance with a specified cryptographic algorithm **[salted MD-5]**and cryptographic key sizes **[32 hexadecimal digits]**that meet the following **[RFC1321].**

FCS_COP.1.1 **SSH**	The TSF shall perform **[encryption]** in accordance with a specified cryptographic algorithm **[SSHv2]**and cryptographic key sizes **[2048 bits]**that meet the following **[RFC 4251, RFC 4252, RFC 4253, RFC 4254].**

6.1.7.2 Cryptographic key management
FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	FCS_CKM.4 Cryptographic key destruction FCS_COP.1 Cryptographic operation

FCS_CKM.1.1 **SSH**	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[SSHv2]** and specified cryptographic key sizes **[2048 bits]**.

FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	FCS_CKM.1

FCS_CKM.4.1 **SSH**	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[overwrite]** that meets the following: **[None]**.

6.2 TOE SECURITY ASSURANCE REQUIREMENT

The TOE meets the security assurance requirements for EAL1. The following table is the summary for the requirements:

ASSURANCE CLASS	ASSURANCE COMPONENT
ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
AGD: Guidance documents	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1 Labeling of the TOE
	ALC_CMS.1 TOE CM Coverage
ADV: Development document	ADV_FSP.1 Functional Specification
ATE: Tests	ATE_IND.1 Independence Testing – Conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability Survey

Table 6.1- Security Assurance Requirements

7. TOE SUMMARY SPECIFICATION

This section provides summary information on how the security requirements are met by the TOE. The objective is to give a high-level view of the security requirements satisfied by the TOE.

7.1 SECURITY AUDIT

7.1.1 AUDIT EVENTS

The OAM Module creates and stores audit records for the following events:

- **For Superuser**
  - An entry in the LOG for every successful login attempt of the superuser (over USB/RS232 serial port).
  - An entry in the LOG for every 3 unsuccessful login attempts of the superuser (over USB/RS232 serial port).
  - Whenever a systemuser is added to the system successfully.
  - When a systemuser is deleted successfully.
  - Change of password of audituser by superuser successfully.
  - When self-password is changed by superuser successfully.
  - Exit successfully.
- **For systemuser**
  - An entry in the LOG for every successful attempt of the systemuser.
  - An entry in the LOG for every unsuccessful attempt of the systemuser(when connected through RJ45 port).
  - An entry in the LOG for every 3 unsuccessful attempt of the systemuser(when connected through USB/RS232).
  - Reaching maximum number of 5/10 attempts allowed for the systemuserafter passing incorrect/correct username (when connected through RJ45 port) after which the active SSH client session is made inactive. User is required to establish a new session.
  - Change of self-passwordsuccessfully.
  - Exit successfully.
- **Audit user**
  - An entry in the LOG for every successful attempt of the audituser.
  - An entry in the LOG for every unsuccessful attempt of the audituser (when connected through SSH).

- Change self password (Only on first time login)

7.1.2 AUDIT RECORDS

Following fields are available in LOG records:
[Date and Time System name Event Type Event information]
Date and Time:

Format- [Month Date Time]

System name:

MXV6-OAM

Event type:

Information type shows LOG event is associated with which section of OAM or OAM environment.

Ex-*Sep 27 17:17:13 MXV6-OAM* **auth.info***login[1029]: root login on 'ttyGS0'*

Event information:

Event information is the data associated with the event. Event information carries a message that identifies which audit event is performed by which user.

Following dataisalso stored in event information:

- Username (if identified)
- IP address and MAC Address of remote user (If connected through RJ45 port)
- Physical port of local user (If connected through USB/RS232 port)

7.1.3AUDIT STORAGE

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.

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.

7.1.4AUDIT VIEW

“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 audit user only super user can view filtered LOGS through CLI interface.

Superuser can view user authentication related audit records (successful and unsuccessful login attempts by superuser, systemuser and audituser).Audituser can view complete logs with all audit records (successful and unsuccessful login attempts by superuser, systemuser and audituser, addition of user, deletion of user, password change, exit)

The logs areread only and cannot be deleted or modified by any user including the “superuser” and the “audituser”.

The Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1
- FAU_GEN.2
- FAU_SAR.1
- FAU_STG.2
- FAU_STG.4

7.2 IDENTIFICATION AND AUTHENTICATION

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" and "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 MD-5 algorithm.

No user is allowed to perform any function before identification and authentication. Every user is required to provide username and password. System interacts with the user using a login screen and request to enter a username and a password. The username entered at the username prompt is reflected to the screen, but no feedback is provided while the password entry is being made by the user. As the Enter key is pressed, system verifies this data. The username is compared. The password is hashed and compared to the stored value, and success/failure is indicated. In case of a failure the user is not told which of the two, the entered password or user id is wrong. Other than this a user is not allowed access if a wrong access port is used. Following are correct ports of access as per the user role:

Audituser – using RJ45 port

Superuser – using serial ports (USB/RS232)

Systemusers – using USB/RS232 and RJ45 ports.

7.2.1 USERNAME AND PASSWORD

Only superuser can change password of audituser and its own self-password.

Default passwords are assigned bysuperuser during systemuser creation and these passwords do not fulfill password strength requirements. Systemusers and audituser are forced to change the default password to a secure password of strength >=14. Locally stored authentication data is a case-sensitive value comprises of any combination of upper and lower case letters, numbers and special character (from the set "!" "@" "#" "$" "%" "^" "&" "*" "," ";").

Username criteria

Username length (minimum): 8 characters

Username length (maximum): 30 characters

Password strength criteria

The strength of the password is calculated in the following manner:-

Password Strength for acceptance >= 14

Password strength for rejection < 14

Calculating the Password strength

Password strength = { Total length of the characters

+ 2 point for at least one lower case

+ 2 points for at least one upper case

+ 2 points for at least one number

+ 2 points for at least one special character }

The maximum number of characters allowed in a password are 30 characters.

7.2.2 IDENTIFICATION AND AUTHENTICATION FAILURE

The TSF detects when unsuccessful authentication attempts occur related to wrong user names or passwords. When unsuccessful authentication attempts are made through:

- Serial Port (USB/RS232) for superuser and systemuser

  After 3 unsuccessful attempts present login screen is terminated and user is brought back to the home screen.

- Ethernet (RJ45) for systemuser and audituser

  After 5/10 unsuccessful attempts after passing incorrect/correct usernamethe active SSH client session is made inactive. User is required to establish a new session.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1
- FIA_ATD.1
- FIA_SOS.1
- FIA_UAU.2
- FIA_UID.2

7.3 SECURITY MANAGEMENT

There are three default user roles (superuser, systemuser, adituser) available in the TOE and these are associated with the users by the TOE itself. The Authorized Administrator (Superuser) is responsible for managing (creation, deletion) user accounts.User accounts in the TOE have the following attributes: user identity (user name), authentication data (password) and type of user ("Superuser", "Systemuser" "Adituser").

The TOE provides systemuser access either through the physical serial port (USB/RS232) or remotely over the Trusted Path using the SSH protocol. Users are required to provide unique identification (username) and authentication data (passwords) before any access to the system is granted. A password is assigned to each user before allowed to log into the system. Password is stored as salted hashed data.

7.3.1 MANAGEMENT ROLES

The functional access of the users have been defined below:

Superuser:

- Log-in in the system through serial port (USB/RS232)
- View system settings.
- Change the network configuration i.e. IP Address, Subnet Mask, Gateway and DNS Addresses.
- Enable / Disable SNMP traps
- Change the SNMP Configuration, i.e., SNMP Read Community, SNMP Write Community, Target IP Address, Target Port and Target Community
- See the users registered in the system except Adituser.
- Change self-password
- Change the password of 'adituser'.
- Add a systemuser, delete a systemuser.
- View Audit Records stored in the system’s non-volatile memory.
- Initiate Ping command to check network connectivity.

Systemuser:

- Log-in in the system through Ethernet port over SSH and through serial port (USB/RS232).
- View system settings. Configure, manage and control the system.
- Change the SNMP Configuration i.e. Target IP Address, Target Port and Target Community.
- Change self-password only after verifying its old password.

