Security Target
For
C-DOT Compact Encryption Module (CEM)
Running
CEML1_1_1.x_1 Software

Released on: 26-June-2020

Any hard copy unless authorized or a soft copy in a directory other than the central repository is an Uncontrolled Copy.

This hard copy of the document is a Controlled Copy only when signed by an authorized signatory.

Issued to: _____

Signature and Date

CENTRE FOR DEVELOPMENT OF TELEMATICS
MANDI ROAD, MEHRAULI, NEW DELHI 110030, INDIA
ELECTRONICS CITY (PHASE I), HOSUR ROAD, BANGALORE 560100, INDIA

Approval Block

Organizational responsibility	Name	Signature	Date
PMT Coordinator / GL PI	Prashant Chugh		

Revision Chart

This document replaces

Document code : CDOT-FT-ST-CEM-v01d01
Document name : Security Target for C-DOT Compact Encryption Module (CEM) running CEML1_1_1.x_1 software

Version/ Draft no.	Submitted on	Summary of changes	Reference Sections	Reason of change
v01d01	17.06.2020	NA	All	First Draft
v01d02	26.06.2020	All the sections	All	Review feedback

Participation

This document has been authored/modified by

CEM Team of FT Group
C-DOT Delhi

Table of Contents

List of Tables

List of Figures

1. ST INTRODUCTION

1.1 ST and TOE Reference Identification

ST reference	Security Target for C-DOT Compact Encryption Module (CEM) running CEML1_1_1_1.x_1 Software
ST Version	Version 1.0
Publication Date	26-Jun-2020
ST Author	CEM Team, C-DOT Delhi
Developer of the TOE	C-DOT
TOE Reference	C-DOT Compact Encryption Module (CEM) running CEML1_1_1.x_1 software
TOE Hardware Models	CEM with ARMv7 based processor
TOE Software Version	CEML1_1_1.x_1
Keywords	IP, Encryption, Cryptography

1.2 Acronyms

AAA	Authentication, Authorization, and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Compact Encryption Module
CLI	Command Line Interface
CM	Configuration Management
CTR	Counter Mode
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FM	Fault Management
FTP	File Transfer Protocol
HA	High Availability
HMAC-SHA	Hash Message Authentication Code - Secure Hash Algorithm
I/O	Input/Output
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
NTP	Network Time Protocol
PP	Protection Profile

RADIUS	Remote Authentication Dial In User Service
RSA	Rivest-Shamir-Adleman Algorithm
SA	Security Association
SF	Security Functions
SFP	Security Functional Policy
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
SPI	Security Parameter Index
SSH	Secure Shell
SSHv2	Secure Shell Version 2
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

Table 1: Acronyms List

1.3 TOE Overview

1.3.1 Usage and major features of the TOE

The TOE is CEML1_1_1.x_1 software running on processor based IP encryption module called Compact Encryption Module (CEM). CEM is 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 keys derivations and authentications.

1.3.2 Major security features of the TOE

The TOE is comprised of several security features which consist of following security functionalities -

- User Data Protection Function
- Identification and Authentication Function
- Security Management Function
- Audit Function
- TOE Access Function
- Protection of TOE Security Functions (TSF)
- Cryptographic Support

1.4 TOE Description

TOE is software running on CEM board which is a Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 CPU. The board is mainly designed to run software-based encryption algorithms adding security to the outgoing IP packets at IP layer. The board is designed to support many other security features which are required in an IP Encryptor. CEM shall receive 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 work as L2 and L3 encryptor. It provides standard compliant software and hardware interfaces for interoperability.

C-DOT CEM is powered through 12V DC supply. AC to DC converter shall be provided with the packaging of the module. The hardware and software functionalities run on the platform are independent on the AC /DC supplies.

CEM Configuration

In IP encryptor configuration, when two CEM devices want to engage in secure communication, they set up a secure path between themselves that may traverse across many insecure intermediate systems (through Internet). To accomplish this, they perform (at least) the following tasks:
They must agree on a set of security protocols to use so that each one sends data in a format the other can understand.
They must decide on a specific encryption algorithm to use in encoding data.
They must exchange keys that are used to "unlock" data that has been cryptographically encoded.
Once this background work is completed, each CEM device shall use the protocols, methods, and keys previously agreed upon to encode data and send it across the network.

The actual data traffic is encrypted /decrypted in IPsec layer and never travels to higher layers, while IPsec control (IKEv2) messages are encrypted/decrypted at upper layer only. The encryption for data is done in IPsec module of kernel while encryption of IKEv2 messages are done at application layer.

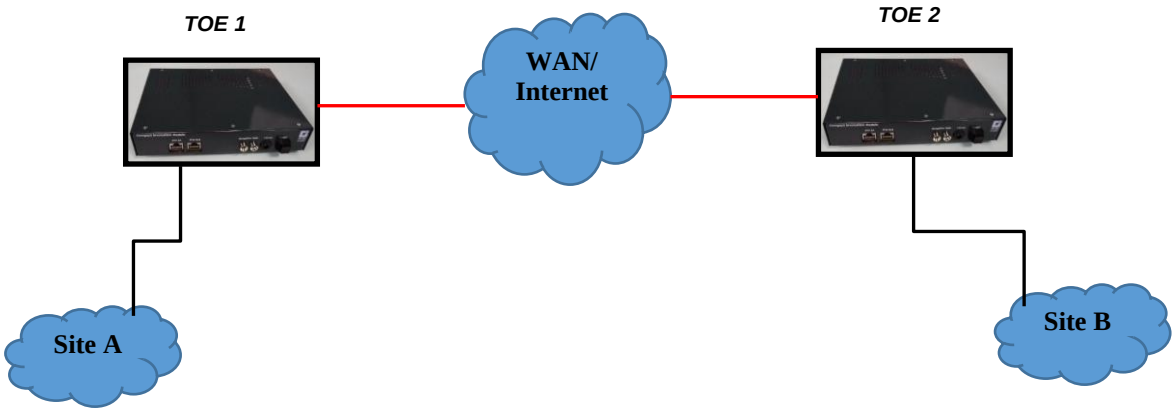


Figure 1: Deployment scenario for CEM

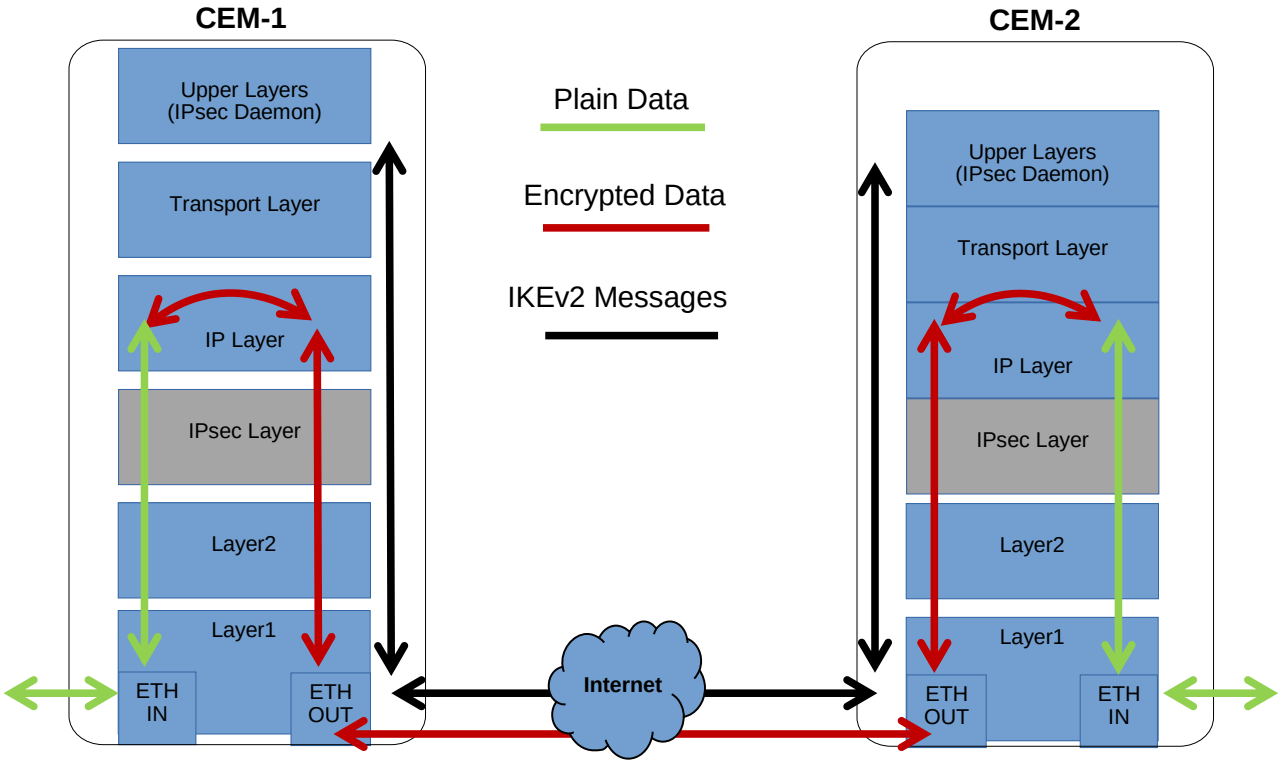


Figure 2: Data flow diagram of IPsec in CEM system

Following are the parts/items shall be delivered to the TOE user-

S.N.	Part/Item Description	Delivery method
1.	C-DOT CEM Hardware along with power adaptor	Packed in box and shipped by post
2.	CEML1_1_1.x_1 Software with Software Release Note	In a CD and shipped by post
3.	Installation Manual-v01	In a CD and shipped by post
4.	User Manual-v01	In a CD and shipped by post

1.4.1 TOE Type

The TOE is encryptor software running on Marvell based Armada 380 System on Chip with ARMv7 Cortex-A9 providing cryptographic functions like encryption, authentication, integrity etc.

