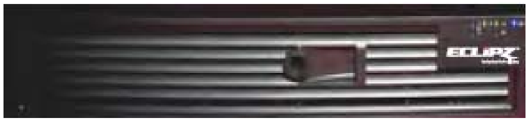
OPTICA™
Technologies Incorporated

Enterprise Connectivity and Security Solutions

Optica Technologies
Eclipz ESCON Tape Encryptor
Part Number 44200-04
Firmware Version 1.3.10.0
Security Policy

FIPS 140-2 Level 2 Validation



July 26, 2008
Version 1.15

1 Introduction

This document is the Security Policy for Optica Technologies Eclipz ESCON Tape Encryptor (P/N 44200-04) cryptographic module. This Security Policy specifies the security rules under which this cryptographic module shall operate to meet the requirements of FIPS 140-2 Level 2. It describes how the module functions to meet the FIPS requirements, and the actions that operators must take to maintain the security of the module.

This Security Policy describes the features and design of the Optica Technologies Eclipz ESCON Tape Encryptor cryptographic module using the terminology contained in the FIPS 140-2 specification. *FIPS 140-2, Security Requirements for Cryptographic Modules* specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST Cryptographic Module Validation Program (CMVP) validates cryptographic modules to the FIPS 140-2 standard. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

The FIPS 140-2 standard, and information on the CMV program, can be found at csrc.nist.gov/groups/STM/index.html. More information describing the Eclipz ESCON Tape Encryptor can be found at www.Optica Technologies.com.

In this document, the Optica Technologies Eclipz ESCON Tape Encryptor device is also referred to as “the module” or “the encryptor”.

This Security Policy contains only non-proprietary information. All other documentation submitted for FIPS 140-2 conformance testing and validation is “Optica Technologies - Proprietary” and is releasable only under appropriate non-disclosure agreements.

The Optica Technologies Eclipz ESCON Tape Encryptor cryptographic module meets the overall requirements applicable to Level 2 security for FIPS 140-2 as shown in Table 1.

Table 1. Cryptographic Module Security Requirements.

Security Requirements Section	*Level*
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DRNG	Deterministic Random Number Generator
DH	Diffie-Hellman Algorithm
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
EMI	Electromagnetic Interference
ESCON	Enterprise Systems Connection
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LAN	Local Area Network
LED	Light Emitting Diode
NDRNG	Non-Deterministic Random Number Generator
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir Adleman public key cryptosystem
SHA-1	Secure Hash Algorithm
SHA-384	Secure Hash Algorithm
T-DES	Triple-DES (Data Encryption Standard)

