Security Target

TejNOS software running on Tejas Networks POTP / PTN Access Systems

[Version: 1.8]

P/N: 999-DOC000056-E

“This is a ***Controlled Document***”. No other document should be referred unless and until Tejas Networks replaces this document with the latest version. Only documents with controlled copy stamped should be used.

Template ID: D – GD;Ver 1.00
Revision History:

Revision	Date	Author	Reason	Reviewed By	Approved By
1.0	07/07/2015	ANAND .A.N	INITIAL DRAFT COPY	ANAND.A.N	Kannan
1.1	25/10/2016	ANAND .A.N	Changes implemented as per the OR dated 15/09/2016	ANAND.A.N	Kannan
1.2	8/11/2016	ANAND.A.N	Changes implemented as per the OR dated 08/11/2016	ANAND.A.N	Kannan
1.3	28/1/2019	Mathan	Changes implemented as per the OR dated 25/01/2019	ANAND.A.N	Kannan
1.4	19/02/2019	Mathan	TOE S/W details added	ANAND.A.N	Kannan
1.5	15/03/2019	Mathan	SFR modified	ANAND.A.N	Kannan
1.6	02/04/2019	Mathan	SFR modified	ANAND.A.N	Kannan
1.7	25/09/2019	Mathan	SFR Modified	ANAND.A.N	Kannan
1.8	14/11/2019	Mathan	SFR Modified	ANAND.A.N	Kannan

Table of Contents

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	**:** Security Target TejNOS software running on Tejas Networks POTP / PTN Access Systems
ST Revision	**:** 1.8
ST Publication Date	**:** 14/11/2019

1.2 TOE Reference

TOE Reference	**:**TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 - ST Organization and Section Descriptions

1.4 Document Terminology

The following table describes the acronyms used in this document:

TERM	DEFINITION
3DES	Triple Data Encryption Standard
ACL	Access control List
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CC	Common Criteria version 3.1
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMAP4	Internet Message Access Protocol 4
MD5	Message Digest 5
MSP	Managed Service Provider
MSPP	Multiservice Provisioning Platform
NTP	Network Time Protocol
OSP	Organizational Security Policy
PKCS	Public-Key Cryptography Standards
POP3	Post Office Protocol 3
POTP	Packet optical transport platform
PTN	Packet transport network
RFC	Request for Comment
RSA	Rivest Shamir Adelman
SA	Security Association
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMNP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SRRD	System requirement document
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
SYSLOG	System Log
TDES	Triple Data Encryption Standard
TejNOS	Tejas Networks Operating System
TLS	Transport Layer Security

Table 2 - Acronyms Used in Security Target

1.5 Conventions

The CC defines operations on security requirements. The font conventions listed below state the conventions used in this ST to identify the operations.

Assignment: indicated in italics

Selection: indicated in underlined text

Assignments within selections: indicated in italics and underlined text

Refinement: indicated with bold text

Iterations of security functional requirements may be included. If so, iterations are specified at the component level and all elements of the component are repeated. Iterations are identified by numbers in parentheses following the component or element (e.g., (1), (2), (3)).

1.6 TOE Overview

The TOE is the TejNOS EN software running on POTP/PTN access system TJ1400 & TJ1600 series of products for management of the system and control of user data flow.

TJ1400 Ultra-Converged Broadband family of products is one of the industry’s most feature-rich packet access and aggregation platforms. It provides unparalleled integration of Access, Transport and IP Network technologies in one integrated box and introduces a revolutionary way of building modern-day telecom infrastructure. TJ1400 Ultra-Converged Broadband platform is designed for cost-optimized delivery of Mobile Backhaul, Broadband Access and Enterprise Cloud Services migration infrastructure.

The TJ1600 balances Packet and TDM transport in a way unique to the industry. Its hybrid architecture allows for three configurations; TDM with Packet Transport, Hybrid TDM and Packet Transport and all DWDM Optical Transport using the same hardware, software and features. This flexibility creates a unique opportunity for network designs by allowing every service to be optimized based upon the service requirements, not the limitations of a particular transport technology.

Features under evaluation

- Manages users and their profiles
- User Identification and Authentication
- Audit log generation and verification
- User Session Management
- Password complexity and usage settings configuration
- Cryptographic Support

- Trusted Path
- Cross connect management

Features not under evaluation

- Alarms/Fault: Filtering and managing alarms
- Configuration: MSP groups, overhead tunnel, Environment alarm input and SNMP traps.
- Node facility management
- Timing / Clock block to Node Synchronization
- License enabling
- Performance monitoring
- Maintenance
- Communication of TOE with IT entities like Radius or AAA server
- Synchronize Node element clock times in a network like NTP server

1.7 TOE Description

1.7.1 Physical Boundary

TOE Type: Software package running in POTP / PTN Access systems.

Tejas Network POTP/PTN Access system model TJ1400 and TJ1600 are completely self-contained, housing the software and hardware necessary to perform all functions. The TOE, TejNOS Software has two basic components Data plane and control & management plane. The data plane (sometimes known as the user plane, forwarding plane, carrier plane or bearer plane) is the part of a network that carries user traffic. Control and management plane manages the security function of the TOE and sets the control for the data flow in the data plane.

The TOE has logical interfaces for the end users including Admin users and for data traffic. The admin interface to the TOE includes a Web-Based administrative interface. The end user interfaces to the TOE uses Web-Based user interface.

The TOE includes a proprietary web server developed by Tejas, which provides the main interface for both users and administrators of the TOE. The web server provides users an interface to submit connection requests via an HTTPS encrypted tunnel. The web server provides administrators an interface to administrate the TOE using a web browser. The web server component is included as part of the TOE. **TOE shall be installed and managed only in private network through NMS/EMS and not in public network.**

The TOE is realized in combination with the hardware. Table -3: provides Evaluated Configuration of hardware models and software versions for TOE components and Non TOE components.

The TOE boundary is shown below:

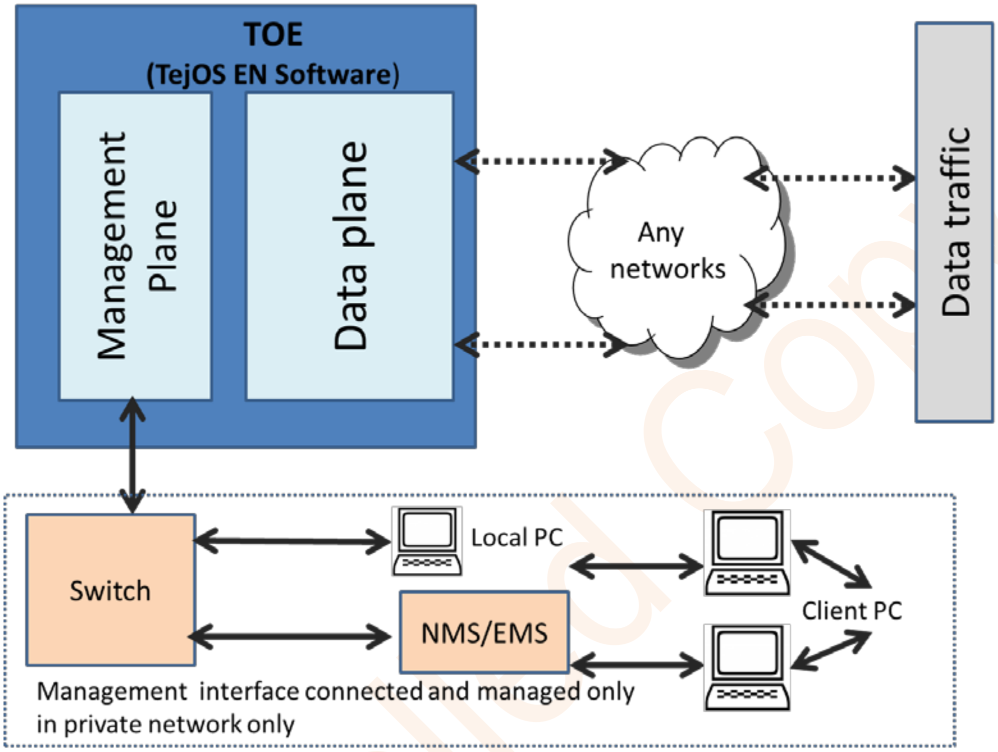


Figure 1 – TOE Boundary

The TejNOS provides the internal infrastructure to perform the security functions of the TOE, including the implementation of the following:

- Access Control System
- Authentication System
- Protocol and Connection Handlers
- System Logging Facility

The above areas are further detailed in the proprietary architectural and design evidence for this evaluation.