1.5 TOE Boundaries

The TOE physical and logical boundaries are as follows-

1.5.1 Physical Boundary

The TOE is CEML1_1_1.x_1 software running within the physical boundary of CEM board which is a single card platform having network data and management interfaces. The TOE can be configured through Command Line Interface (CLI) over SSH connection. The date and time of the device can be synchronized with a NTP server. The user authentication for remote login can be done using external RADIUS server. The system logs are usually kept in the local memory of the device, while the same can also be transferred to an external syslog server as and when required. As per the configurations and functionalities of the CEM, it shall have following software applications running on it -

1) Module responsible for implementing IPsec
2) CLI (Command Line Interface)
3) SNMP agent
4) Health monitoring process
5) Module responsible for implementing QKD-CEM interface for key exchange.
6) Module to synchronize with NTP server.
7) Module for user authentication for remote login can also be done through external RADIUS server.
8) Module for system logs can be transferred to external syslog server from time to time.

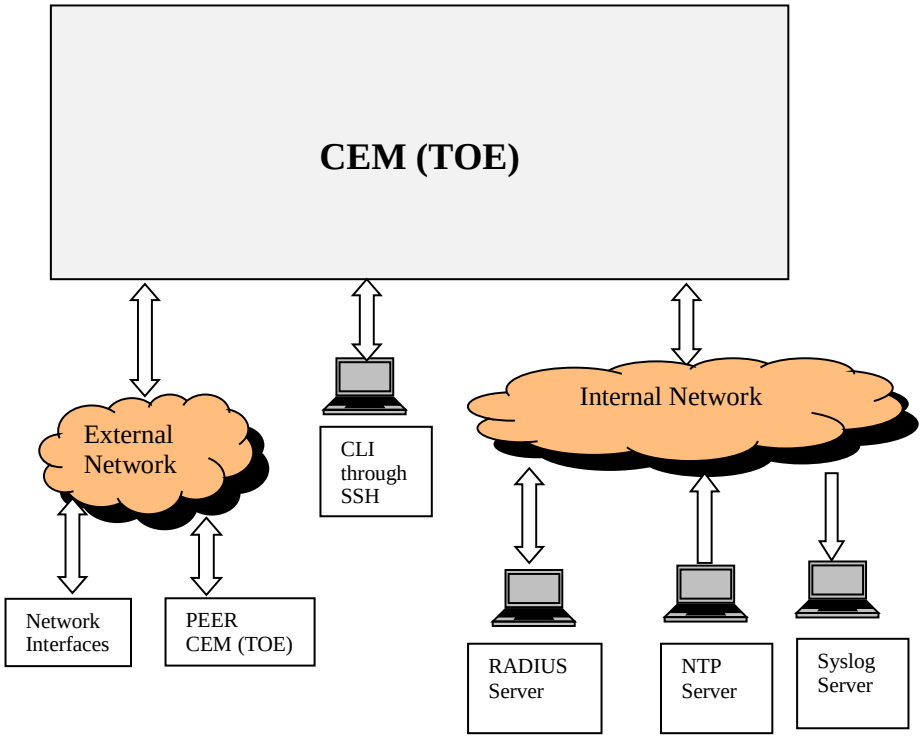


Figure 3: TOE Architecture Block Diagram

1.5.2 Logical Boundaries

TOE provides following security features:

- User Data Protection
- Identification and Authentication
- Security Management
- Audit
- TOE Access Function
- Protection of TOE Security Functions (TSF)
- Cryptographic Support

1.5.2.1 User Data Protection

The TOE receives the data on ETH-IN port from private network and uses IPsec security policies to encrypt and send user data on ETH-OUT port to peer TOE as defined in TOE IPsec policies. The peer TOE decrypts the received ESP packet and check for authenticity as defined in its own policies. Then peer TOE sends the IP packet to its destination address present in its private sub-network.

1.5.2.2 Identification and Authentication

The TOE performs identification and authentication of TOE users before granting access to the system by providing user name and password. The TOE authenticates users through its local database (user name, passwords) or through a remote RADIUS authentication server (external authentication server is outside the scope of TOE).

Applications exchanging information with TOE through management interface needs to be successfully authenticated prior to any exchange via SSH.

1.5.2.3 Security Management

The CEM is configured and managed through a Command Line Interface (CLI) protected by SSH. The TOE users are Operator, System-Admin and Root-System. The Operator user can only view different settings and attributes of the system. The TOE allows authorized System-Admin to create, modify and delete configurations and even authorized to modify/set the system date and time. The Root-System can perform all the configurations done by System-Admin and user management functions, including creating and deleting users of TOE.

1.5.2.4 Audit

The TOE maintains a syslog where TOE auditable events are stored which can be sent to external log server (external syslog server is outside the scope of TOE). The audit events include authentication and configuration change activities. User name, date and time associated with each event is maintained. The audit syslog can only be viewed by Root-System and System-Admin user. It also maintains the log of various events related to IPsec functioning.

1.5.2.5 TOE Access Function

TOE access requires authentication before any administrative action. Administrative access is restricted to specific functions related to user account management and configuration of TOE. Inactive sessions both local and remote can be terminated by TOE after a time-period which can be configured by an administrator. Once a session is terminated the user is required to re-establish a new session.

1.5.2.6 Protection of TOE Security Functions (TSF)

The TOE protects its security functions through various mechanisms. The TOE performs self-test during start-up and brings the system to a secure state. In case of Self-Test failure, TOE remains in secure state. The TOE provides accurate date and time from internal clock. The system clock can also be synchronized with an NTP server (NTP server is outside the scope of TOE). The TOE IPsec functionality operations are controlled by authentication mechanism thus protecting any accidental or intentional interference by others.

1.5.2.7 Cryptographic Support (TSF)

The TOE supports cryptography for secure communication, protection of information on Management interface and IPsec functionalities. The TOE uses SSHv2 protocol for allowing remote or local clients for logging through CLI. SSHv2 provides encryption methods to create a secure channel of communication. SSHv2 encrypts the data flowing through the session with the help of a shared secret key. IPsec provides confidentiality and authentication for site-to-site communication over unsecure network (i.e. Internet).

1.5.3 Summary of items out of the TOE boundary

The following items are out of the scope of TOE / evaluation:

- All hardware
- External servers (NTP, RADIUS, SNMP, Syslog servers)
- Use of the serial port
- Use of SNMP
- Telnet is a filtered service. Use of Telnet by default it is disabled.
- FTP is a filtered service. Use of FTP by default it is disabled.

2. CC CONFORMANCE

CC identification-

[CC1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model April 2017 Version 3.1 Revision 5 Final CCMB-2017-04-001

[CC2] Common Criteria for Information Technology Security Evaluation Part 2: Introduction and general model April 2017 Version 3.1 Revision 5 Final CCMB-2017-04-002

CC Part 2 (Version 3.1, Revision 5, April 2017) extended due to the use of the components FPT_TST_EXT, FCS_SSHC_EXT and FCS_SSHS_EXT

[CC3] Common Criteria for Information Technology Security Evaluation Part 3: Introduction and general model April 2017 Version 3.1 Revision 5 Final CCMB-2017-04-003

[CEM] Common Methodology for Information Technology Security Evaluation, April 2017 Version 3.1, Revision 5, Final CCMB-2017-04-004.

This ST document does not claim conformance to any PPs.

This ST document and the TOE described is CC Part 2, CC Part 3 (version 3.1 Revision 5) conformant and meet EAL 3 certification requirements.

This ST document and the TOE described is also conformant to the following extended components -
CC Part 2 (version 3.1 Revision 5) extended due to the use of the components FPT_TST_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT and FCS_IPSEC_EXT

3. SECURITY PROBLEM DEFINITION

Security Problem Definition describes-

- Assets of TOE.
- Assumptions related to TOE's operational environment to provide security functionality.
- Threats countered by TOE to protect itself and the environment in which it operates.
- Organizational policies that TOE must enforce.

3.1 Assets

3.1.1 AST.DATA

The primary asset is the data communications made between 2 parties (i.e. end points).

3.1.2 AST.TSF_DATA

Secondary assets are TOE configuration files and cryptographic keys used for authentication.

3.2 Assumptions

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

3.2.1 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.

Table 2: TOE Physical Assumption

3.2.2 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.

Table 3: TOE Personal Assumption

3.2.3 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

Assumption (Operations)	Assumption Description
	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 platform 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 for particular types of network devices.

Table 4: TOE IT Environment Assumption

3.3 Threats

A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset. Threat agents are entities that can adversely act on assets – the threat agents in the threats below are unauthorized user, network attacker, and authorized user. The assets are the entities that can be user's data or TOE data related to its functions. The TOE protects user data as primary asset by means of cryptographic functions. Thus, the cryptographic functions, their keys and CSP itself are also objects of attacks. These threats are defined here. In the following threat definition, the generic term "attacker" is used, which shall denote to either:

- An individual not being a user of the TOE trying to compromise AST.TSF_DATA and/or AST.DATA of any user of the TOE; or
- An authorized user of the TOE trying to compromise AST.TSF_DATA and/or AST.DATA of other users of the TOE, which this user is not authorized to access.

The TOE communicates with another TOE and/or other network entities. The endpoints of this communication can be geographically and logically distant and may pass through a variety of other systems. The intermediate systems may be un-trusted providing an opportunity for unauthorized communication with the TOE/network device or for authorized communication to be compromised.

Threat Name	Threat 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 AST.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 AST.DATA.
	An unauthorized process or application may get access to TOE security functions and data to disrupt the security function of TOE by changing the configuration data.

T.UNAUTH_APPL	
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 AST.DATA or AST.TSF_DATA.
T.UNIDENTIFIED_ACTIONS	Unauthorized changes to the TOE configurations and other management information may not be 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	Network traffic may be intercepted and unauthorized changes to management traffic from or to the TOE may be done.

Table 5: Threat Description addressed by TOE

3.4 Organizational Security Policies

There are no organizational security policies that the TOE must meet.