2 Optica Technologies Eclipz ESCON Tape Encryptor

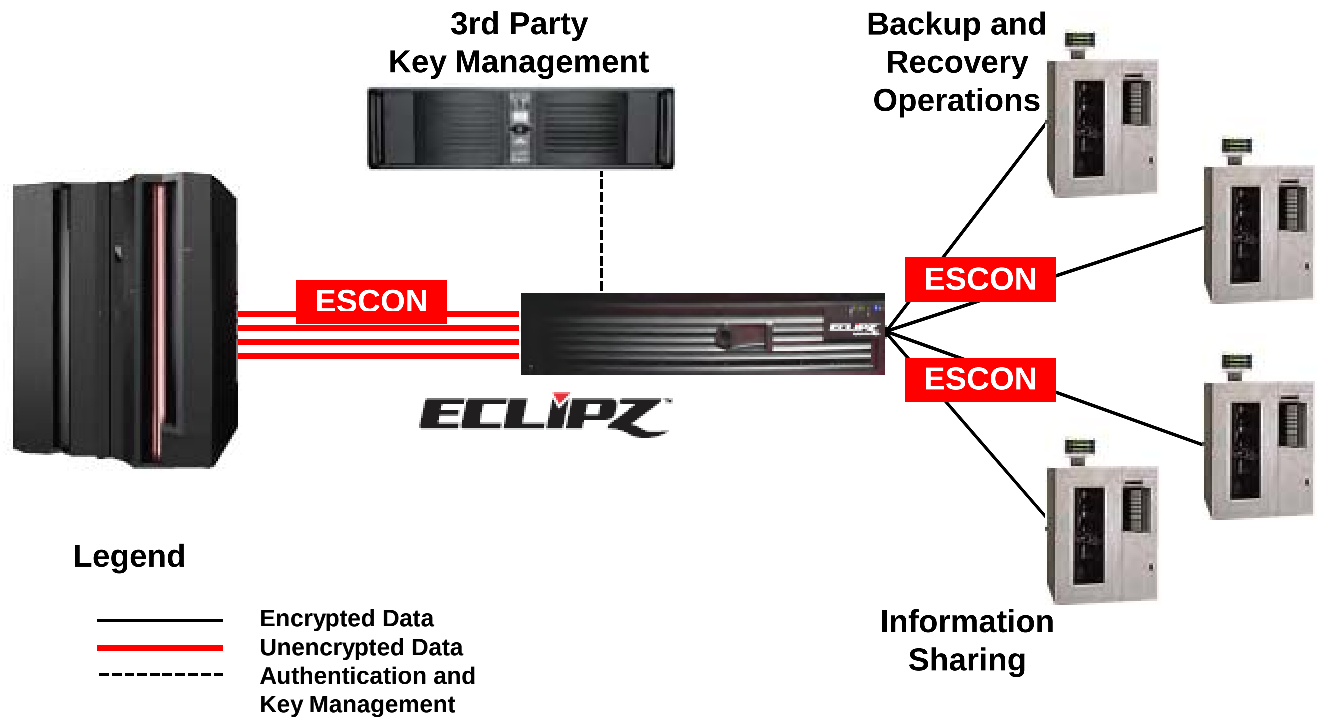
2.1 Functional Overview

The Optica Technologies Eclipz ESCON Tape Encryptor is an inline encryption appliance that directly integrates hardware accelerated encryption into native ESCON channels. It provides fully transparent, high performance data encryption for legacy ESCON tape systems. Eclipz preserves legacy ESCON tape device investments and interoperates with leading appliance-based key management solutions. . It supports 4 ESCON channels within a single appliance. The encryptor provides encryption for tape backup and recovery operations, and tape-based information sharing with business partners.

Eclipz's crypto-accelerator hardware supports the Advanced Encryption Standard (AES) with a key size of 128 or 256 bits. The crypto-accelerator also has an on-board compression capability and can deliver a nominal throughput of 10MB to 14MB/second per channel. The impact on system throughput and latency is minimal. The Eclipz Encryptor is based on an industry standard 2U server platform and provides encryption for a variety of ESCON tape drives including Sun 9490 / 9840 and IBM 3490 / 3950 system models.

Figure 1 shows the cryptographic module installed directly into native ESCON channels. Key management is provided built in or alternatively by a 3rd party key management system, possibly on the mainframe itself.

Figure 1. Functional View of the Cryptographic Module.



2.2 Module Description

The Optica Technologies Eclipz ESCON Tape Encryptor is a multi-chip standalone cryptographic module consisting of production-grade components contained within an opaque hard production-grade enclosure (the outside case is steel). The removable cover is protected by tamper evident security tape in accordance with FIPS 140-2 Level 2. The cryptographic boundary is the metal enclosure of the encryptor with the exception of removable, hot-swappable dual power supplies that are excluded from the cryptographic boundary.

The module has a limited operational environment. While only a single operator in the user role (the host tape system) may use the module at any one time, multiple operators (defined accounts for human operators) in the crypto officer role may access the administration interface concurrently. The module has a bypass mode wherein data may pass through the module without being encrypted. The tape volume serial number controls the policy decision to encrypt or bypass encryption.

The module has a maintenance mode that is accessible only by Optica Technology maintenance engineers and then only when that capability is enabled by the crypto officer administering the module. A maintenance password is needed to access the maintenance interface. The password is known only to Optica Technology maintenance engineers. Maintenance mode cannot be entered unless cryptographic keys and CSPs are zeroized.

The Eclipz ESCON Tape Encryptor meets applicable Federal Communication Commission (FCC) Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements as defined in Subpart B of FCC Part 15, for Class B devices.

2.3 Module Ports and Interfaces

The cryptographic module has numerous physical ports and four logical FIPS 140-2 interfaces. The physical ports and logical interfaces are described in Table 2.

Where distinct logical interfaces share the same physical port, communication protocols (such as TCP/IP, 802.3, and ESCON) logically separate and isolate these interfaces from one another. The system processor manages data as it passes through the module. The module relies on programmatic functionality and the system processor to ensure that logically distinct categories of data do not occupy the data path at the same time. The system processor, system timing, and programmatic controls logically disconnect the input and output data paths from the circuitry and processes that perform key generation and key zeroization.

Table 2. Physical Ports and Logical FIPS 140-2 Interfaces.