The TOE appliances utilize a Linux operating system (TejNOS Operating System in the figure above) that includes the Kernel Version 2.6.32. The operating system is relied upon for all access to the physical hardware devices connected to the TOE and for providing reliable time stamping.

The TOE includes various software clients specified in Table 3 – Evaluated Configuration for the TOE running on remote IT systems. These clients open and manage a secure connection to the appliance for user connections.

The following tables show hardware and software components included in TOE and Non-TOE:

TOE COMPONENT	VERSION/MODEL NUMBER
Appliance Software	TejNOS EN software Version 6.2 and Version 10.0 running on Tejas Networks POTP/PTN Access Systems Model TJ1400 and TJ1600 respectively.
Appliance Hardware	• TJ1400 POTP / PTN (Type-7SR, Type-3SR & Type-5SEP) • TJ1600 POTP / PTN

Non-TOE Components	Description / Version
Client	o Windows OS (all version supported) o Linux/Ubuntu OS
Management Workstation	General management of the unit from a PC hosted Management Interface. All management services occur only through this interface via UDP/IP protocol. o TejEMS /TejNMS o Windows OS (All version supported) o Linux/Ubuntu OS
RADIUS or TACACS+ AAA Server	This includes any authentication server that can be leveraged for remote user authentication.
NTP Server	Synchronize Node element clock times in a network

Table 3 - Configuration for the Non-TOE

The following table shows TOE delivery details:

S/N	Part Number	Description	Version
1	142-SW0000130-S	TejNOS EN software Version 6.2 running on Tejas Networks POTP/PTN Access System Model TJ1400	6.2
2	142-SKU000059-P	TJ1400 POTP / PTN System	1.2
3	170-SW0000034-S	TejNOS EN software Version 10.0 running on Tejas Networks POTP/PTN Access System Model TJ1600	10.0
4	170-PCA000052-E	TJ1600 POTP / PTN System	2.6
5	142-DOC000110-E	TJ1400 Preparative guidance document	1.8
6	142-DOC000111-E	TJ1400 Operation guidance document	1.8
7	170-DOC000097-E	TJ1600 Preparative guidance document	1.8
8	170-DOC000098-E	TJ1600 Operation guidance document	1.6

Table 4 – TOE delivery details

1.7.2 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.

TSF	DESCRIPTION

Security Audit	TOE generates audit records for security events. The administrator is the only role with access to the audit trail and has the ability to view the audit trail.
Cryptographic Operations	TOE supports secure communications between users and the TOE and between TOE components. This encrypted traffic prevents Modification and disclosure of user information.
User Data Protection and Protection of the TSF	TOE provides an information flow security policy. The security policy limits traffic to specified ports.
Identification and Authentication	All users are required to perform identification and authentication before any management actions are performed.
Security Management	TOE provides a wide range of security management functions. Administrators can configure the TOE, manage users, the information flow policy, and audit among other routine maintenance activities.
TOE Access	TOE provides time initiated termination of any interactive session that is open for a more than specified duration.
Time Stamps	TOE provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware.
Trusted Path	Connection to and from the TOE are protected using the protocols mentioned within the Cryptographic Support section. Trusted paths are used to secure all user sessions through HTTPS. All connections for the TOE are protected using the HTTPS cryptographic mechanism.

Table 5 - Logical Boundary Descriptions

1.8 TOE Configuration details

TJ1400 (Type-7SR) Overview : The TJ1400 (Type-7SR) is a 2 unit base chassis supporting redundant cross-connect fabric, timing/synchronization subsystem and control processor subsystem and east/west aggregate ports on separate circuit packs. It also has redundant power supply modules enabling power supply redundancy.

Figure-2 Model: TJ1400 (Type-7SR)

TJ1600 POTP Overview: The TJ1600 POTP is an 8U high, half-depth, multi-slot product (9 service slots in addition to 2 cross connect card slots), supporting redundancy of cross-connect fabric, timing/synchronization subsystem, and control processor subsystem.

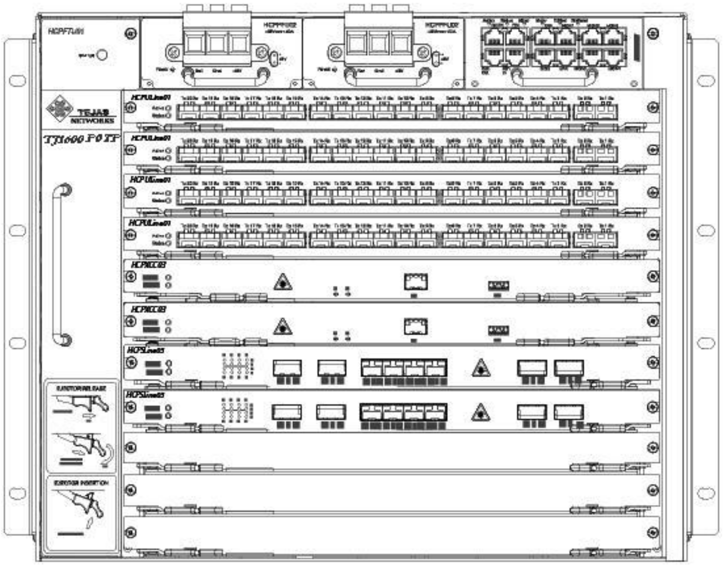


Figure-3 Model: TJ1600 (Type-7SR)

The TOE interfaces are comprised of the following:

1. Networks traffic
   - E1 interface (optional)
   - E3 interface (optional)
   - STM-1/4/16/64 interface through optical SFP /XFP ports
   - OTN-1/OTN-2 optical interfaces [CFP ports]
   - 10/1000 Base –T electrical interface for Ethernet traffic.
   - 1/10 Gige interface through optical SFP /XFP ports
2. Management interface
   - 10/100 Base –T electrical interface (one of the Ethernet traffic port can be used has management interface).

1.9 TOE Software component details

The TJ1400 and TJ1600 system is built around below listed aggregate cards which have the Processor complex where the core S/W (TOE) is running. Aggregate cards are selected based on the required cross connect capacity. There is no change in security feature requirements and functionality of the management plane and only the data plane are modified based on the cross connect capacity of the card.

Following is the Evaluated TOE configuration and (S/W) version.