4. SECURITY OBJECTIVES

4.1 Security Objectives for the TOE

The following security objectives are intended to be satisfied by the TOE-

Objective Name	Objective Definition
O.AUTHORISED_PEER	The TOE shall ensure it is communicating with an authorized peer TOE by authenticating the peer TOE before a VPN communication channel is established.
O.AUDIT	The TOE shall record a readable audit trail of security relevant events to assist in the detection of potential attacks on the TOE.
O.ACCESS_CONTROL	The TOE must restrict access to TOE security functions and data to authorized users and processes (applications).
O.CORRECT_OPERATIONS	The TOE shall enter into a secure, non-operational state upon negative results of self-tests
O.PROTECTED_COMMUNICATIONS	The TOE shall provide protected communication channel or path between TOE and peer TOE
O.ADMIN_IDENT_AUTH	The TOE shall ensure that all Administrators are identified and authenticated before any administrative actions on the TOE can be performed.
O.CONN	The TOE must limit the IP addresses from which an administrator is able to manage the TOE and from which control data is accepted.
O.ENCRYPT	The TOE must provide Encryption of management data in a remote management session.

Table 6: Security Objectives Description for TOE

4.2 Security Objectives for the Environment

The following security objectives for the environment of the TOE must be satisfied in order for the TOE to fulfill its own security objectives -

Environmental Objective Name	Environmental Objective Definition
OE.EXT_AUTH	External authentication services must be available via a RADIUS server within internal trusted network.
OE.TIME_SYNC	NTP server must be available within internal trusted network to provide accurate/synchronized time services to the CEM.
OE.PHYSICAL	The TOE must be protected from any physical attack.
OE.ADMIN	Authorized users must be trained and follow all administrator guidance.

Environmental Objective Name	Environmental Objective Definition
OE.NWCOMP	The IT environment network components that have access to the management interface of the TOE must be protected.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it until/unless the same is configured.

Table 7: Security Objectives for Environment Description for TOE

5. EXTENDED COMPONENT DEFINITION

TOE supports extended components which are not part of existing CC Part 2. The extended component is part of TOE Security Functional Requirement (SFR) with an extension "_EXT" to TOE SFR name. The extended SFR is modeled using SFR included in CC Part 2.

In this ST, the extended SRF is part of the identified class of requirements FCS and FPT. The extended SFR dependencies on other SRF, Management requirements, and Audit requirements are identified in respective section.

5.1 Requirement for Extended Components

Class of Requirement FPT
In order to check the integrity of security function of the TOE, the TOE performs self-test at time of start-up.

Class of Requirement FCS
In order to have a secure communication channel between TOE and remote terminals for administration, SSH protocol is used. SSH uses two way authentications between TOE and remote terminal to provide secure communication channel so that it can prevent any attack to disrupt the management interface information or TOE configurations. Another requirement is use of IPsec for IP encryptor Functionality. IPsec uses different key exchange, encryption and authentication mechanisms for VPN's.

5.2 Definition

The FPT_TST_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT is taken from collaborated Protection Profile for Network Devices version 1.0. It is defined as a requirement specific to SSH protocol supported by the TOE.

5.3 FPT_TST_EXT.1 Self Test

Family Behavior
The component in this family addresses the requirements for self-testing the TSF for selected correct operation.

Component Leveling

FPT_TST_EXT: Self Test	1

FPT_TST_EXT.1 The TSF shall run a suite of self-tests during initial start-up to demonstrate the correct operation of the TSF therefore ensuring TOE integrity.

Management: FPT_TST_EXT.1
None

Audit: FPT_TST_EXT.1
The following action should be auditable if FAU_GEN Security audit data generation is included in ST:

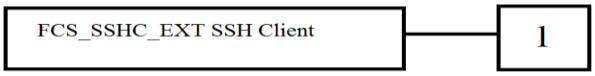
a) Self-Tests results.

Hierarchical to: No other components
Dependencies: None

5.4 FCS_SSHC_EXT.1 SSH Client

Family Behavior
The component in this family addresses the ability for a client to use SSH to protect data between the client and a server using the SSH protocol.

Component Leveling



FCS_SSHC_EXT.1 SSH Client requires that the client side of SSH be implemented as specified.

Management: FCS_SSHC_EXT.1
The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit: FCS_SSHC_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Failure of SSH session establishment.
b) SSH session establishment
c) SSH session termination

FCS_SSHC_EXT.1	SSH Client Protocol
Hierarchical to:	No other components
Dependencies:	FCS_COP.1.1 Cryptographic operation (AES Data Encryption/Decryption; Signature Verification; Hash Algorithm)

5.5 FCS_SSHS_EXT.1 SSH Server Protocol

Family Behavior
The component in this family addresses the ability for a server to offer SSH to protect data between the client and a server using the SSH protocol.

Component Leveling

FCS_SSHS_EXT.1 SSH Server requires that the server side of SSH be implemented as specified.

Management: FCS_SSHC_EXT.1

The following actions could be considered for the management functions in FMT:
a) There are no management activities foreseen.

Audit: FCS_SSHS_EXT.1
The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:
a) Failure of SSH session establishment.
b) SSH session establishment
c) SSH session termination

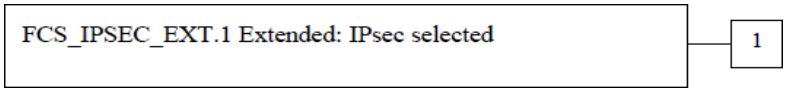
FCS_SSHS_EXT.1	SSH Server Protocol

Hierarchical to: No other components
Dependencies: FCS_COP.1.1 Cryptographic operation (AES Data Encryption/Decryption; Signature Verification; Hash Algorithm)

5.6 FCS_IPSEC_EXT Extended: IPsec

Family Behavior
This family addresses requirements for protecting communications using IPsec.

Component leveling



FCS_IPSEC_EXT.1 This component requires that IPsec be implemented as specified.

Management

The following actions could be considered for the management functions in FMT:

a) There are no management actions foreseen.

Audit

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the ST:

a) Initiation to establish an IPsecSA

b) IPsec IKE SA established

c) IPsec Child SA established.

d) IPsec SA destroyed.

e) Failure to establish an IPsec SA

FCS_IPSEC_EXT.1 Extended: IPsec selected
Hierarchical to: No other components.
Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys) FCS_COP.1.1 Cryptographic operation (AES Data

Encryption/ Decryption; Signature Verification;
Hash Algorithm)

FCS_IPSEC_EXT.1 Extended: IPsec selected

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall implement [*selection: tunnel mode, transport mode*].

FCS_IPSEC_EXT.1.3 The TSF shall have a nominal, final entry in the anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithm [*selection: AES-CBC-128 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA)-based HMAC, AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA2)-based HMAC (as specified by RFC 4868)*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [selection: IKEv2 as defined in RFCs 7296, no other RFC and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [selection: IKEv1, IKEv2] protocol uses the cryptographic algorithms AES-CBC-256 as specified in RFC 3602 and [selection: AES-CTR-256, AES-CBC-128, AES-CTR-128, no other algorithms].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [selection: IKEv2 SA lifetimes shall be established based on [selection: number of packets/number of bytes; length of time, where the time values shall not exceed: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs];].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: Elliptic curve 25519, other DH group algorithm].

FCS_IPSEC_EXT.1.9 The TSF shall ensure that all IKE protocols perform Peer Authentication using the [selection: RSA, ECDSA, Pre-shared Key] algorithm.

6. SECURITY REQUIREMENTS

6.1Conventions

The following conventions have been applied in this document-

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: assignment, selection, refinement and iteration.
- The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**.
- The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by [*italicized text within square brackets*].
- The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value in square brackets, [assignment value].
- The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration sequence letter following the component identifier.

6.2 Security Functional Requirements

This section describes the Security Functional Requirements (SFRs) for the TOE, organised by CC class. SFRs implemented by the TOE are identified in the Table No 8 below. In the subsequent sections, they are further described in details.

Security Functional Class	Security Functional Components
Audit (FAU)	Security alarms (FAU_ARP.1)
	Audit data generation (FAU_GEN.1)
	User identity association (FAU_GEN.2)
	Audit review (FAU_SAR.1)
	Restricted Audit review (FAU_SAR.2)
	Potential violation analysis (FAU_SAA.1)
	Protected audit trail storage (FAU_STG.1)
User data protection (FDP)	Subset information flow control (FDP_IFC.1)
	Simple security attributes (FDP_IFF.1)
Identification and authentication (FIA)	User attribute definition (FIA_ATD.1)
	Specification of secrets (FIA_SOS.1)
	User authentication before any action (FIA_UAU.2)
	User identification before any action (FIA_UID.2)

Security Functional Class	Security Functional Components
	Authentication failure (FIA_AFL.1)
	Multiple authentication mechanisms (FIA_UAU.5)
Security management (FMT)	Static attribute initialisation (FMT_MSA.3)
	Management of TSF data (CEM configuration) (FMT_MTD.1a)
	Management of TSF data (User attributes) (FMT_MTD.1b)
	Management of TSF data (Audit logs) (FMT_MTD.1c)
	Management of TSF data (Date/time) (FMT_MTD.1d)
	Management of TSF data (Sessions) (FMT_MTD.1e)
	Specification of Management Functions (FMT_SMF.1)
	Specification Management Roles (FMT_SMR.1)
Protection of the TSF (FPT)	Time stamps (FPT_STM.1)
	Self Test (FPT_TST_EXT.1)
	Fail Secure (FPT_FLS.1)
TOE access (FTA)	TOE session establishment (FTA_TSE.1)
	Limit multiple concurrent sessions (FTA_MCS.1)
	Session Termination on Inactivity (FTA_SSL.3)
Cryptographic support (FCS)	Cryptographic key generation (FCS_CKM.1)
	Cryptographic key destruction (FCS_CKM.4)
	Cryptographic operation (FCS_COP.1)
	FCS_SSHC_EXT.1 : SSH
	FCS_SSHS_EXT.1 : SSH
	FCS_IPSEC_EXT.1: IPsec

Table 8: Security Function Requirement for TOE

6.2.1 Audit (FAU)

6.2.1.1 Security Alarms (FAU_ARP.1)

FAU_ARP.1.1
The TSF shall take [the following actions: generate an alarm, create a log entry and lock user account for a specified time] upon detection of a potential security violation.

6.2.1.2 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1
The TSF shall be able to generate an audit record of the following auditable events-

a) ~~Start-up and shutdown of the audit functions~~ Note: start up and shut down of the audit function will not be captured in Audit Log as Audit function will always be on;
b) All auditable events for the [not specified] level of audit specified in APPENDIX-A; and
c) [User login/logout;
d) Login failures;
e) Committing the TOE configuration;
f) Alarms generated during any operation].