Physical Port	*FIPS 140-2 Logical Interface*
NIC 1	Control input and status output.
NIC 2	Control input and status output.
ESCON connectors (4 to Mainframe computer)	Data input, data output, and status output.
ESCON connectors (4 to tape devices)	Data input, data output, and status output.
Front Panel LEDs (6)	Status Output. Indicates Ethernet port activity, power, hard drive activity, fault condition, and system identification.
Front Panel Video Adapter	Status Output
PS2 keyboard interface	Control Input [This feature is only available to Optica engineers, and is protected by PIN]
Diagnostic LEDs	Status Output
Rear Panel Video Adapter	Status Output
Power Input (dual, hot-swappable)	This is not a FIPS 140-2 logical interface. Power enters the module via the power input connectors.

The FIPS 140-2 logical interfaces correspond to physical ports as described in Table 3.

Table 3. FIPS 140-2 Logical Interfaces.

Logical Interface	***Description***
Data input	Data input consists of plaintext data entering the cryptographic module from the mainframe via the ESCON interface for the purpose of being stored on a tape. Data input also consists of ciphertext or plaintext data entering the cryptographic module from a tape device via the ESCON interface for the purpose of being restored to the mainframe system.
Data output	Data output consists of ciphertext or plaintext data exiting the cryptographic module via the ESCON interface to a tape device for storage. Data output consists of plaintext data exiting the cryptographic module via the ESCON interface for the purpose of being restored to the mainframe system.
Control input	Control input from crypto officers enters the module using the Ethernet (NIC 2 or NIC 1) interface, and the PS2 keyboard interface (direct attached console 2 only for maintenance access if enabled by a crypto officer). Control input (cryptographic keys) from external 3rd party key management servers enter the module via the Ethernet (NIC 2) interface.
Status output	The status output consists of module status returned from status requests by crypto officers and other module outputs indicating module conditions. Status output data includes LEDs indicating power, fault conditions or interface activity, the web interface provided over NIC 2 or NIC 1 showing configuration information, SNMP data sent to an SNMP trap receiver via NIC 2, console output to a video monitor, and link control information passed on the ESCON interface for interoperation with external devices.

3 Security Functions

The Eclipz ESCON Tape Encryptor cryptographic module implements the security functions described in Table 4.

Table 4. Module Security Functions.

Security Function	*Purpose or Use*	*Certificate*
Approved Security Functions		
AES (FIPS PUB 197) CBC(e/d; 128) CBC(e/d; 256)	TLS 1.0 and user data encryption and decryption,	771, 266
TDES (FIPS 46-3) TECB(e/d; KO 2,3) TCBC (e/d; KO 2,3)	TLS 1.0	670
SHA-1 (BYTE-only) **SHA-224** (BYTE-only) **SHA-256** (BYTE-only) SHA-384 **(BYTE-only)** **SHA-512** (BYTE-only) **(FIPS PUB 180-2)**	Signature generation, verification, data integrity	776, 345
HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512	Data integrity	422, 78 (HMAC), 776, 345 (SHS)
RNG (ANSI X9.31 PRNG, Appendix A.2.4)	Key generation	442
RSA (FIPS PUB 186-2) ALG[RSASSA-PKCS1_V1_5]; SIG(gen); SIG(ver); 2048, 4096, SHS: SHA-1	TLS 1.0 key exchange	366
DSA (FIPS PUB 186-2) KEYGEN(Y) MOD(1024); SIG(gen) MOD(1024); SIG(ver) MOD(1024);	TLS 1.0 key exchange	289
Elliptic Curve DSA (FIPS PUB 186-2) PKG: CURVES(P-256 P-384 P-521) PKV: CURVES(P-256 P-384 P-521) SIG(gen): CURVES(P-256 P-384 P-521) SIG(ver): CURVES(P-256 P-384 P-521)	TLS 1.0 key exchange, firmware validation	84 SHS: 776 RNG: Cert# 442
Allowed Security Functions		
Elliptic Curve Diffie Hellman [Key agreement; key establishment methodology provides 192 bits of encryption strength.]	Key agreement	Vendor Affirmed
Diffie Hellman [Key agreement; key establishment methodology provides 112 bits of encryption strength.]	Key agreement	Vendor Affirmed

4 FIPS Approved Mode of Operation

The module's approved mode of operation is restricted to performing only FIPS-approved and FIPS-allowed cryptographic algorithms and security functions. The module enters FIPS approved mode on power up as soon as it successfully completes the power-on self test. In the FIPS approved mode, crypto officers may configure the module for operation and they may make administrative changes. Users may access the module's data encryption and decryption services.

The Eclipz ESCON Tape Encryptor supports manual updates to the microcode (device firmware); however, any updates of the module firmware must use only FIPS certified firmware. Updates that use non-FIPS certified firmware invalidate the module's FIPS evaluated configuration.

The module has a non-approved mode that is active only if the crypto officer configures all encryption rules to No Encryption. To put the module into the Approved mode of operation (FIPS Mode) the user must refer to the User Guide.