Product and cards	Evaluated TOE configuration and (S/W) Version
TJ1400 with XA60G / XA60G-ET	Software version : 6.2 Build Release • xa60g-ppc-REL_6_2_0_a75_1_55.squash.img • fw_xa60g_1_35.tgz
TJ1600 with HCPXCC03	Software version : 10.0 Build Release • xcc360g-ppc-REL_10_0_2_a49_25.squash.img • fw_lpss11_6_29.tgz

- TejNOS EN Supported Software version for TJ1400

Cross Connect Cards	Supported (S/W) Version
XA14ET	6.0
XA140T5	6.0
XA10G	6.2
XA20G	6.2
XA60G/XA60G-ET	6.2 and 10.0
CEF4	6.2 and 10.0

- TejNOS EN Supported Software version for TJ1600

Cross Connect Cards	Supported (S/W) Version
HCPXCC01	8.0 and 10.0
HCPXCC03	8.0 and 10.0
HCPXCC04	10.0
OSMC01	10.0

1.10 TOE Application Network Diagram

Following is the TOE application network diagram.

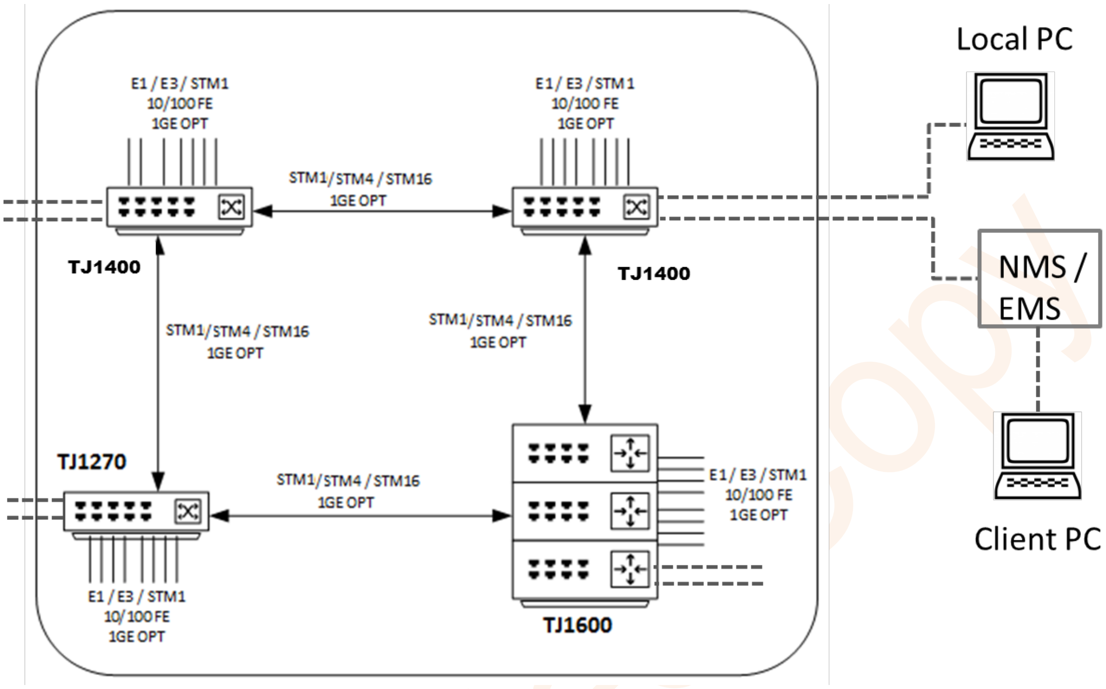


Figure-4 TOE Application Network Diagram

2. Conformance Claims

2.1 CC Conformance Claim

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

2.2 PP Claim

The TOE and ST do not claim conformance to any registered Protection Profile.

2.3 Package Claim

The TOE and ST claim conformance to the EAL2 assurance package defined in Part 3 of the Common Criteria Version 3.1 Revision 5, April 2017

2.4 Conformance Rationale

Conformance as per 2.1 and 2.3

3. Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required
- Any organizational security policy statements or rules with which the TOE must comply
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.AUDACC	Persons may not be accountable for the actions that they conduct because the audit records are generated and reviewed, thus allowing an attacker to modify the behavior of TSF data without being detected.
T.AUDFUL	An unauthorized person may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions. Audit record may fail to record auditable events in case of audit trail exceeds the storage capacity
T.MEDIAT	An unauthorized person may change the flow policy to send information through the TOE which results in the exploitation of resources.
T.NOAUTH	An unauthorized person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
T.OLDINF	An unauthorized person may gather residual information from a previous information flow or internal TOE data by monitoring the padding of the information flows from the TOE.

THREAT	DESCRIPTION
T.PROCOM	An unauthorized person or unauthorized external IT entity may be able to view, modify, and/or delete security related information or information properties sent between a remotely located authorized administrator and the TOE.
T.REPLAY	An unauthorized person may replay valid identification and authentication data obtained while monitoring the TOE's network interface to access functions provided by the TOE.
T.SELPRO	An unauthorized person may read, modify, or destroy security critical TOE configuration data.
T.TUSAGE	The TOE may be inadvertently configured, used and administered in an insecure manner by either authorized or unauthorized persons.

Table 6 - Threats Addressed by the TOE

The IT Environment does not explicitly addresses any threats.

3.2 Organizational Security Policies

The TOE is not required to meet any organizational security policies.

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
A.NOEVIL	Authorized administrators are non-hostile and follow all administrator guidance.
A.PHYSEC	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.PUBLIC	The TOE does not host public data.
A.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 7 - Assumption

4. Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCOUN	The TOE must provide user accountability for information flow through the TOE and for authorized administrator use of security functions related to audit.
O.AUDREC	The TOE must provide a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes. In case of audit trail full , the TOE shall delete oldest record to make space for current record.
O.ENCRYP	The TOE must protect the confidentiality of its dialogue with an authorized administrator and/or user through encryption.
O.IDAUTH	The TOE must uniquely identify and authenticate the claimed identity of all users, before granting a user access to TOE functions.
O.MEDIAT	The TSF must prevent to mediate the flow of all information by unauthorized users and must ensure that residual information from a previous information flow is protected and not transmitted in any way.
O.SECFUN	The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality.
O.SECKEY	The TOE must provide the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt management traffic flows.
O.SECSTA	Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must not compromise its resources.
O.SELPRO	The TOE must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
O.SINUSE	The TOE must prevent the reuse of authentication data for users attempting to authenticate at the TOE from a connected network.

Table 8 - TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.ADMTRA	Authorized administrators are trained to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.GUIDAN	The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
OE.PHYSEC	Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from any physical attack.
OE.PUBLIC	The TOE does not host public data.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 9 - Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies.

THREATS / ASSUMPTIONS OBJECTIVES	T.AUDACC	T.AUDFUL	T.MEDIAT	T.NOAAUTH	T.OLDINF	T.PROCOM	T.REPLAY	T.SELPRO	T.TUSAGE	A.GENPUR	A.NOEVIL	A.PHYSEC	A.PUBLIC	A.SINGEN
O.ACCOUN	✓													
O.AUDREC	✓	✓												
O.ENCRYP						✓								
O.IDAUTH				✓										
O.MEDIAT			✓		✓									
O.SECFUN		✓						✓						
O.SECKEY						✓								
O.SECSTA								✓						
O.SELPRO		✓						✓						
O.SINUSE							✓							
OE.ADMTRA									✓		✓			
OE.GENPUR										✓				
OE.GUIDAN									✓					
OE.PHYSEC												✓		
OE.PUBLIC													✓	
OE.SINGEN														✓