FAU_GEN.1.2
The TSF shall record within each audit record at least the following information:-
a) Date and time of the event, event and subject identity (if applicable);
b) For each audit event type, based on the auditable event definitions of the functional components included in the ~~PP~~/ST [no additional information].

6.2.1.3 User Identity Association (FAU_GEN.2)

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.

6.2.1.4 Audit Review (FAU_SAR.1)

FAU_SAR.1.1
The TSF shall provide [System-Admin, Root-System] with the capability to read [all information] 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.

6.2.1.5 Restricted Audit Review (FAU_SAR.2)

FAU_SAR.2.1
The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.6 Potential Violation Analysis (FAU_SAA.1)

FAU_SAA.1.1
The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2
The TSF shall enforce the following rules for monitoring audited events:-
a) Accumulation or combination of [failed authentication attempt events] known to indicate a potential security violation;
b) [No other events].

6.2.1.7 Protected Audit Trail Storage (FAU_STG.1)

FAU_STG.1.1
The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2
The TSF shall be able to [prevent] unauthorized modifications to the stored audit records in the audit trail.

6.2.2 User Data Protection (FDP)

6.2.2.1 Subset Information Flow Control (FDP_IFC.1)

FDP_IFC.1.1
The TSF shall enforce the [VPN SFP] on

a) [subjects: (i) Source Subjects: TOE interface (Trusted ports) on which User information is received, (ii) Destination Subjects: TOE interface (External Port) on which user information is destined;
b) Information (IP packets): User data traffic sent through the TOE's Trusted and External interface port;
c) Operation: Encrypt, decrypt, or deny information].

6.2.2.2 Simple Security Attributes (FDP_IFF.1)

FDP_IFF.1.1
The TSF shall enforce the [VPN SFP] based on the following types of subject and information security attributes: [

a) Subjects:
   - Source Subjects: TOE interface (Trusted ports) on which User information is received
   - Destination Subjects: TOE interface (External port) on which User information is destined
b) Information: User data traffic sent through the TOE's Trusted and External interface port
c) Information Security attributes: Source IP address, Destination IP address, IP protocol (only ESP), UDP destination port 4500, Security Policy of TOE.

FDP_IFF.1.2
The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

a) Receiving from Source Subjects (on trusted interface), Sending to Destination Subjects (through External interface):
   - The IP packet contains an authorized source and destination IP addresses
   - The TSF can find an associated Security Association (SA) using the source and destination IP addresses of the IP packet
b) Receiving from Destination Subjects (on External interface), Sending to Source Subjects (through Trusted interface):

- UDP 4500/500 for IPsec traffic
- If the IPsec packet contains a SPI (within ESP header)
  - The TSF can find an associated Security Association (SA) using the SPI within the IPsec packet.
- The IP packet has been properly protected according to the SA referred by the associated SA.
- The decrypted IP packet contains an authorized source and destination IP addresses.

FDP_IFF.1.3
The TSF shall enforce the [no additional VPN SFP rules].

FDP_IFF.1.4
The TSF shall explicitly authorize an information flow based on the following rules: [no additional rules that explicitly authorize information flows].

FDP_IFF.1.5
The TSF shall explicitly deny an information flow based on the following rules: [no additional rules that explicitly deny information flows].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 User Attribute Definition (FIA_ATD.1)

FIA_ATD.1.1
The TSF shall maintain the following list of security attributes belonging to individual users:-
[For interactive users:
a) User identity
b) Privilege levels
c) Password
For neighbour device:
a) IP address
b) Password]

6.2.3.2 Verification of Secrets (FIA_SOS.1)

FIA_SOS.1.1
The TSF shall provide a mechanism to verify that secrets meet [password length of 8-16 characters with at least one change of character set (upper, lower, numeric, special character) for interactive users].

6.2.3.3 User Authentication before any Action (FIA_UAU.2)

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.

6.2.3.4 User Identification before any Action (FIA_UID.2)

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.

6.2.3.5 Authentication Failure (FIA_AFL.1)

FIA_AFL.1.1
The TSF shall detect when [3] unsuccessful authentication events occur related to [login of users].

FIA_AFL.1.2
When the defined number of unsuccessful authentication attempts has been met, the TSF shall [lock the user account for a specified period which can be un-locked by the Root-System; never lock Root-System account].

6.2.3.6 Multiple Authentication Mechanisms (FIA_UAU.5)

FIA_UAU.5.1
The TSF shall provide [internal password mechanism and external server (RADIUS) mechanism to support user authentication.

FIA_UAU.5.2
The TSF shall authenticate any user's claimed identity according to the [authentication mechanism specified by System-Admin, Root-System].

6.2.4 Security Management (FMT)

6.2.4.1 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1
The TSF shall enforce the [VPN SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2
The TSF shall allow the [Root-System, System-Admin] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.2 Management of TSF Data (CEM configuration) FMT_MTD.1a

FMT_MTD.1.1a
The TSF shall restrict the ability to [modify] the [CEM configuration data] to [System-Admin, Root-System].

6.2.4.3 Management of TSF Data (User attributes) (FMT_MTD.1b)

FMT_MTD.1.1b
The TSF shall restrict the ability to [modify] the [user account attributes] to [Root-System].

6.2.4.4 Management of TSF data (Audit logs) (FMT_MTD.1c)

FMT_MTD.1.1c
The TSF shall restrict the ability to [modify or delete] the [audit logs] to [None].

6.2.4.5 Management of TSF data (Date/time) (FMT_MTD.1d)

FMT_MTD.1.1d
The TSF shall restrict the ability to [modify] the [NTP Server address and system clock] to [System-Admin, Root-System].

6.2.4.6 Management of TSF data (Sessions) (FMT_MTD.1e)

FMT_MTD.1.1e
The TSF shall restrict the ability to [modify, delete] the [rules that restrict the ability to establish management sessions] to [Root-System].

6.2.4.7 Security Roles (FMT_SMR.1)

FMT_SMR.1.1

The TSF shall maintain the privilege levels to differentiate [Root-System, System-Admin and Operator]

S.N.	Privilege Level	User Role	User Privileges/Functions Performed
1.	1	Operator	User with "operator" role privileges can perform following functions: • View CEM configurations only. • Change own password.
2.	2	Sysadmin	User with "sysadmin" role privileges can perform following functions: • View CEM configurations. • Import CA, admin public certificate • Configure VPN policies. • Export device public certificate. • Change own password. • View audit logs. • Configure and modify CEM interfaces and manage routing tables. • Configure RADIUS for user authentication. • Delete, add, or modify communicating peers. • Import/generate/purge Device keys • View and configure IP of CEM interface. • Configure external syslog server information on the CEM. • Configure, modify system date and time.

S.N.	Privilege Level	User Role	User Privileges/Functions Performed
			• Configure NTP client. • Configure, modify and apply information flow control attributes (VPN SFP) on TOE interfaces. • Configure or modify time limit of user inactivity. • Save CEM configurations to a configuration file.
3.	3	Rootsystem	User with "rootsystem" role can perform following functions: • View CEM configurations. • Import CA, admin public certificate • Export device public certificate. • Change own password. • View audit logs. • Configure VPN policies • Configure and modify CEM interfaces and manage routing tables. • Configure RADIUS for user authentication. • Delete, add, or modify communicating peers. • Import/generate/purge Device keys. • View and configure IP of CEM interface. • Configure external syslog server information on the CEM. • Configure, modify system date and time. • Configure NTP client and server. • Configure, modify and apply information flow control attributes (VPN SFP) on TOE interfaces. • Configure or modify time limit of user inactivity. • Save CEM configurations to a configuration file. • Can reset CEM to factory setting. • Can load a saved configuration file. • FTP configuration files to/from external machine. • Create, modify and delete users and its roles (sysadmin, operator) /privileges/passwords. Can not create a user with rootsystem role. • Configure or modify the number of concurrent session of a user. • Configure or modify the number of concurrent session of a user. • Configure Management ACL white-list to control management sessions.

Table 9: TOE User's Privileges and roles

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.4.8 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions: [

- Configure, modify, save CEM configuration data.
- Configure or modify date and time.
- Import CA, admin public certificates
- Export device public certificate.
- Configure VPN policies.
- Import/generate/purge Device keys.
- View and configure IP of CEM interface.
- Configure or modify information flow control attributes (VPN SFP).
- Create, modify and delete user attributes and privileges to authenticate and identification of users before providing access to the system.
- Configuring User Login control (identification and authentication mechanism through local, or RADIUS).
- Configure or modify time limit of user inactivity.
- Configure or modify the number of concurrent session of a user.
- Configure or modify number of unsuccessful consecutive login attempts before locking the user account.
- Configure external authentication server (RADIUS).
- Configuring NTP client/server.
- Configuring external Syslog server.
- Manage IP table/ routing tables.
- Manage the audit logs.
- Controlling management sessions.]

The user privilege/role to perform the above mentioned security function is defined in table 10 of section 6.2.4.8

6.2.5 Protection of the TOE Security Functions (FPT)

6.2.5.1 Time Stamps (FPT_STM.1)

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

6.2.5.2 Self Test (FPT_TST_EXT.1)

FPT_TST_EXT.1.1
The TSF shall run a suite of self tests [during start-up] to demonstrate the correct operation of TSF [

- Cryptographic operations

].

6.2.5.3 Fail Secure (FPT_FLS.1)

FPT_FLS.1
The TSF shall preserve a secure state when the following types of failures occur: [

- Self Test failure – During start-up if cryptographic operation checks are failed then the further software start-up is prevented and system does not provide any services. In this situation, System Administrator intervention is required to re-install correct configurations/files.

].

6.2.6 TOE Access (FTA)

6.2.6.1 TOE Session Establishment (FTA_TSE.1)

FTA_TSE.1.1
The TSF shall be able to deny session establishment based on [presumed origin of the request].

6.2.6.2 Basic limitation on Multiple Concurrent Sessions (FTA_MCS.1)

FTA_MCS.1.1
The TSF shall restrict the maximum number of concurrent sessions of the same user.