4.1 Setup and Initialization Procedures

The Optica Quick Start Instructions provide the following steps to set up and initialize the module into FIPS mode:

1. Check the packaging and the module for signs of tampering. If tampering is detected, contact the manufacturer for instructions.
2. Power up the module.

   The SHA-1 hashes on the pre-extracted firmware image files are compared against the release notes provided by Optica, and must match the values in the release notes. (Release Notes are shipped to the end user with the module and this information is also available on the Optica web site). The pre-extracted firmware image hashes display on a monitor connected the module's video port after the self-tests have executed.
3. After setting the temporary IP address and connecting the network cable, log into the web interface using the default username "DefaultSecurityOfficer" and password "ChangeThisPassword".
4. Add a security officer account. Note the Security Officer can create other Security Officer or Operator (User) accounts as required
5. Log into the module with that security officer account.
6. Delete the DefaultSecurityOfficer account.
7. Set the time zone and enable ping.
8. Enter the appropriate IP address, subnet mask, gateway, and DNS info, and click **set**.
9. Set up the workstation to be used for administration and ping the Eclipz device from the workstation.
10. Enter the required information to create an organizational key.
11. When the organizational key creation is complete, verify that "FIPS Mode" appears at the top left of the screen.

4.2 Non-FIPS Mode

The module only uses FIPS approved or FIPS allowed algorithms.

The module will indicate that it is in non-FIPS mode if as a result of its configuration a condition is detected where there is not at least one rule that results in tape encryption. Modifying the configuration so that there is at least one rule that results in encryption will cause the module to once again indicate that it is in FIPS mode.

5 Identification and Authentication

The module supports a security officer (crypto officer) role, an operator (user) role, a web support role and a maintenance role.

Multiple concurrent role-based sessions (security officers, operators, web support, and maintenance roles) are allowed but roles cannot be changed while authenticated to the module. An account's role is assigned by a security officer at the time the account is created. An account's role can subsequently only be changed by a security officer.

Separation of roles is achieved by first requiring authentication before granting access to services offered to a particular role. The firmware then programmatically separates roles and services during module use by providing role-specific services to the specific authenticated role. The firmware programmatically separates concurrent sessions within a role through the use of atomic operations for all operations that change configuration data. The event messaging system associates all configuration changes with the identity of the session making the change.

The module does not display any authentication data entered into the module other than black dot feedback characters indicating a key was pressed.

When an account is initially created, the security officer assigns an arbitrary password to the new account. When a successful authentication occurs for the new account, the user interface automatically requests that the password be changed.

Access to the authorized roles is restricted as explained in Table 5:

Table 5. Roles and Required Identification and Authentication.

Role	*Type of Authentication*	*Authentication Data*
Security Officer (Crypto Officer)	Identity-based	A security officer authenticates by entering a user name and a password.
Operator (User)	Identity-based	An operator authenticates by entering a user name and a password.
Web Support	Identity-based	A web support user authenticates by entering a user name and a password.
Maintenance	Identity-based	A maintenance role user authenticates by entering a user name and a password.

The strength of the operator authentication, per the above roles, is as follows in Table 6:

Table 6. Strength of Authentication.

Authentication Mechanism	*Strength of Mechanism*
Password	Security Officers, Operators, Web Support and Maintenance account users authenticate using a minimum 8-character password that must include at least three of the following: one upper case character, one lower case character, one digit (0-9), and one special character (printable characters excluding space and alphanumerics). The characters used in the password must be from the ASCII character set providing at least 72 possible characters (a conservative count). This yields a minimum of 7.22204E+14 or over 722 trillion possible combinations; thus, the possibility of correctly guessing a password is less than 1 in 1,000,000. The possibility of randomly guessing a password in 60 seconds is less than 1 in 100,000. It takes about .5 to 1 seconds to enter a user name and a

Authentication Mechanism	*Strength of Mechanism*
	password, limiting a total number of attempts to guess the password within 60 seconds to about 120. Moreover, accounts (except for the last active Security Officer account) are locked out after 5 unsuccessful login attempts.

When the cryptographic module is powered off and subsequently powered on, the results of previous authentications (the authentication states of sessions) are cleared from memory. When the module is powered up again, operators must re-authenticate, entering the correct role account name and password.

6 Cryptographic Keys and CSPs

The following table identifies the Cryptographic Keys and Critical Security Parameters (CSPs) used within the module. Cryptographic keys and CSPs are never output from the module in plaintext. An Approved key generation method is used to generate keys.

Table 7. Cryptographic Keys and CSPs.