Table 10 - Mapping of Assumptions, Threats, and OSPs to Security Objectives

4.3.1 Rationale for Security Threats to the TOE

THREAT	RATIONALE
T.AUDACC	This threat is completely countered by • O.ACCOUN which ensures the TOE provides user accountability for information flow through the TOE and for Administrator use of security functions related to audit. • O.AUDREC which ensures The TOE provides a means to record a readable audit trail of security-related events, with accurate dates and times, and a means to search the audit trail based on relevant attributes
T.AUDFUL	This threat is completely countered by • O.AUDREC which will delete oldest record to make space for current record • O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality. • O.SELPRO which ensures the TOE protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
T.MEDIAT	This threat is completely countered by • O.MEDIAT which ensures that the TSF prevents to mediate the flow of all information by unauthorized users
T.NOAUTH	This threat is completely countered by • O.IDAUTH which ensures the TOE uniquely identifies and authenticates the claimed identity of all users before granting a user access to TOE functions.
T.OLDINF	This threat is completely countered by • O.MEDIAT which ensures that residual information from a previous information flow is protected and not transmitted.
T.PROCOM	This threat is completely countered by • O.ENCRYP which ensures the TOE protects the confidentiality of its dialogue with an Administrator through encryption. • O.SECKEY which ensures the TOE provides the means of protecting the confidentiality of cryptographic keys when they are used to encrypt/decrypt traffic flows
T.REPLAY	This threat is completely countered by • O.SINUSE which the TOE prevents the reuse of authentication data for users attempting to authenticate at the TOE from a connected network
T.SELPRO	This threat is completely countered by • O.SECSTA which ensures the TOE does not compromise its resources

THREAT	RATIONALE
	or those of any connected network upon initial start-up or recovery from an interruption in TOE service. • O.SECFUN The TOE must provide functionality that enables an authorized administrator to use the TOE security functions, and must ensure that only authorized administrators are able to access such functionality • O.SELPRO which ensures the TOE protects itself against attempts by unauthorized users to bypass, deactivate, or tamper with TOE security functions.
T.TUSAGE	This threat is completely countered by • OE.ADMTRA which ensures the operational environment provides well- trained administrators to appropriately install, configure, and maintain the TOE within its evaluated configuration according to the installation and guidance documents for the TOE. • OE.GUIDAN which ensures the operational environment provides a secure manner of TOE delivery, installation, administration, and operation.

4.3.2 Rationale for Security Objectives to the TOE

OBJECTIVE	RATIONALE
O.ACCOUN	This security objective is necessary to counter the threat: T.AUDACC because it requires that users are accountable for information flows through the TOE and those administrators, operator2, operator and user admins are accountable for the use of security functions related to audit.
O.AUDREC	This security objective is necessary to counter the threat: T.AUDACC and T.AUDFUL by requiring a readable audit trail and a means to search the information contained in the audit trail. It will delete oldest record to make space for current record for possible audit data loss in case of audit trail full.
O.ENCRYP	This security objective is necessary to counter the threat T.PROCOM by requiring that an administrator, operator2, operator and user use encryption when performing administrative functions on the TOE.
O.IDAUTH	This security objective is necessary to counter the threat: T.NOAUTH because it requires that users be uniquely identified before accessing the TOE.
O.MEDIAT	This security objective is necessary to counter the threats: T.MEDIAT and T.OLDINF which have to do with changing information flow control policy to flow through the TOE. This security objective requires that all information that passes through the networks is mediated by the TOE and that no residual information is transmitted
O.SECFUN	This security objective is necessary to counter the threat T.SELPRO by requiring that the TOE provides functionality that ensures that only the administrator, operator2, and user admin has access to the TOE security functions.
O.SECKEY	The objective mitigates the threat of data modification or disclosure by ensuring that cryptographic keys are generated sufficiently, kept confidential, and destroyed property (T.PROCOM).

OBJECTIVE	RATIONALE
O.SECSTA	This security objective ensures that no information is comprised by the TOE upon startup or recovery and thus counters the threat T.SELPRO.
O.SELPRO	This security objective is necessary to counter the threats: T.SELPRO and T.AUDFUL because it requires that the TOE protect itself from attempts to bypass, deactivate, or tamper with TOE security functions.
O.SINUSE	This security objective is necessary to counter the threats: T.REPLAY because it requires that the TOE prevent the reuse of authentication data so that even if valid authentication data is obtained, it will not be used to mount an attack.
OE.ADMTRA	This non-IT security objective is necessary to counter the threat T.TUSAGE and support the assumption A.NOEVIL because it ensures that authorized administrators receive the proper training in the correct configuration, installation and usage of the TOE.
OE.GENPUR	There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.
OE.GUIDAN	This non-IT security objective is necessary to counter the threat: T.TUSAGE because it requires that those responsible for the TOE ensure that it is delivered, installed, administered, and operated in a secure manner.
OE.PHYSEC	The objective to provide physical protection for the TOE supports the assumption that the TOE will be located within controlled access facilities, which will prevent unauthorized physical access (A.PHYSEC).
OE.PUBLIC	The TOE does not host public data.
OE.SINGEN	Information cannot flow among the internal and external networks unless it passes through the TOE.

Table 11 - Mapping of Threats, Policies, and Assumptions to Objectives

5. Extended Components Definition

5.1 Definition of Extended Components

There are no extended components in this Security Target.

6. Security Functional Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit Review
	FAU_STG.1	Protected Audit Trail Storage
	FAUSTG.3	Action in case of possible audit data loss
Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.2	Cryptographic Key Distribution
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1	Cryptographic Operation
User Data Protection and Protection of TSF	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
	FDP_RIP.1	Subset Residual Information Protection
Identification and Authentication	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_MSA.1	Management of Security Attributes
	FMT_MSA.2	Secure Security Attributes
	FMT_MSA.3	Static Attribute Initialization
	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Time Stamps	FPT_STM.1	Reliable Time Stamps
TOE Access	FTA_SSL.3	TSF-initiated termination
Trusted Path	FTP_TRP.1	Trusted Path

Table 12 - TOE Security Functional Requirements

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, which are summarized in the following:

6.2 Security Audit (FAU)

6.2.1 FAU_GEN.1 – Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
(Note: Audit function gets on / off along with the TOE startup/shutdown and there is no interface to stop the audit log function.)

a) All auditable events for the [not specified] level of audit; and

b) [*The events in column two of Table 13 – Auditable Events*]

FAU_GEN.1.2 The TSF shall record within each audit record at last the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 13 – Auditable Events*].

SFR	EVENT	DETAILS
FMT_SMR.1	Modifications to the users that are part of a role.	The identity of the Administrator performing the modification and the user identity being associated with a role
FIA_UID.2	All use of the user identification mechanism.	None
FIA_UAU.2	Any use of the user authentication mechanism.	None
FPT_STM.1	Changes to the time.	The identity of the Administrator performing the Operation.
FMT_MOF.1	• Create, delete, and modify information flow security policy rules that permit or deny information flows • Create, delete, and modify user attribute values • Enable and disable external IT entities from communicating to the TOE by Admin	As defined in the FMT_MTD.1;

Table 13 - Auditable Events

6.2.2 FAU_SAR.1 – Audit Review

FAU_SAR.1.1 The TSF shall provide [*an Administrator*] with the capability to read [*all audit 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.

6.2.3 FAU_STG.1 – Protected Audit Trail Storage

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 [*<u>prevent</u>*] unauthorized modifications to the audit records in the audit trail.

6.2.4 FAU_STG.3 – Action in case of possible Audit Data Loss

FAU_STG.3.1 The TSF shall [*continue audit log generation by deleting oldest audit records*] if the audit record exceeds [*limit approximately 1000 records*]

6.3 Cryptographic Support (FCS)

6.3.3 FCS_CKM.1 – Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*ANSI X9.31*] and specified cryptographic key sizes [*128-bits or 256-bit AES, CAMELLIA and SEED, key*] that meet the following: [*FIPS 197 for AES*].

6.3.4 FCS_CKM.2 – Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [RSA] that meets the following: [*RSA_WITH_CAMELLIA_CBC_SHA or RSA_WITH_AES_GCM_SHA or RSA_WITH_AES_CBC_SHA or RSA_WITH_AES_CCM or RSA_WITH_SEED_CBC_SHA or RSA_WITH_IDEA_CBC_SHA in the TLS specification in RFC 2246*].