FTA_MCS.1.2
The TSF shall enforce by default, a limit of [10 total maximum number of sessions per user who is not Root-System, which is configurable. The Root-System can have only one session.]

6.2.6.3 Session Termination on Inactivity (FTA_SSL.3)

FTA_SSL.3.1
The TSF shall terminate an interactive session after [5 minutes of user inactivity, inactive duration can be configured by System-Admin or Root-System].

6.2.7 Cryptographic Support (FCS)

6.2.7.1 Cryptographic Key Management (FCS_CKM.1)

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:

- DSA (Digital Signature Algorithm) schemes using cryptographic key sizes of 1024-bit that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)",
- RSA (Rivest-Shamir-Adleman Algorithm) schemes using cryptographic key sizes of 2048-bit that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)",
- Elliptical-curve 25519 schemes using cryptographic key size of 256-bit that meet the following :RFC 8031
- Diffie-hellman(2048-MODP) scheme using cryptographic key size of 2048-bit that meets the following :RFC 2631]

~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

6.2.7.2 Cryptographic Key Destruction (FCS_CKM.4)

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

6.2.7.3 Cryptographic Key Operation (FCS_COP.1)

Remote administration by SSH

FCS_COP.1.1
The TSF shall perform [encryption/decryption of remotely authorized user sessions] in accordance with a specified cryptographic algorithm [for host key generation: Digital Signature Standard as specified in FIPS PUB 186-4 with key length 1024 bits; for asymmetric encryption: RSA as specified in FIPS PUB 186-4 with key length 2048 bits; for key exchange: diffie-hellman-group-exchange-sha256 as per RFC 4419; for user authentication: Digital Signature Algorithm (DSA) and Rivest-Shamir-Adleman Algorithm(RSA) as specified in FIPS PUB 186-4;for symmetric encryption: Advanced Encryption Standard (AES) used in [CTR, CBC] mode with key lengths 128, 192 or 256 bits that meet the following: AES as specified in ISO 18033-3, [CTR as specified in ISO 10116,CBC as specified in FIPS PUB 197]; for data integrity check: Hash Message Authentication Code - Secure Hash Algorithm 2 (HMAC-SHA2) with block size 256/512 as specified in FIPS PUB 180-4] ~~and cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards]~~.

6.2.7.4 SSH Client Protocol (FCS_SSHC_EXT.1)

FCS_SSHC_EXT.1.1
The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, 4254].

FCS_SSHC_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: password- based.

FCS_SSHC_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [AES-128-CTR, AES-192-CTR and AES-256-CTR].

FCS_SSHC_EXT.1.5
The TSF shall ensure that the SSH transport implementation uses [RSA-2048, DSA-1024] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHC_EXT.1.6
The TSF shall ensure that the SSH transport implementation uses [HMAC-SHA2 256/512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7
The TSF shall ensure that [diffie-hellman-group-exchange-sha256] are the only allowed key exchange methods used for the SSH protocol.

6.2.7.5 SSH Server Protocol (FCS_SSHS_EXT.1)

FCS_SSHS_EXT.1.1
The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253 and 4254].

FCS_SSHS_EXT.1.2
The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: password- based.

FCS_SSHS_EXT.1.4
The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [AES-128-CTR, AES-192-CTR and AES-256-CTR].

FCS_SSHS_EXT.1.5
The TSF shall ensure that the SSH transport implementation uses [RSA-2048, DSA-1024] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6

The TSF shall ensure that the SSH transport implementation uses [HMAC-SHA2 256/512] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7
The TSF shall ensure that [diffie-hellman-group-exchange-sha256] are the only allowed key exchange methods used for the SSH protocol.

6.2.7.6 FCS_IPSEC_EXT.1 : IPSEC Selected

FCS_IPSEC_EXT.1.1
The TSF shall implement the IPsec architecture as specified in RFC 4301, 4306.

FCS_IPSEC_EXT.1.2
The TSF shall implement both tunnel and transport mode.

FCS_IPSEC_EXT.1.3
The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.4
The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-256 (as specified by RFC 3602) together with a Secure Hash Algorithm (SHA2)-based HMAC (as specified by RFC 4868).

FCS_IPSEC_EXT.1.5
The TSF shall implement the protocol: IKEv2 as defined in RFC 7296, and RFC 4868 for hash functions.

FCS_IPSEC_EXT.1.6
The TSF shall ensure the encrypted payload in the IKEv2 protocol uses the cryptographic algorithms AES-CBC-256 as specified in RFC 3602 and [no other algorithm].

FCS_IPSEC_EXT.1.7
The TSF shall ensure that IKEv2 SA lifetimes shall be established based on [length of time, where the time values shall not exceed: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs].

FCS_IPSEC_EXT.1.8
The TSF shall ensure that all IKE protocols implement DH Groups 14 [2048-bit MODP and Elliptic curve 25519].

FCS_IPSEC_EXT.1.9
The TSF shall ensure that all IKE protocol perform peer authentication using [RSA or ECDSA or pre-shared Key] algorithm

6.3 Security Assurance Requirements

The following Table 11 describes the TOE security assurance requirements drawn from Part 3 of the CC.

Assurance Class	Assurance Components
Security Target (ASE)	*ST introduction (ASE_INT.1)*
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Conformance Claim (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	*Security architecture description (ADV_ARC.1)*

Assurance Class	**Assurance Components**
	Functional specification with complete summary (ADV_FSP.3)
	Architectural design (ADV_TDS.2)
Guidance documents (AGD)	*Operational user guidance (AGD_OPE.1)*
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	*Authorisation controls (ALC_CMC.3)*
	Implementation representation CM coverage (ALC_CMS.3)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
Tests (ATE)	*Analysis of coverage (ATE_COV.2)*
	Testing: basic design (ATE_DPT.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	*Vulnerability analysis (AVA_VAN.2)*

Table 10: TOE Security Assurance Requirement

7. TOE SUMMARY SPECIFICATION

7.1 TOE Security Functions

7.1.1 Information Flow Function

FDP_IFC.1: Subset Information Flow Control and
FDP_IFF.1: Simple Security Attributes

The TOE implements IPsec for VPN functionality. The TOE apply VPN SFP on all the user data and only apply VPN policies on the IP traffic that is defined in TOE. TOE protect the user data with the encryption, authentication mechanism defined in IPsec policies for respective user data. Ensuring confidentiality of the user's data provides the capability to prevent the disclosure of these data when they flow through a non-secure public network. For that purpose, these data can be ciphered before going through the public network and deciphered in the entry of the private network recipient. The encryption/decryption algorithm and used keys characteristics are defined in the security context associated to the VPN security policy defined on a given communication link.

To ensure the applicative data authenticity, TOE ensure at the same moment the on-the-fly integrity of these data as well as the authentication of the origin of these. Ensuring the data integrity provides the capability to detect that they were not modified accidentally or intentionally during their transmission from one TOE (i.e. encryptor) to another.

TOE ensure all the rules defined in FDP_IFF.1 for subset information flow between controlled subject and controlled object for controlled operations.

7.1.2 Identification and Authentication Function

FIA_ATD.1: User Attribute Definition
User accounts in the TOE have the following attributes: user name, authentication data (password) and privilege (Level). The System-Admin or Root-System can configure TOE to handover the authentication process to a RADIUS server.

FIA_SOS.1: Verification of Secrets
Locally stored authentication data for password authentication is a case-sensitive, alphanumeric value. The password has a minimum length of 8 ASCII characters with at least one change of character set (upper, lower, numeric, special character), and can be up to 16 ASCII characters in length.

FIA_UAU.2: User Authentication before any Action,
FIA_UAU.5: Multiple Authentication Mechanisms and
FIA_UID.2: User Identification before any Action
The TOE requires users to provide unique identification and authentication data (passwords) before any administrative access to the system is granted.

The CEM software supports three methods of user authentication: local password authentication and external authentication server Remote Authentication Dial-In User Service (RADIUS).

With local password authentication, a password is configured for each user allowed to log into the CEM. RADIUS is an authentication method for validating users who attempt to

access the CEM. Both are distributed client/server systems—the RADIUS clients run on the appliance, and the server runs on a remote network system in the IT environment.

If the user identity specified is defined locally, the TOE can successfully authenticate that identity if the authentication data provided matches that stored in conjunction with the provided identity. Alternately, if the TOE is configured to work with a RADIUS (by System-Admin, Root-System), the identity and authentication data is provided to the server and the TOE enforces the result returned from the server. Regardless user authentication mechanisms, no administrative actions are allowed until successful authentication is done as an authorized administrator.

FIA_AFL.1 Authentication Failure
After 3 (configurable by Root-System) consecutive login failures for a particular user, the account will be locked for a specified period and Root-System can unlock the account.

7.1.3 Security Management Function

FMT_MSA.3: Static Attribute Initialisation
The TOE boots up with default security attributes, some of which can only be configured by Root-System user by configuring an ACL rule to restrict/allow network access to the TOE. As default, allows SSH connection to access the TOE from serial port or a predefined subnet. The TOE allows only authorized administrators (Root-System, System-Admin) depending on their privileges to create alternative policy over and above default attributes/policy to access TOE.

FMT_MTD.1a: Management of TSF Data (CEM Information)
The TOE restricts the ability to administer the CEM configuration data based on the privilege level of users. The CLI provides a text-based interface from which the CEM configuration can be managed and maintained. From this interface all TOE functions, such as peer TOE addition, network topology can be managed and including date/time.

FMT_MTD.1b: Management of TSF Data (User Data)
The TOE restricts the ability to administer user data to Root-System. The CLI provides Root-Admin users with a text based interface from which all user data can be managed. From this interface new accounts can be created, and existing accounts can be modified or deleted. This interface also provides administrator an ability to configure an external authentication server, such as a RADIUS server. When this is assigned, a user can be authenticated to the external server instead of directly to the TOE.

FMT_MTD.1c: Management of TSF Data (Audit logs)
The TOE can be configured to transfer audit logs automatically to external syslog server by System-Admin or Root-System. Audit logs can’t be modified or deleted by any of the administrator or user.

FMT_MTD.1d: Management of TSF Data (Date/time)
The TOE will allow System-Admin or Root-System to modify/update the date/time setting on the device.