Data Item	*Description*
HTTPS Key	RSA 2048-bit public key pair used for the symmetric key wrapping in the Web administration interface (TLS). The key is generated using a FIPS approved RNG (cert # 442) and is stored in unencrypted form in the file system on an encrypted disk partition. The public key is maintained in an X.509 certificate. This key is implicitly zeroized on a factory default. The factory default procedure zeroizes the current disk partition key, allocates a new disk encryption key and uses it to reformat the encrypted disk partition before re-installing the factory default files.
TLS AES Encryption Key	AES 256-bit ephemeral symmetric key used for encrypting the TLS sessions for the Web administration interface. It is generated using a FIPS approved RNG (cert # 442). This key is destroyed on TLS session completion.
TLS Triple-DES Encryption Key	T-DES 112-bit ephemeral symmetric key used for encrypting the TLS sessions for the Web administration interface. It is generated using a FIPS approved RNG (cert # 442). This key is destroyed on TLS session completion.
Organizational key pair (ORG)	A DSA 2048-bit or an ECC 384 bit prime modulus public key pair shared by all Eclipz cryptographic modules in an organization for key exchange and bypass validation (signature generation and verification) purposes. The ORG key pair may be generated on the module using the FIPS approved RNG (certificate 442) or the key pair may be imported in encrypted form from another Eclipz device. The ORG key is stored on an encrypted disk partition. It is zeroized on a zeroize or restore to factory default command.
Key Encrypting Key (KEK)	A 256-bit AES key used to wrap or unwrap a Media Encryption Key (MEK). This key is produced using Diffie-Hellman or Elliptic Curve Diffie-Hellman key agreement techniques as described in NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes. Wrapping is performed according to the AES Key Wrap Specification. The KEK key is deleted from the system after use.
Media Encryption Key (MEK)	A 128-bit or 256-bit AES key used to encrypt the data on the media (tape). This key is generated dynamically using a FIPS approved RNG (certificate 442) and is stored in wrapped (encrypted) form in the tape header on the media or on a 3rd party key management system or both. Wrapping is performed using the KEK as the wrapping key according to the AES Key Wrap Specification. The MEK key is deleted from the system after use.
Ephemeral Key Pair	Either DSA 2048-bit or ECC 384 bit prime modulus ephemeral key material generated for use in key agreement to generate a Key Encrypting Key (KEK). The ephemeral private key component is destroyed after use. The ephemeral public key component is stored in the header on the media.
Optica ECC Public Key	A 384-bit prime modulus ECC public key used for the firmware integrity tests (to verify digital signatures on installed firmware). The key is entered into the module with the firmware and is stored in the file system on an encrypted disk partition. The key is contained in a digital certificate.

Data Item	Description
Optica RSA Public Key	A 2048-bit RSA public key used by a Security Officer or Operator to encrypt a randomly generated password when the DefaultSupport web support account is reset. This encrypted password can be conveyed to an Optica support technician when support services are required.
Unit Key Pair	RSA public key pair used for key exchange with 3rd party key management systems if these external systems are used. The unit key may be 2048 or 4096-bits depending on the needs of the external key management system. The key is generated using a FIPS approved RNG (cert # 442) and is stored in the file system on an encrypted disk partition. It is zeroized on a zeroize command or restore to factory default command. Currently nCipher KeyVault (formerly NeoScale) and NetApp Lifetime Key Manager 3rd party key management systems are supported.
RNG Seed	The module contains an RNG in both firmware and hardware. Seeding material for the firmware based RNG is gathered by the underlying OS. Eclipz performs continuous tests on the random numbers generated. The module provides a continuous RNG test for both the RNG in firmware and the hardware RNG. The hardware RNG is used to assist in seeding and reseeding the firmware based RNG.
Security Officer Password	A minimum 8-character password used by crypto officers to authenticate to the Web Administration interface. Each crypto officer has his or her own password. Crypto officer passwords are stored as SHA-512 hash values in the file system on an encrypted disk partition.
Operator Password	A minimum 8-character password used by operators to authenticate to the Web Administration interface. Each operator has his or her own password. Operator passwords are stored as SHA-512 hash values in the file system on an encrypted disk partition.
Web Support Password	A minimum 8-character password used by an Optica Technologies support engineer to access the web maintenance interface (if the support account is enabled). The support password is stored as a SHA-512 hash value in the file system on an encrypted disk partition.
Maintenance Password	A minimum 8-character password used by an Optica Technologies support engineer to access the maintenance interface (if the account is enabled). The maintenance password is stored as an MD5 hash value in the file system on an encrypted disk partition.
Maintenance Root Password	A minimum 8-character password used by an Optica Technologies support engineer to access the Eclipz operating system software files directly from within the maintenance interface (if the support account is enabled by a crypto officer and the current value of the root password is provided to the support engineer by a crypto officer). The root password is stored as an MD5 hash value in the file system on an encrypted disk partition.