6.3.5 FCS_CKM.4 – Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*overwrite*] that meets the following: [*Federal Information Processing Standard 140-2 requirements for key zeroization*].

6.3.6 FCS_COP.1 – Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [*the operations described in Table 14 – Cryptographic Operations*] in accordance with a specified cryptographic algorithm [*multiple algorithms in the modes of operation described in Table 14 – Cryptographic Operations*] and cryptographic key sizes [*multiple key sizes described in Table 14 – Cryptographic Operations*] that meet the following: [*multiple standards described in Table 14 – Cryptographic Operations*].

OPERATIONS	ALGORITHM (MODE)	KEY SIZE IN BITS	STANDARDS
Encryption And Decryption	AES (CBC mode)	128, 256	FIPS 197
	CAMELLIA	128, 256	--
	IDEA	128	--
	SEED	128	--
Hashing	SHS (SHA-1)	160 (size of digest)	FIPS 180-2
	MD5	128	RFC 1321
Random Number Generation	ANSI X9.31	Not Applicable	ANSI X9.31

Table 14 - Cryptographic Operations

6.4 Information Flow Control (FDP)

6.4.3 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [*Flow control SFP*] based on the following types of subject, information and operation: [

- *Subject: Remote network systems sending data / packet through a port on the NEs*
- *Information: Data /packet and*
- *Operation: Forwarding of received data / packets*]

6.4.4 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the data /traffic filtering SFP based on the following types of subject and information security attributes: [

- *Subject attributes: Receiving port and configured ACL;*
- *Information attributes: Presumed source and destination port.]*

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: [

- *If an ACL is configured for the receiving port, Data /packet are forwarded if the presumed source or destination port is explicitly included in the ACL.]*

FDP_IFF.1.3 The TSF shall enforce the [*No additional rules*].

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

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

6.4.5 FDP_RIP.1 – Subset Residual Information Protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*allocation of the resource to*] the following objects: [*destination*].

6.5 Identification and Authentication (FIA)

6.5.1 FIA_ATD.1 – User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*identity, association of a human user with a role, password*].

6.5.2 FIA_SOS.1 – Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet: [

1. *Exactly eight (8) character only,*
2. *It can be of eight (8) numeric characters,*
3. *It can be of eight (8) alphabetic characters,*
4. *Combination of both uppercase and lowercase alphabetic characters,*

5. *Combination of alphanumeric and special characters*

6.5.3 FIA_UAU.2 – User Authentication before Any Action

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.

6.5.4 FIA_UID.2 – User Identification before Any Action

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.

6.6 Security Management (FMT)

6.6.1 FMT_MOF.1 – Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behavior of, disable, enable, and modify the behavior of the functions*] [

1. *Create and delete information flow security policy rules that permit or deny information flows to [operator, operator2 and Admin];*
2. *Create, delete, and modify user attribute values by Admin user;*
3. *Enable and disable external IT entities from communicating to the TOE by Admin;*
4. *Modify and set the time and date as per FMT_MTD.1 ;*
5. *Archive the audit trail;] to [the Admin role]*
6. *Configuration of inactive session timeout to Admin.*

Management Function	User Roles – Privileges			
	USER	OPERATOR	OPERATOR2	ADMIN
System Time	No Access*	No Access*	View	View/Modify
Inventory	View/Modify	View/Modify	View/Modify	View/Modify
Protection	View	View	View	View/Modify
Configuration	View	View/Modify	View/Modify	View/Modify
License	View	View	View	View/Modify
Faults	View	View/Modify	View/Modify	View/Modify
Profiles	View	View/Modify	View/Modify	View/Modify
Performance	View	View	View	View/Modify
Security	View Manage User	View Manage User	View Manage User	View/Modify All options
Maintenance	View	View	View	View/Modify
Maintenance > Loopback	View	View/Modify	View/Modify	View/Modify
Maintenance > Diagnostics	View	View	View	View/Modify
Maintenance > Configuration Management	No Access*	No Access*	View/Modify	View/Modify
Maintenance > Upgrade operation	No Access*	No Access*	View/Modify	View/Modify

Table 15 - Management of Security Functions Behaviour

6.6.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [*Information flow control SFP*] to restrict the ability to [create & delete] the security attributes [*information flow security policy rules that permit or deny information flows*] to [*as defined in the FMT_MTD.1*].

6.6.3 FMT_MSA.2 – Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for [*security attributes listed as per the Information flow control]*.

6.6.4 FMT_MSA.3 – Static Attribute Initialization

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

FMT_MSA.3.2 The TSF shall allow the [*the Administrator role*] to specify alternative initial values to override the default values when an object or information is created.

6.6.5 FMT_MTD.1 – Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to control the [*data described in Table 15 – Management of Security Functions Behaviour*] to [*User's privilege / role as defined in the below table*]:

User Identity	User Privilege			
	Audit log Viewing /Archive	Information flow control	Time Setting	User Security attributes modification
User	✗	✗ (only viewing)	✗	✗
Operator	✗	✓	✗	✗
Operator2	✗	✓	✓	✗
Admin	✓	✓	✓	✓

Table 16 - Management of TSF data

6.6.6 **FMT_**SMF.1 - Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions as defined in the FMT_MTD.1: [

a) *Create, delete and view information flow security policy rules that permit or deny information flows;*
b) *Create, delete, modify, and view user attribute values defined in FIA_ATD.1;*
c) *Enable and disable external IT entities from communicating to the TOE;*
d) *Modify and set the time and date;*
e) *Archive, clear, and review the audit trail*].
f) *Configuration of inactive session timeout.*

6.6.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [User, Operator, Operator2, and Admin].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.7 Time Stamps

6.7.1 FPT_STM.1 Reliable Time Stamps

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

6.8 TOE Access (FTA)

6.8.1 FTA_SSL.3 – TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an inactive session after a [*default 60 minutes session period or as defined by Admin role*].

6.9 Trusted Path (FTP)

6.9.1 FTP_TRP.1 –Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself 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 [modification or disclosure].

FTP_TRP.1.2 The TSF shall permit [*remote users*] 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 communication after authentication*].

6.10 Security Functional Requirements for the IT Environment

There are no Security Functional Requirements for the IT Environment.

6.11 Security Assurance Requirements

The Security Assurance Requirements for this evaluation are listed in Section 6.12.3 – Security Assurance Requirements.

6.12 Security Requirements Rationale

6.12.1 Security Functional Requirements

The following table provides the correspondence mapping between security objectives for the TOE and the requirements that satisfy them.

OBJECTIVES / SFR	O.IDAUTH	O.MEDIAT	O.SECSTA	O.SECKEY	O.ENCRYP	O.SELPRO	O.AUDREC	O.ACCOUN	O.SECFUN	O.SINUSE
FAU_GEN.1							✓	✓		
FAU_SAR.1							✓			
FAU_STG.1						✓			✓	
FAU_STG.3							✓			
FCS_CKM.1				✓						
FCS_CKM.2				✓						
FCS_CKM.4				✓						
FCS_COP.1					✓					
FDP_IFC.1		✓								
FDP_IFF.1		✓								
FDP_RIP.1		✓								
FIA_ATD.1	✓									✓
FIA_SOS.1	✓									
FIA_UAU.2	✓									
FIA_UID.2	✓							✓		
FMT_MOF.1			✓						✓	
FMT_MSA.1		✓								
FMT_MSA.2		✓								
FMT_MSA.3		✓						✓		
FMT_MTD.1	✓	✓	✓		✓				✓	
FMT_SMF.1									✓	
FMT_SMR.1									✓	
FPT_STM.1							✓			
FTA_SSL.3						✓				
FTP_TRP.1					✓					

Table 17 - Mapping of TOE Security Functional Requirements and objectives

6.12.2 Sufficiency of Security Requirements

The following table presents a mapping of the rationale of TOE Security Requirements to Objectives.