FMT_MTD.1e: Management of TSF Data (Sessions)
The TOE will allow Root-System to create, delete or modify the policy which controls the presumed address from which management sessions can be established.

FMT_SMF.1: Management of Security Functions
The TOE provides the ability to manage the following security functions:

a) Create, modify and delete User attributes and privileges;
b) Configure VPN policies.
c) Configure User login control (Local or RADIUS);
d) User authentication (authentication data, roles);
e) CEM configuration (date/time, configuration rollback, ACL filter/Rules, and update/management of routing tables and deletion of routing information learned from the network);
f) Configure time limit for user inactivity.
g) Session establishment management/restrictions which depends on number of concurrent sessions of types of users and their privileges.
h) Configure the limit on unsuccessful consecutive login failures after which the login account is locked.
i) Configure NTP client/server and external RADIUS, Syslog servers.
j) Audit management and review;

FMT_SMR.1: Security Roles
The TOE has privilege levels defined per user role. When a new user account is created, it must be assigned one of the following user roles –

Operator Role
This role can view TOE status and statistics only in addition to change its own password.

System-Admin Roles
a) Create, modify, delete, save and view TOE configuration.
b) Change own password
c) Configure VPN policies
d) modify date/time;
e) create or delete static routes and routing protocols
f) configure external authentication server (RADIUS)
g) configure external syslog server
h) Import CA, admin public certificate.
i) Export device public certificate.
j) Import device keys.
k) View and configure IP of CEM interface.
l) configure NTP client
m) configure and apply ACL rules
n) configure time limit of user inactivity
o) Can review the audit records

Root-System Roles
Root-System has permission to all commands for System-Admin. In addition to that Root-System can perform configuration of Management ACL white-list, TOE user administration, reset CEM to factory setting, ftp configuration files and load a saved configuration file.

7.1.4 Audit Function

FAU_GEN.1: Audit data generation
CEM creates and stores audit records for the following events:

1. User login/logout;
2. Login failures;

3. SSH session establishment and termination;
4. Failure to set up SSH session;
5. Configuration is committed;
6. Configuration is changed.
7. Modification of date/time;
8. Alarms generated during any operation.

CEM shall also record Date and time of the above auditable event, event and subject identity (if applicable).

FAU_GEN.2: User Identity Association
CEM will associate Date and time of the event, event and subject identity causing the event.

FAU_SAR.1: Audit Review
CEM provides System-Admin, Root-System users with the ability to display audit data from the CLI. CEM provides the ability to display audit records as complete files, or selective records based on user-defined filters.

FAU_SAR.2: Restricted Audit Review
Audit log view shall be restricted to any other user except those who have been given the privilege to review.

FAU_STG.1: Protected Audit Trail Storage
Audit records will be saved in files. The Root-System and System-Admin user may display the content of Audit logs on screen using CLI commands. There is no CLI command to edit or delete the Audit log files. Hence, they are protected from any modification or deletion.

FAU_ARP.1: Security Alarms
While authenticating a user, an audit log message is generated and the user account is locked after 3 successive login failures and alarm is generated.

FAU_SAA.1: Potential Violation Analysis
CEM shall analyse the failed authentication attempts to identify activity indicating a potential violation. The potential violation is defined as 3 successive login failures, and the action taken is that the user account is locked for a specified period.

7.1.5 TOE Access Function

FTA_TSE.1: TOE Session Establishment
The TOE can be configured by Root-System such that users can only gain access from specific management networks/stations at specific IP addresses.

FTA_MCS.1: Maximum number of Concurrent Sessions
The TOE allows a maximum of 10 concurrent sessions for every user by default, which is configurable up to 32 for users who are not Root-System and a single session each for Root-System.

FTA_SSL.3: Session termination on user inactivity
The TOE will terminate a session after 5 minutes (configurable by System-Admin or Root-System) of inactivity.

7.1.6 Clock function

FPT_STM.1: Time stamps
The clock function of the TOE provides a source of date and time information, used in audit timestamps. The clock function is reliant on the system clock.

For better accuracy of timestamp and synchronization of time across devices in the IT environment, an external NTP server can be deployed. In such deployments the audit timestamps will be synchronized with external NTP servers, if configured (by Root-System).

7.1.7 TOE Self Test

FPT_TST_EXT.1: Self Test

<SECURE STATE TEST>

7.1.8 Fail Secure

FPT_FLS.1: Fail Secure
The TOE remains in a secure state in case of Self Test failure during start-up and does not provide any services. The system can be rebooted or re-installed by TOE user to recover it.

7.1.9 Cryptographic Support for Protection of Management Interface Sessions

FCS_CKM.1: Cryptographic key management,
FCS_CKM.4: Cryptographic key destruction,
FCS_COP.1: Cryptographic key operation,
FCS_SSHC_EXT.1: SSH Client Protocol,
FCS_SSHS_EXT.1: SSH Server Protocol and
FCS_IPSEC_EXT.1: IPsec

The TOE protects remote user sessions over management interface from any cryptographic attack. The TOE uses Open SSHv2 protocol for allowing remote clients for logging through CLI. SSHv2 uses DSA/RSA key generation (conformant to FIPS PUB 186-4), session key using Diffie-Hellman Exchange Algorithm (diffie-hellman-group-exchange-sha256) and 128, 192 or 256 bits AES (CTR mode) for encryption. HMAC-SHA 2 256/512 is used for Data Integrity as specified in FIPS PUB 180-4. The keys are overwritten when new keys are generated. The TOE uses IPsec for IP encryptor functionality as specified in RFC 4301 and 4306. TOE IPsec uses AES-CBC-256 for encryption of user data as specified in FIPS PUB 197 and RFC 3602, HMAC-SHA2 for authenticity of user data as specified in FIPS PUB 180-4 and RFC 4868. TOE implements IKEv2 protocol as specified in RFC 7296.TOE implements IKE protocol:MODP-2048 as specified in RFC 8031 and Elliptical curve 25519 as specified in RFC 2631 .TOE ensures peer authentication using RSA or ECDSA or Pre-Shared Key.

8. RATIONALE

This section provides the rationale for completeness and consistency of the security target. The rationale addresses the following areas:

- Security Objectives
- Security Functional Requirements
- Security Assurance Requirements
- Dependencies

8.1 Rationale for Security Objectives

This section shows that all assumptions and threats are countered by security objectives, and that each security objective addresses at least one assumption or threat.

8.1.1 Rationale for Security Objectives for the TOE

	T.UNAUTHORIZED_PEER	T.EAVSDROP	T.UNAUTH_APPL	T.INTERCEPT	T.MALFUNCTION	T.UNIDENTIFIED_ACTIONS	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	A.ACCESS	A.COMP_NOEVIL	A.TIME	A.EXTAUTH	A.NWCOMP	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION
O.AUTHORIZED_PEER	✓													
O.ADMIN_IDENT_AUTH							✓							
O.ACCESS_CONTROL			✓				✓							
O.PROTECTE_COMMUNICATION		✓												
O.AUDIT	✓		✓	✓		✓	✓							
O.CONN			✓	✓			✓							
O.ENCRYPT			✓	✓			✓							

	T.UNAUTHORIZED_PEER	T.EAVSDROP	T.UNAUTH_APPL	T.INTERCEPT	T.MALFUNCTION	T.UNIDENTIFIED_ACTIONS	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	A.ACCESS	A.COMP_NOEVIL	A.TIME	A.EXTAUTH	A.NWCOMP	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION
O.CORRECT_OPERATIONS					✓									

Table 11: TOE Security Objective Rationale

O.AUTHORIZED_PEER: This objective requires that the TOE shall authenticate all peer TOE (T.UNAUTHORISED_PEER) before setting up a VPN communication channel with the peer TOE upon which user data is transmitted to.

O.ADMIN_IDENT_AUTH: This objective ensures that only identified and authenticated Administrators (T.UNAUTHORIZED_ADMINSITRATOR_ACCESS) will be able to access the TOE and perform management functions.

O.ACCESS_CONTROL: This objective addresses the need to protect the TOE's operations and data. This helps counter the threats of unauthorised access (T.UNAUTH_ACCESS and T.UNAUTH_APPL).

O.PROTECTED_COMMUNICATION: This objective requires the TOE to establish a mutually authenticated secure channel (T.EAVSDROP) prior to transmitting of user data traffic.

O.AUDIT: This objective serves to discourage and detect inappropriate use of the TOE (T.UNIDENTIFIED_ACTIONS), and as such helps counter T.UNAUTHORISED_PEER T.UNAUTH_ACCESS, T.UNAUTH_APPL and T.INTERCEPT, which relate to inappropriate (deliberate or accidental) use of the TOE.

O.CONN: This objective helps to counter the threats relating to unauthorised modification by an attacker to the TOE configuration (T.UNAUTH_ACCESS & T.UNAUTH_APPL) by limiting the IP addresses from which the TOE accepts management and control traffic connections (T.INTERCEPT).

O.ENCRYPT: This objective helps to counter the interception of management data by encrypting the remote management data (T.INTERCEPT) and prevent the unauthorised access (T.UNAUTH_ACCESS, T.UNAUTH_APPL) to TOE.

O.CORRECT_OPERATIONS: This objective prevents TOE failure by performing and verifying that the TOE's self-test has pass (T.MALFUNCTION), indicating that TOE components are functional and operating correctly.

8.1.2 Rationale for Security Objectives for the Environment

	T.UNAUTHORIZED_PEER	T.EAVSDROP	T.UNAUTH_APPL	T.INTERCEPT	T.MALFUNCTION	T.UNIDENTIFIED_ACTIONS	T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	A.ACCESS	A.COMP_NOEVIL	A.TIME	A.EXTAUTH	A.NWCOMP	A.LIMITED_FUNCTIONALITY	A.NO_THRU_TRAFFIC_PROTECTION
OE.EXT_AUTH							✓				✓			
OE.TIME_SYNC										✓				
OE.PHYSICAL								✓						
OE.ADMIN									✓					
OE.NWCOMP												✓		
OE.NO_GENERAL_PURPOSE													✓	

Table 12: TOE Security Objectives for Environment Rationale

OE.EXT_AUTH: The objective to have an authentication server in the TOE environment which helps to counter the threat of unauthorised access enforcing authentication of users attempting to access to TOE security functions and data (T.UNAUTH_ADMINISTRATOR_ACCESS), and supports the assumption that such a server is present (A.EXTAUTH).