7 Roles and Services

The module supports services that are available to users in the various roles. All of the services are described in detail in the module's user documentation. Table 8 shows the services available to the various roles.

Table 8. Roles and Services

Service	*Web Support*	*Operator (User)*	*Security Officer (Crypto Officer)*	*Maintenance*
login	●	●	●	
key_management	●	●	●	
org_cert	●	●	●	
create_org_cert			●	
export_org_csr		●	●	
import_org_cert			●	
export_org_cert	●	●	●	
export_org_key			●	
import_org_key			●	
km_cert	●	●	●	
create_km_cert			●	
export_km_csr		●	●	
import_km_cert			●	
edit_kmip		●	●	
export_km_keys			●	
import_km_keys			●	
zeroize_km_keys		●	●	
Partners	●	●	●	
edit_partner			●	
delete_partner			●	
add_partner_cert			●	
partner_details	●	●	●	

Service	***Web Support***	***Operator (User)***	***Security Officer (Crypto Officer)***	***Maintenance***
partnerkey_details	●	●	●	
delete_partnerkey			●	
encryption_controls	●	●	●	
volsers	●	●	●	
edit_volser		●	●	
delete_volser		●	●	
users	●	●	●	
add_user (note 1)	**r**		●	
edit_user (note 2)	**r**	**r**	●	
delete_user (note 3)			●	
network	●	●	●	
set (ip address)		●	●	
set (update_nic2) (note 4)	●			
enable_ping	●	●	●	
disable_ping	●	●	●	
snmp_config		●	●	
snmp_test	●	●	●	
support	●	●	●	
enable_ssh (note 5)	●	●	●	
disable_ssh (note 5)	●	●	●	
enable_maintenance (note 5)		●	●	
disable_maintenance (note 5)		●	●	
flash_locate_LED	●	●	●	
set_root_password			●	
update_notes (note 6)	●			
system_status	●	●	●	

Service	***Web Support***	***Operator (User)***	***Security Officer (Crypto Officer)***	***Maintenance***
hardware_status	●	●	●	
port_status/global	●	●	●	
port_status/0	●	●	●	
port_status/1	●	●	●	
port_status/2	●	●	●	
port_status/3	●	●	●	
system_controls	●	●	●	
https	●	●	●	
create_https_cert			●	
export_https_csr		●	●	
import_https_cert			●	
export_https_cert	●	●	●	
system_clock	●	●	●	
change_timezone		●	●	
set (system_clock)		●	●	
config_mgmt		●	●	
backup_config		●	●	
restore_config			●	
reboot		●	●	
shutdown		●	●	
software_update (note 7)	●	●	●	
software_upload	●	●	●	
delete_upgrade		●	●	
activate_upgrade			●	
factory_default	●	●	●	
audit_log	●	●	●	

Service	Web Support	Operator (User)	Security Officer (Crypto Officer)	Maintenance
(view audit log)	●	●	●	
download_audit_log	●	●	●	
(snap engineering log) (note 8)	●			
(bundle engineering log) (note 9)	●			
(download engineering log) (note 10)	●			
(delete_eng_log) (note 11)	●			
zeroize		●	●	●
change_password	●	●	●	
Logout	●	●	●	
Log in as maintenance				●
Perform maintenance functions				●
Control encryption/decryption of data		●		

Table Notes:

1. A Support user can create another Support user; a Security Officer cannot create a Support user.
2. A Support user can only edit other Support users; an Operator or Security Officer can only enable/disable Support users and reset the DefaultSupport password.
3. The DefaultSupport account cannot be deleted - it can be disabled or its password can be reset.
4. Only Support users can reconfigure NIC 2.
5. Requires zeroization of CSPs.
6. Scratch pad area where support personnel can make notes for future reference related to this system.
7. This screen permits viewing upgrade files that exist on the Eclipz.
8. Only Support users can snap an engineering log.
9. Only Support users can bundle an engineering log.
10. Only Support users can download engineering log files.
11. Only Support users can delete engineering log files.

8 Access Control

Table 9 shows services that use or affect cryptographic keys or CSPs. For each service, the key or CSP is indicated along with the type of access.

R - The item is read or referenced by the service.
W - The item is written or updated by the service.
E - The item is executed by the service. (The item is used as part of a cryptographic service.)
D - The item is deleted by the service.