Adituser:

- View and review the logs by accessing the system through SSH.
- Change self password (Only on first time login)

The TSF restricts the ability to modify the behavior of these functions.

7.3.2 TSF DATA

Only superuser and systemusers take part in management functions.
Users have access to TSF data as per their role as given below:

Systemuser:

- Self-password (change_default,modify)
- SNMP Target IP Address (change_default, modify, query)
- SNMP Target Port (change_default, modify, query)
- SNMP Target Community (change_default, modify, query)
- Version (query)
- SNMP Read Community (query)
- SNMP Write Community (query)

Superuser:

- Self-password (change_default, modify)
- Adduituser password (change_default, modify)
- Systemuser password (create, delete)
- Systemuser username (create, query, delete)
- Network IP Address (change_default, modify, query)
- Subnet Mask (change_default, modify, query)
- Gateway (change_default, modify, query)
- DNS Addresses (change_default, modify, query)
- SNMP Status(Enable/Disable) (change_default, modify, query)
- SNMP Read Community (change_default, modify, query)
- SNMP Write Community (change_default, modify, query)
- SNMP Target IP Address (change_default, modify, query)
- SNMP Target Port (change_default, modify, query)
- SNMP Target Community (change_default, modify, query)
- Version (query)
- Audit data(query)

Audit User:

- Audit data(query)
- Change Self-password [Only on first time login].

The Security Management function is designed to satisfy the following security functional requirements:

- FMT_MOF.1
- FMT_MTD.1

- FMT_SMF.1
- FMT_SMR.1

7.4 PROTECTION OF TSF

7.4.1 RTC (REAL TIME CLOCK)

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. 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 TSF data includes system configuration data, Username and Password of Superuser, Systemuser,Audituser.All users are able to query the current version of the TOE firmware/software.

7.4.2 SECURE STATE IN CASE OF FAILURE

The system closes the existing sessions immediately if it is interrupted due to power failure and resetting.
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. Secure state is defined as the state after last correctly executed command.
The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_FLS.1
- FPT_STM.1

7.5 TOE ACCESS

Before establishing the session, a welcome banner is shown along with system configuration when session is established through serial port (USB/RS232).
After the username has been given a welcome banner is shown along with system configuration when session is established through SSH through Ethernet port (RJ45).
User sessions can be terminated by users. The sessions through SSH expire after 6 minutes.The TSF enforces, by default, a limit of 1session per user.The system closes the existing sessions immediately if it is interrupted due to reasons such as time-out, power failure, resettingand link disconnection.

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 RJ45 port

Superuser – using serial port (USB/RS232)

Systemusers – using serial port (USB/RS232) and Ethernet port (RJ45).

If an unsuccessful attempt is made by systemuser5/10 times after passing incorrect/correct username over SSH, his terminal goes into inactive state. He needs to close the third party software and restart it.

If an unsuccessful attempt is made by systemuser or superuser 3 times over serial port (USB/RS232), he will be brought back to the login screen.

The TOE Access function is designed to satisfy the following security functional requirements:

- FTA_MCS.1
- FTA_TSE.1

7.6 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 and audituser). Serial port (USB/RS232), a physical connection port can be used by both superuser and systemuser to access the TOE.

The Trusted Path/Channels function is designed to satisfy the following security functional requirements:

- FTP_TRP.1

7.7 CRYPTOGRAPHIC SUPPORT

The TOE uses salted MD-5 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.

The cryptographic support is designed to satisfy the following security functional requirements:

- FCS_COP.1
- FCS_CKM.1
- FCS_CKM.4

8. CORRESPONDENCE AND RATIONALE

8.1 TOE SECURITY OBJECTIVES RATIONALE

The following table maps threats to the security objectives.

	T.PHYSICAL_ACCESS	T.REMOTE_ACCESS	T.TIME_STAMP	T.MGMT_FLAWS	T.DATA	T.AUDIT	A.TRAIN_AUDIT	P.PASS_STRENGTH	
O.ACCESS_CONTROL	X	X			X				The objective ensures that users need to connect through correct mode of access and after connection user roles limit their access to TSF and TSF data.
O.AUDIT			X			X			The objective ensures that audit generation is never stopped and that audit data cannot be deleted and modified. Time stamp on audit records ensures that events can be reviewed correctly.
O.CFG_MANAGE				X					Objective ensures that TSF and TSF data can be effectively managed to minimize management flaws.
O.ID_AUTH	X	X			X			X	Objective ensures that identification and authentication is required for physical and remote mode of access. Username and password (salted MD5 hashed) are stored as TSF data. Password needs to follow password strength policy which is enforced by the TOE.