OE.TIME_SYNC: The objective to have an NTP server in the TOE environment which supports the assumption (A.TIME) that time services are available to provide the appliance with accurate/synchronised time information.

OE.PHYSICAL: The objective to provide physical protection for the TOE supports the assumption that the TOE will prevent unauthorised physical access (A.ACCESS).

OE.ADMIN: The objective that users should follow administrator guidance supports the assumption that they will not be careless, wilfully negligent or hostile (A.COMP_NOEVIL).

OE.NWCOMP: The objective to protect those network components with access to the management interface of the TOE supports the assumption that these network components will be protected (A.NWCOMP).

OE.NO_GENERAL_PURPOSE: The objective protects the TOE from performing any other function other than its intended operation, administration and its support functions (A.LIMITED_FUNCTIONALITY).

8.2 Rationale for Security Requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and that each security functional requirement for the TOE addresses at least one security objective for the TOE. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 12 demonstrate the relationship between the threats (T), assumptions (A) and the security objectives (O). Table 13 identifies relationship between the threats (T), assumptions (A) and the environmental objectives (OE). Table 14 illustrates the mapping between security functional requirements (SFRs) and security objectives (O) for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

	O.AUTHERIZED_PEER	O.ADMIN_IDENT_AUTH	O.ACCESS_CONTROL	O.PROTECTED_COMMUNICATION	O.AUDIT	O.CONN	O.ENCRYPT	O.CORRECT_OPERATIONS
FAU_ARP.1		✓			✓			
FAU_GEN.1					✓			
FAU_GEN.2					✓			
FAU_SAA.1		✓			✓			
FAU_SAR.1					✓			
FAU_SAR.2					✓			
FAU_STG.1					✓			
FDP_IFC.1				✓				
FDP_IFF.1				✓				
FIA_ATD.1		✓	✓		✓			
FIA_AFL.1			✓					
FIA_SOS.1			✓					
FIA_UAU.2		✓	✓		✓			
FIA_UAU.5		✓	✓		✓			
FIA_UID.2		✓	✓		✓			
FMT_MSA.3				✓				
FMT_MTD.1a		✓						
FMT_MTD.1b			✓					
FMT_MTD.1c					✓			
FMT_MTD.1d					✓			
FMT_MTD.1e			✓					
FMT_SMF.1	✓	✓	✓		✓			

	O.AUTHERIZED_PEER	O.ADMIN_IDENT_AUTH	O.ACCESS_CONTROL	O.PROTECTED_COMMUNICATION	O.AUDIT	O.CONN	O.ENCRYPT	O.CORRECT_OPERATIONS
FMT_SMR.1		✓	✓	✓	✓			
FPT_TST_EXT.1								✓
FPT_FLS.1								✓
FPT_STM.1					✓			
FTA_TSE.1			✓			✓		
FTA_MCS.1			✓					
FTA_SSL.3			✓					
FCS_CKM.1	✓		✓	✓			✓	
FCS_CKM.4	✓		✓	✓			✓	
FCS_COP.1	✓		✓				✓	
FCS_SSHS_EXT.1			✓				✓	
FCS_SSHC_EXT.1			✓				✓	
FCS_IPSEC_EXT.1	✓			✓				

Table 13: TOE Security Requirements Rationale

8.2.1 Rationale for TOE Security Functional Requirements

This section demonstrates that all security objectives for the TOE are met by security functional requirements for the TOE, and that each security functional requirement for the TOE addresses at least one security objective for the TOE. The functional requirements are mutually supportive, and their combination meets the security objectives. Table 10 and Table 11 demonstrate the relationship between the threats and assumptions and the security objectives. Table 12 illustrates the mapping between security functional requirements and security objectives for the TOE. Together these tables demonstrate the completeness and sufficiency of the requirements.

FAU_ARP.1: This component takes action towards detection of potential security violations, and therefore contributes to meeting O.ADMIN_IDENT_AUTH and O.AUDIT.

FAU_GEN.1: This component outlines what events must be audited, and aids in meeting O.AUDIT.

FAU_GEN.2: This component required that each audit event be associated with a user, and aids in meeting O.AUDIT.

FAU_SAA.1: This component helps to detect potential security violations, and aids in meeting O.PROTECT and O.AUDIT.

FAU_SAR.1: This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_SAR.2: This component requires that the audit trail can be read, and aids in meeting O.AUDIT.

FAU_STG.1: This component requires that unauthorized deletion of audit records does not occur, and thus helps to maintain accountability for actions, as required by O.AUDIT.

FDP_IFC.1: and FDP_IFF.1 enforces information flow control when subjects exchange data traffic between the TOEs based on the security attributes presented at each interface (Trusted, External). Information (user data) permitted shall be protected according to the SA and security policy defined within the TOE and sent to peer TOE via the secure communication channel (IPsec) established and thus aids in meeting O.PROTECTED_COMMUNICATIONS.

FIA_ATD.1: This component specifies that individual user attributes are to be maintained and aids in meeting O.ADMIN_IDENT_AUTH, O.ACCESS_CONTROL and O.AUDIT.

FIA_AFL.1: This component protects against repeated unauthorized access attempts and hence helps meeting O.ACCESS_CONTROL.

FIA_SOS.1: This component specifies metrics for authentication, and aids in meeting objectives to restrict access O.ACCESS_CONTROL

FIA_UAU.2: This component ensures that users are authenticated to the TOE. As such it aids in meeting objectives to restrict access and aids in meeting O.PROTECT, O.ACCESS_CONTROL, and O.AUDIT.

FIA_UAU.5: This component was selected to ensure that appropriate authentication mechanisms can be selected. As such it aids in meeting objectives to restrict access O.PROTECT, O.ACCESS_CONTROL.AND O.AUDIT

FIA_UID.2: This component ensures that users are identified to the TOE. As such it aids in meeting objectives to restrict access O.ADMIN_INDENT_AUTH, O.ACCESS_CONTROL and O.AUDIT.

FMT_MSA.3: This component ensures that there is a default deny policy for the information flow control security rules. As such it aids in meeting O.PROTECTED_COMMUNICATIONS.

FMT_MTD.1a: This component restricts the ability to modify routing configuration details, and as such aids in meeting O.ADMIN_IDENT_AUTH.

FMT_MTD.1b: This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.ACCESS_CONTROL and O.PROTECT.

FMT_MTD.1c: This component restricts the ability to delete audit logs, and as such contributes to meeting O.AUDIT.

FMT_MTD.1d: This component restricts the ability to modify the date and time, and as such contributes to meeting O.AUDIT.

FMT_MTD.1e: This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.ACCESS_CONTROL.

FMT_SMF.1: This component lists the security management functions that must be controlled. As such it aids in meeting O_AUTHERIZED_PEER, O_PROTECTED_COMMUNICATION, O_AUDIT, O_ACCESS_CONTROL.

FMT_SMR.1: Each of the components in the FMT class listed above relies on this component (apart from FMT_MSA.3). It defines the roles on which access decisions are based. As such it aids in meeting O.PROTECTED_COMMUNICATION, O.ADMIN_INDENT_AUTH, O.EADMIN, O.ACCESS_CONTROL and O.AUDIT.

FPT_STM.1: This component ensures that reliable time stamps are provided for audit records and aids in meeting O.AUDIT.

FPT_TST_EXT.1: This component ensures that reliable self test are performed to ensure the integrity of TSF and aids in meeting O.CORRECT_OPERATIONS.

FPT_FLS.1: This component ensures that TOE remains in secure state in case self test fails and aids in meeting O.CORRECT_OPERATIONS.

FTA_TSE.1: This component limits the range of locations from which a user session can be established, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS_CONTROL. It also aids in meeting O.CONN.

FTA_MCS.1: This component limits the number of sessions a user can establish, and hence reduces the chance of unauthorized access. It aids in meeting O.ACCESS_CONTROL.

FTA_SSL.3: This self-terminates idle sessions after a timeout, and hence reduces the chances of unauthorized access via unattended sessions. This helps meeting O.ACCESS_CONTROL.

FCS_CKM.1: This component defines cryptographic key management functions, namely the generation of keys. This key management secures the cryptographic operations. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL, O.AUTHERIZED_PEER, O.PROTECTED_COMMUNICATION.

FCS_CKM.4: This defines cryptographic key management functions, namely the destruction of keys. This key management secures the cryptographic operations. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL, O.AUTHERIZED_PEER, O.PROTECTED_COMMUNICATION.

FCS_COP.1: This defines the actual cryptographic operation that secures the communication between TOE and users. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL, O.AUTHERIZED_PEER, O.PROTECTED_COMMUNICATION.

FCS_SSHS_EXT.1 and FCS_SSHC_EXT.1: The SSH protocol is used to secure communications between the TOE and the endpoints; authentication of users; mainly for remote administration. Securing the communication channel provides interoperability and resistance to cryptographic attack by means of two-way authentication of each end-point. This helps in meeting O.ENCRYPT and O.ACCESS_CONTROL.

