PacketLight Networks Ltd.

PL-4000M and PL-4000T

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.0
July 2025

Prepared by:

Lightship Security

Applus

www.lightshipsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for the PacketLight Networks Ltd. PL-4000M and PL-4000T cryptographic modules (also referred to as "the module(s)" hereafter) running firmware version 2.1.0. It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard for an overall Security Level 2 module.

1.2 Security Levels

The table below describes the individual security areas of FIPS 140-3, as well as the Security Levels of those individual areas.

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

The Module has an overall security level of 2.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The PL-4000M and PL-4000T are two product variations of the PL-4000x clone. The hardware modules run the same firmware and provide the same cryptographic security services.

The PL-4000M is a cost-effective solution for rolling out multi-rate 10/25/100GbE, 16G FC, OTU2/2e/4 services, or increasing existing network capacity. The device delivers up to 600G in a 1U chassis using dual 400G CFP2-DCO Open ROADM standards-based pluggable coherent modules for metro and long-haul applications. The PL-4000M provides a full demarcation point between the service and the OTN/DWDM network and is interoperable with any third-party switch or router. This provides full visibility and performance monitoring of both line optical transport layer (OTN) and 10/25/100GbE, 16G FC, and OTU2/2e/4 service interfaces.

The PL-4000M can be configured to work in the following system modes:

- Single 400G Muxponder: mix of client interfaces aggregated into a 400G uplink
- Dual 100/200/300G Muxponder: mix of client interfaces aggregated into two 100/200/300G uplinks
- Optical Amplifiers: Up to two EDFA modules (optional)
- Optical Switch: 1+1 facility protection (optional)

The PL-4000T is a cost-effective high-capacity solution for rolling out 400GbE and 100GbE services or increasing existing network capacity. The device has four 400G pluggable uplink optical modules, delivering up to 1.6T in a 1U chassis. The PL-4000T integrates mux/demux, EDFA and OSW and delivers the entire optical layer. This flexible solution enables pay-as-you-grow architecture. The solution provides a full demarcation point between the service and the DWDM network and is interoperable with any third-party switch or router. This provides full visibility and performance monitoring of both the optical transport layer (OTN) and 100GbE/400GbE/OTU4 service interfaces.

The PL-4000T can be configured to work in the following system modes:

- Muxponder: 4x100G clients per 200G/300G/400G slice
- Transponder: 1x400G per 400G
- Optical Amplifiers: Up to two EDFA modules (optional)
- Mux/Demux: 4ch mux/demux module (optional)
- Optical Switch: 1+1 optical switch, 4 x 1+1 optical switches

Module Type: Hardware

Module Embodiment: MultiChipStand

Cryptographic Boundary:

The cryptographic boundary of the modules is defined as the entire outer casing of the chassis as pictured below. The PL-4000T's cryptographic boundary includes uplink module(s) which are protected by Tamper-evident Seals (see Section 7.1).