Table 9. Access Control

Key or CSP	*Service*	*Access Control*
HTTPS Key Pair	Generate HTTPS keys	D,W
	Export HTTPS keys for signing	R
	Import signed HTTPS keys	R
	Access Web Interface	E
TLS AES Encryption Key	Access Web Interface	W, E
	Logout of web interface	D
	Shutdown or Reboot	D
TLS Triple-DES Encryption Key	Access Web Interface	W, E
	Logout of web interface	D
Organizational Key Pair (ORG)	Create organizational key pair	W
	Export organizational CSR for signing	R,E
	Import signed organizational certificate	R,E, W
	Encrypt / Decrypt User Data	E
	Add partner	R
	Shutdown or Reboot	D
	Bypass Test	E
	Set volume serial number	E
Optica ECC Public Key	Integrity Test	E
Optica RSA Public Key	Reset DefaultSuport account password	E
Key Encrypting Key (KEK)	Encrypt MEK	W [1], E,D
	Decrypt MEK	W [1],E,D
Media Encryption Key (MEK)	Encrypt User Data	W,E,D
	Decrypt User Data	R,E,D
	Shutdown or Reboot	D
	Zeroize	W, E, D

Key or CSP	***Service***	***Access Control***
Ephemeral Key Pair	Encrypt User Data	W,E,D [2]
	Decrypt User Data	R,E [3]
Unit Key Pair	Encrypt / Decrypt User Data	R,W,E,D
	Zeroize, Restore Factory Default	D
Security Officer Password	Add, edit, delete crypto officer, operator accounts	W, D
	Authenticate to Web Interface	R
	Restore Factory Default	D
Operator Password	Change own password	W
	Authenticate to Web Interface	R
	Restore Factory Default	D
Web Support Password	Add, edit, or delete Web Support accounts	W, D
	Authenticate to Support Interface	R
	Restore Factory Default	D
Maintenance Password	Edit Maintenance account	W
	Login to Maintenance Account	R
	Restore Factory Default	D
Maintenance Root Password	Set Maintenance Root Password	W
	Log In as Maintenance Root	R
	Restore Factory Default	D
RNG Seed Key	Any RNG function	W,R,E,D

[1] The KEK is computed, used in a wrap or unwrap operation and then destroyed.

[2] The ephemeral key pair is used in the computation of the KEK. Once the KEK(s) have been computed, the private key component is destroyed. The public key component is written to the tape header.

[3] The public key component of the ephemeral key pair is retrieved from a tape header and used in the computation of the KEK so the MEK can be unwrapped.

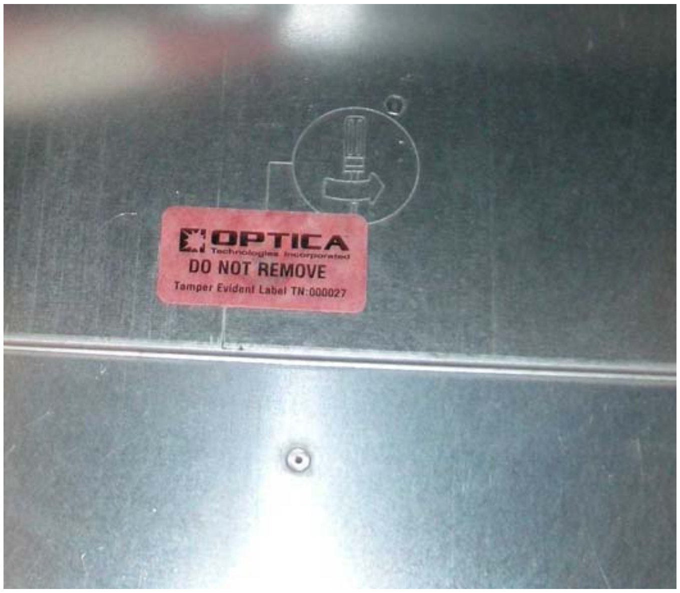
9 Physical Security

The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The cryptographic module consists of production-grade components that include standard passivation techniques (a sealing coat applied over the module's circuitry to protect against environmental or other physical damage). The module meets commercial-grade specifications for power, temperature, reliability, shock and vibration.

Tamper evident seals are placed over the module cover retention screws such that any attempt to remove the cover will leave evidence of tampering. The seal is serialized with serial numbers tracked by Optica Technologies. The crypto officer guidance directs the crypto officer to periodically inspect the module for signs of tampering such as dents or scratches on the module enclosure or damage to the tamper evident seal. If tampering is detected, the crypto officer is instructed to perform a zeroize command and then to contact Optica Technologies Technical support for further assistance.

Figure 7 shows how the tamper evident seal is placed over the module cover retention screw that secures the lid to the module chassis.

Figure 7. Tamper Evident Seal.