FCS_IPSEC_EXT.1: IPsec is used to implement VPN functionalities in the TOE. IPsec authorizes the peer TOE (O.AUTHERIZED_PEER) and also protect the communication channel between communicating TOE's (O.PROTECTED_COMMUNICATION)

8.3 Rationale for Security Assurance Requirements (SAR)

Following are the Security Assurance Requirements selected for EAL3 assurance:

S.N.	Security Assurance Requirement/Components	Description/Rationale
1.	ADV_ARC.1 Security architecture description	*Security Architecture for Compact Encryption Module* document describes the Security Architecture of TSF which can be analysed to assure that self-protection, domain separation and non-bypass-ability properties of TSF are achieved by the design and its correct implementation. Also, it describes that the Security Architecture design is consistent with TSF.
2.	ADV_FSP.3 Functional specification with complete summary	*Function Specification for Compact Encryption Module* document provides the characteristics of all external TSF Interfaces (TSFI), such as, TSFI's purpose, method of use, parameters, parameter descriptions, actions and error message descriptions. This document provides understanding and assurance how TSF meets the claimed SFRs with summary.
3.	ADV_TDS.2 Architectural design	*TOE Security Design for Compact Encryption Module* document provides sufficient information to determine the TSF boundary, and to describe how the TSF implements the SFRs. It describes TOE at both Sub-system level as well as Module level details. It describes the Sub-system interfaces, Module Interfaces and communication between them. The level of assurance increases, as the design description details are provided from the general (subsystem level) to more (module level) detail.
4.	AGD_OPE.1 Operational user guidance	*User Manual for C-DOT Compact Encryption Module* document provides guidelines to understand the TSF's security functionality, instructions including warnings for its users to operate, configure, maintain and administrate TOE in a secure manner. It also specifies for each user their roles, user-accessible functions and privileges as per their group, such as, operator, System-Admin and Root-System. The main objective is to minimize the risk of human or other errors in operation that may deactivate, disable, or lead the TOE into an undetected insecure state.
5.	AGD_PRE.1 Preparative procedures	*Installation Manual for C-DOT Compact Encryption Module* document describes all necessary steps for secure installation of the TOE. It also provides TOE administrator with all information for preparing an intended operational environment necessary to meet the security objectives of the TOE.
6.	ALC_CMC.3 Authorisation controls	*Configuration Management Plan for C-DOT Compact Encryption Module* document describes the Authorisation controls to propagate Configuration Items (CIs), changes to CIs and release of CIs into TOE. The CM manager ensures Authorisation Control is in place into the CM system to develop and maintain the TOE throughout its life cycle.
7.	ALC_CMS.3	*Configuration Management Plan for C-DOT Compact*

S.N.	Security Assurance Requirement/Components	Description/Rationale
	Implementation representation CM coverage	*Encryption Module* document describes the CM system to be followed to develop and maintain the TOE. The CM plan describes the convention followed to uniquely identify the TOE, Configuration Items (CIs) and Non Configuration Items (Non-CIs). The CM manager ensures that the CM system is in place to develop and maintain the TOE throughout its life cycle.
8.	ALC_DEL.1 Delivery procedures	*Configuration Management Plan for C-DOT Compact Encryption Module* document describes the delivery procedure to be followed by developer to ensure delivery of TOE (New Released version or patches) to its consumer in a secure way. The necessary documents are part of delivery procedure, such as, Installation manual, Release Note so that the administrator has sufficient and necessary information to install the correct version of the TOE and bring it to in a secure state.
9.	ALC_DVS.1 Identification of security measures	The TOE development environment security measures and procedures to be followed to maintain the confidentiality and integrity of the TOE design and development is documented in *Configuration Management Plan for C-DOT Compact Encryption Module* document. The Configuration Management (CM) manager ensures that the said procedures are followed and maintains the TOE development environment.
10.	ALC_LCD.1 Developer defined life-cycle model	The Life-Cycle-Model (LCM) to develop and maintain the TOE is documented in *Configuration Management Plan for C-DOT Compact Encryption Module* document. The LCM assures that the TOE is developed and maintained throughout its life cycle in controlled and secured way.
11.	ATE_COV.2 Analysis of coverage	The analysis of the test coverage documented in *Test Case Document for Compact Encryption Module* shall demonstrate that all the functional test cases corresponding to each of the TSFIs in the functional specification have been executed and all the TSFIs are successfully tested.
12.	ATE_DPT.1 Testing: basic design	The analysis of the depth of testing documented in *Test Case Document for Compact Encryption Module* shall demonstrate that all the functional test cases corresponding to each of the TSF Sub-systems have been executed and all the TSF Sub-systems in the TOE design are successfully tested.
13.	ATE_FUN.1 Functional testing	*Test Case Document for CROS Software for Compact Encryption Module* document will provide test procedure for each of the test scenarios along with test environment, test condition, test data parameters and values so that one can perform an independent testing of each of the TSFIs and TSF Sub-systems. The test scenarios also capture any ordering dependencies on the results of other tests. In the Functional Test Report, each of the Test Cases has an expected result and actual result. These results are used for independently verifying the testing of TSFIs and TSF Sub-

S.N.	Security Assurance Requirement/Components	Description/Rationale
		systems along with the test coverage analysis and depth of testing.
14.	ATE_IND.2 Independent testing – sample	The assurance gained through Function Testing, Test Coverage and Depth analysis is independently verified by executing a set of functional test cases by evaluator to confirm TSF operates as specified in design documents and as per guidance documents. For this, evaluator may create a new test case and execute apart from test cases provided by developer in *Test Case Document for Compact Encryption Module.*
15.	AVA_VAN.2 Vulnerability analysis	The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE. The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Table 14: TOE SAR Rationale

Based on the threats defined according to the TOE environment, EAL3 assurance is selected as per CC Part 1 and CC Part 3 (Version 3.1, Revision 4) to establish a sufficient level of confidence in the security offered by the TOE. The TOE will be subject to independent vulnerability analysis for attack potential basic.

8.3.1 Dependencies Rationale

All functional and assurance requirements dependencies indicated in [CC2] and [CC3] have been satisfied, with the exception of the dependency of FMT_MSA.3 on FMT_MSA.1. The requirement for FMT_MSA.3 is included as a dependency from FDP_IFF.1, to specify how the security attributes associated with the information flow rules are initialised. The subsequent dependency from FMT_MSA.3 on FMT_MSA.1 allows for the specification of the management of the security attributes. However, for this TOE the management of the information flow security attributes is specified using FMT_MTD.1a. Therefore, there is no need to include FMT_MSA.1 as FMT_MTD.1a has satisfied the intent of the dependency. The extended component defined for SSH Server, Client Protocol and IPsec (FCS_SSHS_EXT.1, FCS_SSHC_EXT.1, FCS_IPSEC_EXT.1) has dependency on FCS_COP.1 for cryptographic algorithms and their operation to protect the management sessions. No additional dependencies have been identified.

9. APPENDIX - A: LIST OF AUDITABLE EVENTS

S.N.	SFR Family	Description	Auditable Event
1.	FAU_ARP.1	Security alarms	Actions taken due to potential security violations.
2.	FAU_GEN.1	Audit data generation	None (CC Part-2, Page 31)
3.	FAU_GEN.2	User identity association	None (CC Part-2, Page 31)
4.	FAU_SAR.1	Security Audit review	Reading of information from the audit records.
5.	FAU_SAR.2	Restricted Audit review	None
6.	FAU_SAA.1	Potential violation analysis	a) Enabling and disabling of any of the analysis mechanisms; b) Automated responses performed by the tool.
7.	FAU_STG.1	Protected audit trail storage	None (CC Part-2, Page 41)
8.	FDP_IFC.1	Subset information flow control	None (CC Part-2, Page 65)
9.	FDP_IFF.1	Simple security attributes	None
10.	FIA_ATD.1	User attribute definition	None. (CC Part-2, Page 91)
11.	FIA_SOS.1	Specification of secrets	Change of any tested secret (password).
12.	FIA_UAU.2	User authentication before any action	Unsuccessful use of the authentication mechanism.
13.	FIA_UID.2	User identification before any action	Unsuccessful use of the user identification mechanism, including the user identity provided.
14.	FIA_AFL.1	Authentication failure	a) Detect 3 consecutive unsuccessful authentication attempts of the same user account and the actions taken (lock the user account).
15.	FIA_UAU.5	Multiple authentication mechanisms	The final decision on authentication.
16.	FMT_MSA.3	Static attribute initialization	a) Modifications of the default setting of permissive or restrictive rules. b) All modifications of the initial values of security attribute.
17.	FMT_MTD.1a	Management of TSF data (CEM configuration)	All modifications to the values of CEM configuration data.
18.	FMT_MTD.1b	Management of TSF data (User attributes)	All modifications to the values of User attribute data.
19.	FMT_MTD.1c	Management of TSF data (Audit logs)	All attempts to modify or delete to the values of Audit logs data.
20.	FMT_MTD.1d	Management of TSF data (Date/time)	All modifications to the values of NTP server address and System clock data.
21.	FMT_MTD.1e	Management of TSF data (Sessions)	All modifications to the rules to establish management sessions.

S.N.	SFR Family	Description	Auditable Event
22.	FMT_SMF.1	Specification of Management Functions	Use of the management functions.
23.	FMT_SMR.1	Specification Management Roles	Modifications to the group of users that are part of a role.
24.	FPT_STM.1	Time stamps	Changes to the time.
25.	FPT_TST_EXT.1	Self Test	Self Test successful results.
26.	FPT_FLS.1	Fail Secure	None
27.	FTA_TSE.1	TOE session establishment	Denial of a session establishment due to the session establishment mechanism.
28.	FTA_MCS.1	Limit multiple concurrent sessions	Rejection of a new session based on the limitation of multiple concurrent sessions.
29.	FTA_SSL.3	Session Termination on Inactivity	Termination of an interactive session due to user inactivity.
30.	FCS_CKM.1	Cryptographic key generation	None
31.	FCS_CKM.4	Cryptographic key destruction	None
32.	FCS_COP.1	Cryptographic operation	None
33.	FCS_SSHC_EXT.1 : SSH	SSH Client Protocol	CLI command to initiate SSH session along with user identity and timestamp.
34.	FCS_SSHS_EXT.1 : SSH	SSH Server Protocol	a) Failure to establish an SSH Session. b) Establishment and Termination of SSH Session.
35.	FCS_IPSEC_EXT.1:IPsec	IPsec selected	a) IPsec initiating with x.x.x.x :Starting of the key exchange protocol with another trusted IT device b) SA init Established(I): Initiator successfully completed the key exchange protocol with another trusted IT device c) SA init Established(R): Responder successfully completed the key exchange protocol with another trusted IT device. d) Child SA (I) Established: Initiator successfully completed the traffic key exchange protocol with another trusted IT device e) Child SA (R) Established: Responder successfully completed the traffic key exchange protocol with another trusted IT device. f) Destroying IKE_SA to x.x.x.x :Destroying of the key exchange protocol with another trusted IT device g) Failed to establish IKE SA:

S.N.	SFR Family	Description	Auditable Event
			Failure in establishment of IKE SA.

Table 15: Auditable Events

[END OF DOCUMENT]