SFR	RATIONALE
FAU_GEN.1	This component outlines what data must be included in audit records and what events must be audited. This component traces back to and aids in meeting the following objectives: O.AUDREC and O.ACCOUN.
FAU_SAR.1	This component ensures that the audit trail is understandable. This component

SFR	RATIONALE
	traces back to and aids in meeting the following objective: O.AUDREC.
FAU_STG.1	This component is chosen to ensure that the audit trail is protected from tampering. Only the Administrator is permitted to view and download the audit trail. This component traces back to and aids in meeting the following objectives: O.SELPRO and O.SECFUN.
FAU_STG.3	This component ensures that no current audit events are lost in case of audit storage space is full by deleting oldest audit records and aids to meet the objective O.AUDREC
FCS_CKM.1	This component ensures that cryptographic keys and parameters are generated with standards-based algorithms (O.SECKEY).
FCS_CKM.2	This component provides secure key distribution to remote trusted IT products (users or other instances of TOE). The TOE to perform authentication using digital certificates, ensuring the source is trusted (O.SECKEY).
FCS_CKM.4	This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications (O.SECKEY).
FCS_COP.1	This component ensures that when all users communicate with the TOE remotely from an internal or external network that robust algorithms are used to encrypt such traffic. This component traces back to and aids in meeting the following objective: O.ENCRYP.
FDP_IFC.1	This component identifies the ports involved in the flow control SFP (i.e., forwarding / sending information to one port to another port). This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_IFF.1	This component identifies the type of subject and information attributes and permits information flow between the source and destination ports. Then the policy is defined by saying where information is permitted to flow. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FDP_RIP.1	This component ensures that any residual information content pertaining to a resource accessible by a user, such as access to a file server, is not made available upon the allocation of that resource to another designation port. This component traces back to and aids in meeting the following objective: O.MEDIAT.
FIA_ATD.1	This component exists to provide users with attributes to distinguish one user from another, for accountability purposes and to associate the role chosen in FMT_SMR.1 with a user. This component traces back to and aids in meeting the following objectives: O.IDAUTH and O.SINUSE.
FIA_SOS.1	This component exists to ensure that passwords generated by users can be verified to meet the defined minimum password strength requirements. This component traces back to and aids in meeting the following objective: O.IDAUTH.

SFR	RATIONALE
FIA_UAU.2	This component requires successful authentication of a role before having access to the TSF and as such aids in meeting O.IDAUTH.
FIA_UID.2	This component requires successful identification of a role before having access to the TSF and as such aids in meeting O.IDAUTH and O.ACCOUN.

SFR	RATIONALE
FMT_MOF.1	This component was chosen to consolidate all TOE management /

SFR	RATIONALE
	administration / security functions. This component traces back to and aids in meeting the following objectives: O.SECFUN and O.SECSTA.
FMT_MSA.1	This component restricts the ability to create, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way and as such aids in meeting O.MEDIAT.
FMT_MSA.2	This component restricts the ability to create, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way and as such aids in meeting O.MEDIAT.
FMT_MSA.3	This component restricts the ability to create, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way and as such aids in meeting O.MEDIAT and O.ACCOUN.
FMT_MTD.1	This component restricts the ability to modify the Authenticated User SFP, and as such aids in meeting O.ENCRYP, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify identification and authentication data, and as such aids in meeting O.IDAUTH, O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to delete audit logs, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify the date and time and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN. This component restricts the ability to modify the data relating to TOE access locations, and as such contributes to meeting O.MEDIAT, O.SECSTA, and O.SECFUN.
FMT_SMF.1	This component was chosen in an attempt to consolidate all TOE management/administration/security functions. This component traces back to and aids in meeting the following objective: O.SECFUN.
FMT_SMR.1	This component ensures that roles are available to allow for varying levels of administration capabilities and restricts access to perform TSF relevant functionality depending on the role assigned to an authorized administrator. This component traces back to and aids in meeting the following objective: O.SECFUN.
FPT_STM.1	FAU_GEN.1 depends on this component. It ensures that the date and time on the TOE is dependable. This is important for the audit trail. This component traces back to and aids in meeting the following objective: O.AUDREC.
FTA_SSL.3	This component protects the TOE's communication path by terminating default 60 minutes idled session time and terminating sessions lasting longer than 300 minutes. This component traces back to and aids in meeting the following objective: O.SELPRO
FTP_TRP.1	This component works with the encryption provided in the FCS_COP.1 requirement to ensure that user authentication data or other user data is protected from disclosure and modification. This component traces back to and aids in meeting the following objective: O.ENCRYP.

Table 18 - Rationale for TOE SFRs to Objectives

The following table presents a mapping of the rationale of TOE Objectives to Security Requirements:

OBJECTIVE	RATIONALE
O.ACCOUN	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited • FIA_UID.2 ensures that users are identified to the TOE
O.AUDREC	This objective is completely satisfied by • FAU_GEN.1 which outlines what events must be audited • FAU_SAR.1 which requires that the audit trail can be read • FAU_STG.3 which requires that action to be taken in case of possible audit data loss. • FPT_STM.1 ensures that reliable time stamps are provided for audit records
O.ENCRYP	This objective is completely satisfied by • FCS_COP.1 which ensures robust algorithms are used to support encrypted communications between users and TJ1400 and TJ1600 Access • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations • FTP_TRP.1 which ensures all communications between users and Secure Access is encrypted via a secure connection using encryption & decryption algorithms

OBJECTIVE	RATIONALE
O.IDAUTH	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with use. • FIA_SOS.1 which specifies metrics for authentication, and aids in meeting objectives to restrict access. • FIA_UAU.2 which ensures that users are authenticated to the TOE. • FIA_UID.2 which ensures that users are identified to the TOE. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations.
O.MEDIAT	This objective is completely satisfied by • FDP_IFC.1 which ensures the TOE supports an user information flow policy that controls which port can send and receive network traffic. • FDP_IFF.1 which ensures the information flow control SFP based on the subject and information attributes and permits an information flow between controlled subject and information via a controlled operation. • FDP_RIP.1 which ensures the TOE tracks all source and designation ports and ensures that no residual data is exposed to users. • FMT_MSA.1 which restricts the ability to modify, delete and view the parameters for the information flow control to user roles as defined in the FMT_MTD.1 • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information flow control • FMT_MSA.3 which ensures that restricts the ability to modify, delete and view the parameters for the Information flow control SFP as per the defined user's privilege / role and ensure that residual information from a previous information flow is protected and not transmitted in any way • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations

OBJECTIVE	RATIONALE
O.SECFUN	This objective is completely satisfied by • FAU_STG.1 which ensures only the authorized administrator has access to the logs. • FAU_STG.3 which ensures the TOE overwrites the oldest stored audit data with any further audit data generated when the audit trail becomes full. • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to an Administrator. • FMT_MSA.1 which restricts the ability to modify, delete and view the parameters for the information flow control to user roles as defined in the FMT_MTD.1 • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information flow control • FMT_MSA.3 which ensures that there is a default denies policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations. • FMT_SMF.1 lists the security management functions that must be controlled. • FMT_SMR.1 defines the roles on which access decisions are based.
O.SECKEY	This objective is completely satisfied by • FCS_CKM.1 which ensures that cryptographic keys and parameters are generated with standards-based algorithms. • FCS_CKM.2 which provides secure key distribution to remote trusted IT products. • FCS_CKM.4 which ensures that the cryptographic keys and parameters are safely destroyed.
O.SECSTA	This objective is completely satisfied by • FMT_MOF.1 which ensures the ability to perform security management functions is restricted to an authorized Administrator. • FMT_MSA.1 which restricts the ability to modify, delete and view the parameters for the information flow control to user roles as defined in the FMT_MTD.1 • FMT_MSA.2 which ensures that only secure values are accepted for the configuration parameters associated with the Information flow control