10 Self Tests

The module performs both power-on self test (POST) and conditional self tests to verify the integrity and correct operational functioning of the cryptographic module. If the system fails a self test, it reports status indicating which failure occurred and transitions to an error state, blocking all data output via the data output interface.

While the module is performing any power on self test, firmware rules permanently coded within the executable image prevent the module from entering a state where data output via the data output interface is possible. During any conditional tests, the module sets a self test flag. Processes that could output data monitor this flag, preventing data output via the data output interface if it is set.

Anyone with physical or logical access to the module can run the POST on demand by power cycling the module or entering a Reboot command.

Table 10 summarizes the system self tests.

Table 10. Self Tests.

Self Test	***Description***
Mandatory power-up tests performed at power-up and on demand:	
Cryptographic Algorithm Known Answer Tests	Each cryptographic algorithm (AES, TDES, RSA, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, HMAC-SHA1, HMAC-SHA224, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, and RNG) performed by the module, is tested using a “known answer” test to verify the operation of the function.
Pairwise Consistency Tests	The module performs pairwise consistency tests for DSA and ECC asymmetric keys. The is also a KEK test to verify operation of the DH and ECDH algorithms.
Firmware Integrity Test	The module verifies the individual ECDSA signatures on the SHA-1 hashes for each firmware file, as well as verifying a hash which is done collectively on all firmware files.
Bypass Tests	The module tests that configuration records related to bypass have not been altered during the power off state.
Critical function tests performed at power-up:	
None	No security-relevant critical functions tests are performed.
Conditional tests performed, as needed, during operation:	
Pairwise Consistency Tests	The module performs pairwise consistency tests whenever DSA, RSA or ECC asymmetric keys are generated.
Continuous RNG	16 bits continuous testing is performed during each use of the FIPS140-2 approved deterministic RNG. This test is a “stuck at” test to check the RNG output data for failure to a constant value. The test is performed for both the deterministic and non-deterministic RNGs implemented in the module.
Bypass Tests	The module tests for correct operation of the switching mechanism whenever it is modified or used to switch between a cryptographic service and a bypass service.
Software / Firmware Load Test	The module verifies a digital signature for any FIPS-validated firmware that is externally loaded onto the cryptographic module.

Any self test success or failure messages are output to error log files.

Known answer tests for encryption/decryption or hashing, function by encrypting (or hashing) a string for which the calculated output is known and stored within the cryptographic module. An encryption or hashing test passes when the freshly calculated output matches the expected (stored) value. A test fails when the calculated outmatch does not match the expected value. The test then decrypts the ciphertext string. A decryption test passes when the freshly calculated output matches the plaintext value. A test fails when the calculated output does not match the plaintext value.

Known answer tests for Random Number Generators function by seeding the RNG with known values and checking that the output matches the pre-calculated value stored within the cryptographic module. The test passes when the freshly generated output matches the pre-calculated value. A test fails when the generated output does not match the pre-calculated value.

Pairwise consistency tests for RSA, ECC and DSA keys (these keys are used for key transport) use the public key to encrypt a plaintext value. The resulting ciphertext value is compared to the original plaintext value. If the two values are equal, then the test fails. If the two values differ, the private key is used to decrypt the ciphertext and the resulting value is compared to the original plaintext value. If the two values are not equal, the test fails. These errors are the result of hard errors and will likely result in the module requiring service. The options that the customer has to clear the error are to reboot, attempt a factory reset, or contact Optica for service.

The bypass tests the correct operation of the switching mechanism whenever the mechanism governing selection of a bypass service or a cryptographic service is modified and whenever the module encounters a condition causing it to switch between a cryptographic service and a bypass service. The test verifies the digital signature of the configuration table to determine whether it has been modified. If the signature is valid, the test passes. If the signature is invalid, the test fails.

11 Mitigation of Attacks

The cryptographic module is not designed to mitigate specific attacks such as differential power analysis or timing attacks.

12 References

National Institute of Standards and Technology, *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, available at URL: csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex A: Approved Security Functions*, available at URL: csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex B: Approved Protection Profiles*, available at URL: csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex C: Approved Random Number Generators*, available at URL: csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *FIPS 140-2 Annex D: Approved Key Establishment Techniques*, available at URL: csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology and Communications Security Establishment, *Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at URL: csrc.nist.gov/groups/STM/cmvp.

National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standards Publication 46-3, available at URL: csrc.nist.gov/groups/STM/cavp.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, available at URL: csrc.nist.gov/groups/STM/cavp.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, available at URL: csrc.nist.gov/groups/STM/cavp.

National Institute of Standards and Technology, *Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication 180-1, available at URL: csrc.nist.gov/groups/STM/cavp.