O.SELF_PRO	X	X			X				Objective ensures that TSF and TSF data are protected through physical and remote access.
O.SYS_MON						X	X		Objective ensures that audit data is monitored by audit users and can be accessed by superuser if required.
O.TOE_ADMIN		X							Objective ensures that users accessing TOE are created and deletedby the superuser (administrator) only.
O.LOGIN_EXPIRE	X	X							Objective ensures that both physical and remote sessions will terminate in case of time-out, power failure, resettingand link disconnection. Remote session can also terminate after 6 minutes of inactivity.
O.TIME			X						Objective ensures that time stamps are provided for TOE events and are recorded in audit.

8.2 ENVIRONMENTAL SECURITY OBJECTIVES RATIONALE

The following table maps the environmental threats and assumptions to environmental objectives and organizational policies.

	TE.LOCATE	TE.NO_HOSTILE	A.NO_HOSTILE	A.LOCATE	A.LOG_OUT	
OE.LOCATE	X			X		Environmental objective ensures that TOE is located within controlled environment preventing

						unauthorized access.
OE.NO_HOSTILE		X	X		X	Environmental objective ensures that TOE users are responsible and follow user management ethics to prevent TOE from any damage. User should logout before leaving system unattended.

8.3 DEPENDENCY RATIONALE

The following table shows the dependencies of the SFR's.

SFR	DEPENDENCIES	RATIONALE
FAU_GEN.1	FPT_STM.1	Included
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Included Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_STG.2	FAU_GEN.1	Included
FAU_STG.4	FAU_STG.1	Included
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 included (Hierarchical to FIA_UAU.1)
FIA_ATD.1	-	No dependency
FIA_SOS.1	-	No dependency
FIA_UAU.2	FIA_UID.1	FIA_UID.2 included (Hierarchical to FIA_UID.1)
FIA_UID.2	-	No dependency
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Included Included
FMT_MTD.1	FMT_SMR.1	Included

	FMT_SMF.1	Included
FMT_SMF.1	-	No dependency
FMT_SMR.1	FIA_UID.1	FIA_UID.2 included (Hierarchical to FIA_UID.1)
FPT_FLS.1	-	No dependency
FPT_STM.1	-	No dependency
FTA_MCS.1	FIA_UID.1	FIA_UID.2 included (Hierarchical to FIA_UID.1)
FTA_TSE.1	-	No dependency
FTP_TRP.1	-	No dependency
FCS_COP.1	FCS_CKM.1 FCS_CKM.4	Included Included
FCS_CKM.1	FCS_COP.1 FCS_CKM.4	Included Included
FCS_CKM.4	FCS_CKM.1	Included

8.4 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

	O.ACCESS_CONTROL	O.AUDIT	O.CFG_MANAGE	O.ID_AUTH	O.SELF_PRO	O.SYS_MON	O.TOE_ADMIN	O.LOGIN_EXPIRE	O.TIME
FAU_GEN.1		X							
FAU_GEN.2		X				X			
FAU_SAR.1		X				X			
FAU_STG.2		X				X			
FAU_STG.4		X	X			X			
FIA_AFL.1				X					
FIA_ATD.1	X			X			X		
FIA_SOS.1				X					
FIA_UAU.2				X					
FIA_UID.2				X					
FMT_MOF.1	X		X		X				
FMT_MTD.1	X		X		X		X		
FMT_SMF.1	X		X						
FMT_SMR.1	X		X		X				
FPT_FLS.1					X				
FPT_STM.1		X						X	X
FTA_MCS.1				X					
FTA_TSE.1				X					
FTP_TRP.1					X				
FCS_COP.1				X	X				

FCS_CKM.1					X				
FCS_CKM.4					X				