OBJECTIVE	RATIONALE
	• FMT_MSA.3 which ensures that there is a default deny policy for the information flow control security rules. • FMT_MTD.1 which restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations.
O.SELPRO	This objective is completely satisfied by • FAU_STG.1 which ensures only the authorized administrator has access to the logs. • FAU_STG.3 which ensures the TOE overwrites the oldest stored audit data with any further audit data generated when the audit trail becomes full. • FTA_SSL.3 which protects existing encrypted sessions from becoming compromised by enforcing a session timeout when certain conditions are met.
O.SINUSE	This objective is completely satisfied by • FIA_ATD.1 which exists to provide users with attributes to distinguish one user from another, for accountability purposes, and to associate roles with users.

Table 19 - Rationale for TOE Objectives to SFRs

6.12.3 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2). The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing functional specification.
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirement
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 20 - Security Assurance Requirements at EAL2

6.12.5 Security Assurance Requirements Rationale

The EAL-2 was chosen because it is based upon good commercial development practices with thorough functional testing. EAL2 provides the developers and users a moderate level of independently assured security in conventional commercial TOEs. The threat of malicious attacks is not greater than low, the security environment provides physical protection, and the TOE itself offers a very limited interface, offering essentially no opportunity for an attacker to subvert the security policies without physical access.

6.12.6 Security Assurance Requirements Evidence

This section identifies the measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	EVIDENCE TITLE
ADV_ARC.1 Security Architecture Description	Security Architecture: Tejas Networks POTP / PTN Access
ADV_FSP.2 Functional Specification with Complete Summary	Security-enforcing functional Specification: Tejas Networks POTP / PTN Access
ADV_TDS.1 Basic Design	Basic Design: Tejas Networks POTP / PTN Access
AGD_OPE.1 Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: Tejas Networks POTP / PTN Access
AGD_PRE.1 Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: Tejas Networks POTP / PTN Access
ALC_CMC.2 Use of a CM system	CM system: Tejas Networks POTP / PTN Access
ALC_CMS.2 Parts of the TOE CM coverage	CM system: Tejas Networks POTP / PTN Access
ALC_DEL.1 Delivery Procedures	Secure Delivery Processes and Procedures: POTP / PTN Access
ASE_CCL.1 Conformance claims	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ASE_ECD.1 Extended components Definition	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ASE_INT.1 ST introduction	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ASE_OBJ.2 Security objectives	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ASE_REQ.2 Derived security Requirements	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ASE_SPD.1 Security problem definition	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ASE_TSS.1 TOE summary specification	Security Target: TejNOS software running on Tejas Networks POTP / PTN Access Systems
ATE_COV.1 Evidence of coverage	Testing Evidence: Tejas Networks POTP / PTN Access
ATE_FUN.1 Functional Testing	Test report: Tejas Networks POTP / PTN Access
ATE_IND.2 Independent testing	
AVA_VAN.2 Vulnerability analysis	Nessus scan report: Tejas Networks POTP / PTN Access

Table 21 - Security Assurance Rationale and Measures

7. TOE Summary Specification

This section presents the Security Functions implemented by the TOE.

7.1 TOE Security Functions

The security functions performed by the TOE are as follows:

- Security Audit
- Cryptographic Operations
- User Data Protection and Protection of TSF
- Identification and Authentication
- Security Management
- Time stamp and TOE Access
- Trusted Path

7.2 Security Audit

TOE generates a fine-grained set of audit log. These logs are stored in local computer system. The logs are divided into the following categories and are maintained separately:

- Audit logs – used to track system related events such as addition and deletion of cross connect and user creation etc.
- HTTP session logs – records active HTTP sessions at any point in time.
- Session History logs – record user access events .such as retrieving a file.
- Invalid Sessions History – used to records invalid login events.

Each log contains the following fields:

- ID
- Timestamp
- Date
- Entity who initiated the activity : [initiating IP] initiator username if applicable, (user type if applicable),[user role if applicable]
- Description of the activity

The TOE generates logs for the following list of events:

- Modifications to the users that are part of a role, which includes the identity of the Administrator performing the modification and the user identity being associated with a role in each related log;

- All use of the user identification mechanism, which includes the user identities provided to the TOE in each related log;
- Any use of the authentication mechanism, which includes the user identities provided to the TOE in each related log;
- Changes to the time, which includes the identity of the Administrator performing the operation in each related log;
- Information flow security policy rules, user attribute values, and audit trail data.
- Each related log includes the identity of the user performing the operation.

The logs are only accessible through the Web-Based interface, only Admin is authorized to access. Admins can view and, save the logs in xml file in local computer..

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

- FAU_GEN.1: TOE generates all the audit events identified in this requirement. Within each event is the information listed above which addresses all required details.
- FAU_SAR.1: The Administrator -only have the ability to read all of the audit logs. Each log is presented to the administrator in a human-readable format.
- FAU_STG.1: Only the Administrator has access to the logs. The Administrator is not permitted to modify any information in the logs. The only allowed on logs are to, achieve them, save them, or view them.
- FAU_STG.3: Audit log file is stored in terms of entries. It can be store Max 1000 (approx) entries. Once audit log entry reaches 1000, old entries will be deleted automatically to make space for new record . Latest minimum 200 records will be available..

7.3 Cryptographic Operations

TOE provides an encrypted path between users and the TOE. Users connect to the TOE using a secure connection using AES encryption algorithms as per protocol HTTPS.

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

- FCS_CKM.1: This component ensures that cryptographic keys and parameters are generated with standards-based algorithms
- FCS_CKM.2: This component provides secure key distribution to remote trusted IT products
- FCS_CKM.4: This component ensures that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the Administrator forces generation of new keys
- FCS_COP.1: Robust algorithms as listed in Table-22 are used to support encrypted

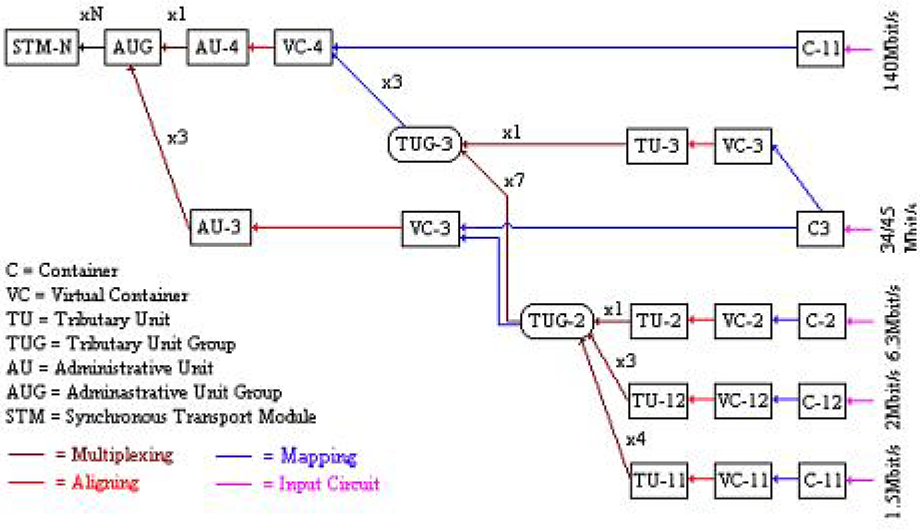
communications between users and POTP / PTN Access.

OPERATIONS	ALGORITHM (MODE)	KEY SIZE IN BITS	STANDARDS
Encryption And Decryption	AES (CBC mode)	128, 256	FIPS 197
	CAMELLIA	128, 256	--
	IDEA	128	--
	SEED	128	--
Hashing	SHS (SHA-1)	160 (size of digest)	FIPS 180-2
	MD5	128	RFC 1321
Random Number Generation	ANSI X9.31	Not Applicable	ANSI X9.31

Table 22 - Cryptographic Operations

7.4 User Data Protection and Protection of the TSF

Digital cross connects made between the source and destination port depends on the resource present in the node. POTP/PTN Access has provision to equip different tributary and aggregate cards depend on the control card used. Tributary and Aggregate cards are the resource for making digital cross connect. Below is a diagrammatic representation of the various levels of multiplexing that a "container" must go through to be mapped within an STM-N frame. This diagram is a standard diagram often used to represent SDH container levels.



SDH Multiplexing Structure for STM Frames

TOE ensures that all packets that are delivered to a user do not contain residual information.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_IFC.1: The TOE supports a user information flow policy that controls which port can send and receive network traffic as the standard SDH architecture.
- FDP_IFF.1: Traffic filtering SFP based on the subject and information attributes and permits an information flow between a controlled subject and controlled information via a controlled operation.
- FDP_RIP.1: The digital cross between source and destination in TOE make as per the standard SDH frame format. There won't be any residual information data exposed to non-designated destination

7.5 Identification and Authentication

TOE performs identification and authentication of all users and administrators accessing the TOE. In the evaluated configuration, TOE performs the authentication locally. Users enter a username and password, which is validated by TOE against the user information stored by the TOE. If the authentication succeeds, the user receives a session token that is used for identification of subsequent requests during that session.

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

- FIA_ATD.1: For each registered user, the TOE stores the following information: user identity, user roles, and password.
- FIA_SOS.1: The TOE is equipped with a mechanism that can be configured by the administrator to verify that user authentication secrets meet a list of criteria for ensuring their strength. The following parameters for authentication secrets are required for the evaluated configuration:
    1. Exactly eight (8) character only,
    2. It can be of eight (8) numeric characters,
    3. It can be of eight (8)) alphabetic characters,
    4. Combination of both uppercase and lowercase alphabetic characters,
    5. Combination of alphanumeric and special characters

Following are the access privilege assigned to the user account.

- USER: Read-only access to all the management information including configuration, faults and performance.
- OPERATOR: Can perform certain configuration operations such as port and acknowledgment of faults, resetting performance statistics, etc.
- OPERATOR2: Can configure node name, configure Router ID and Ethernet IP, perform maintenance operations such as software or configuration backup and restore, limited security access for modification of own password and all other operations similar to operator.
- ADMIN: Can create and delete login users on the network element. Can configure Location, Contact, security parameters and as well as management parameters such as Ethernet/Router IP Address/Masks.

- FIA_UAU.2: The TOE requires a valid password associated with a user name before providing access to the TOE. Passwords must conform to the requirements in FIA_SOS.1
- FIA_UID.2: The TOE requires a user name during the identification and authentication process. The username is entered, then a password. If the password is valid, the user will be associated with a role and set of privileges based on the username.

7.6 Security Management

TOE provides security management functions via a browser interface. The Administrator logs onto the TOE from a protected network and performs all management functions through the browser interface. The Administrator has the ability to control all aspects of the POTP / PTN Access configuration including: user management, information flow policy management, audit management, and system start-up and shutdown.

Administrators set the information flow policy rules on a per user basis. When the Administrator adds a new user, the Administrator defines the user access. Although users are grouped into roles,

Administrators can create rules that except specific users from the constraints of their role. By default, user access is restrictive but the Administrator may override the default upon rule creation.

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

- FMT_MOF.1: The ability to perform the following security management functions is restricted to an Administrator role:

a) create, delete and view information flow security policy rules that permit or deny information flows;

b) create, delete and modify user attribute values, which include a user's identity, association to a role, and authentication credentials;

c) enable and disable external IT entities from communicating to the TOE;

d) modify and set the time and date performed by an defined user roles;

e) Admin can only able to archive, and review the audit trail according to authentication credentials.

f) Configuration of inactive session timeout by setting defined session period.

- FMT_MSA.1: User privilege /roles ensure the ability to create, delete and view the parameters for the information flow policy rule (cross-connect / service provisioning).
- FMT_MSA.2: This component ensures that only secure values are accepted for the configuration parameters associated with the information flow control SFP.
- FMT_MSA.3: The TOE allows restrictive access by default but the Administrator role can assign permissions.
- FMT_MTD.1: The TOE restricts the ability to modify the Authenticated User SFP, restricts the ability to modify identification and authentication data, restricts the ability to delete audit logs, restricts the ability to modify the date and time, restricts the ability to modify the data relating to TOE access locations. All restrictions apply to the Administrator role.
- FMT_SMF.1: Security management functions as per the defined user's privilege and roles:

  a. create, delete, and view information flow security policy rules that permit or deny information flows;

  b. create, delete, modify, and view user attribute values, which include a user's identity, association to a role, and authentication credentials;

  c. enable and disable external IT entities from communicating to the TOE;

  d. modify and set the time and date;

  e. archive and review the audit trail.

  f. Configuration of inactive session timeout.

- FMT_SMR.1: The TOE supports the user, operator, operator2 and admin. The admin role provides a user within the administrator's authentication realm access to perform all management functionalities.
  - USER: Read-only access to all the management information including configuration, faults and performance.
  - OPERATOR: Can perform certain configuration operations such as port and acknowledgment of faults, resetting performance statistics, etc.

- OPERATOR2: Can configure node name, configure Router ID and Ethernet IP, perform maintenance operations such as software or configuration backup and restore, limited security access for modification of own password and all other operations similar to operator.

- ADMIN: Can create and delete login users on the network element. Can configure Location, Contact, security parameters and as well as management parameters such as Ethernet/Router IP Address/Masks.

7.7 Time Stamp and TOE Access

TOE provides a timestamp for its own use. The timestamp is generated from the clock provided in the hardware.

TOE protects all current sessions from compromise by enforcing a timeout. When a session becomes idle for more than 60 minutes or reaches a session timeout (0 – 300) defined by the Admin user and the session times out and is deleted from the session table. Session timeouts are enforceable on sessions initiated on both the administrator and user interfaces of the TOE.

Communications between TOE components (client and appliance) are protected with cryptography provided by FCS_COP.1.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_STM.1: The TOE generates a reliable timestamp for its own use. System time is set based on the real time clock chip that is part of the processor complex. RTC module will be used along with a super-cap to provide backup power. The minimum back-up time is in excess of 10 days. This RTC module can be accessed using the I2C interface implemented in Control FPGA.
- FTA_SSL.3: The TOE protects existing encrypted sessions from becoming compromised by enforcing a session timeout after a session has been idle for more than 60 minutes or as defined session timeout (0 – 300minutes) by the admin.

7.8 Trusted Path

Connection to and from the TOE are protected using the protocols mentioned within the Cryptographic Support section. Trusted paths are used to secure all user sessions through HTTPS. Users initiate the trusted path to the TOE through establishing an HTTPS connection. The trusted path is used for authentication and all user management functions. All connections for the TOE are protected using the HTTPS cryptographic mechanism.

- FTP_TRP.1: All communications between users and TOE is encrypted via a secure connection using encryption & decryption algorithms defined in FCS_COP.1.