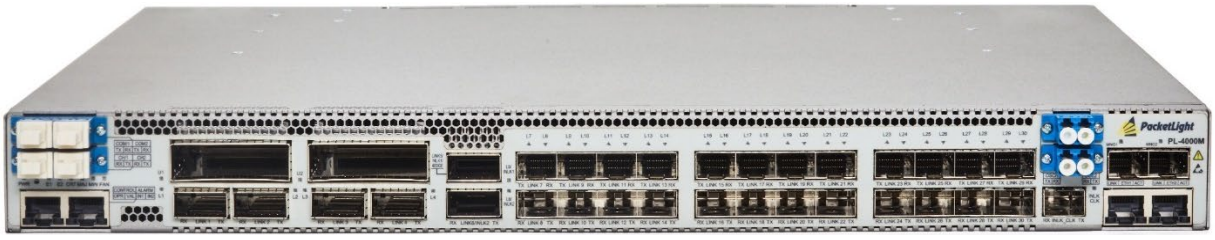


Figure 1: PL-4000M

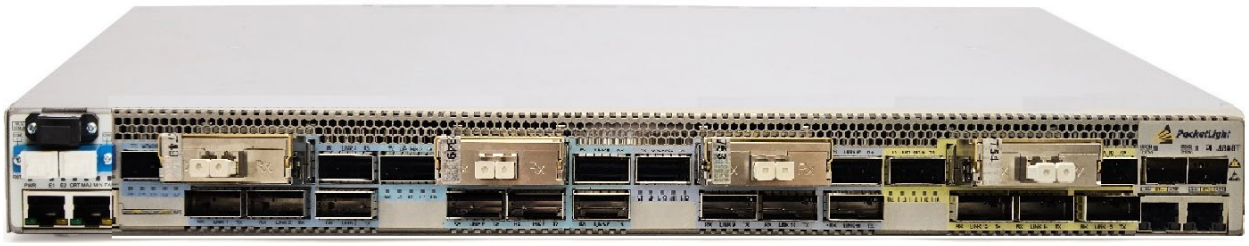


Figure 2: PL-4000T

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PL-4000M	PL-4000M	2.1.0	NXP Layerscape LS1026A	AC/DC PSU
PL-4000T	PL-4000T	2.1.0	NXP Layerscape LS1026A	AC/DC PSU

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

None.

2.4 Modes of Operation

Modes List and Description:

The table below details the Mode of Operation supported by the module.

Mode Name	Description	Type	Status Indicator
Approved Mode	When installed, initialized and configured as specified in Section 11 of the Security Policy, and with the tamper evident seals installed as indicated in Section 7 of the Security Policy, the module only runs in the approved mode of operation.	Approved	Global

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

The table below lists all the Approved Algorithms supported by the module.

Algorithm	CAVP Cert	Properties	Reference
AES-CFB128	A4261	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A4136	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-CTR	A4261	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A2709	Direction - Encrypt Key Length - 256	SP 800-38A
AES-ECB	A4261	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-GCM	A2709	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D
AES-GCM	A4261	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1 Key Length - 128, 256	SP 800-38D
AES-GMAC	A4136	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256	SP 800-38D
Counter DRBG	A4261	Prediction Resistance - Yes Mode - AES-256 Derivation Function Enabled - No	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-5)	A4261	Curve - P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A4261	Curve - P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A4261	Curve - P-384 Hash Algorithm - SHA2-384, SHA2-512/224	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4261	Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-5
HMAC-SHA2-256	A4261	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4261	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A4261	Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4261	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A4261	Domain Parameter Generation Methods - ffdhe2048, ffdhe3072, MODP-2048, MODP-3072, MODP-4096 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA OneStep SP800-56Cr2	A4261	Derived Key Length - 2048 Shared Secret Length - Shared Secret Length: 224-8192 Increment 8	SP 800-56C Rev. 2
KDF SNMP (CVL)	A4261	Password Length - Password Length: 64-160 Increment 8	SP 800-135 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
KDF SSH (CVL)	A4261	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA2-256, SHA2-512	SP 800-135 Rev. 1
RSA KeyGen (FIPS186-5)	A4261	Key Generation Mode - probableWithProbableAux Modulo - 2048 Primality Tests - 2powSecStr Private Key Format - standard	FIPS 186-5
Safe Primes Key Generation	A4261	Safe Prime Groups - ffdhe2048, ffdhe3072, MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
Safe Primes Key Verification	A4261	Safe Prime Groups - ffdhe2048, ffdhe3072, MODP-2048, MODP-3072, MODP-4096	SP 800-56A Rev. 3
SHA2-256	A4261	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4261	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4261	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A4261	Hash Algorithm - SHA2-256, SHA2-384	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A4261	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The table below lists all the Vendor-Affirmed Algorithms supported by the module.

Name	Properties	Implementation	Reference
CKG	Key Type:Asymmetric	PacketLight Cryptographic Implementation	IG D.H, SP800-133r2 (Section 4/example 1) The seed used in asymmetric key generation is the unmodified output from a NIST SP 800- 90A DRBG.

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not support any Non-Approved, Allowed Algorithms.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The module does not support any Non-Approved, Allowed Algorithms with No Security Claimed.

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The module does not support any Non-Approved Algorithms that are not Allowed in the Approved Mode of Operation.

N/A for this module.

2.6 Security Function Implementations

The table below lists the Security Function Implementations supported by the module.

Name	Type	Description	Properties	Algorithms
Config File Encrypt/Decrypt	BC-UnAuth	Encryption/Decryption of respective SSPs in configuration files		AES-CTR: (A4261) Key Length: 256
Key File Encrypt/Decrypt	BC-UnAuth	Encryption/Decryption of respective SSPs in key files		AES-ECB: (A4261)
SNMPv3 Encrypt/Decrypt	BC-UnAuth	Encryption/Decryption of SNMPv3 packets		AES-CFB128: (A4261)
SSH Encrypt/Decrypt 1	BC-UnAuth	Encryption/Decryption of SSH session packets		AES-CTR: (A4261)
SSH Encrypt/Decrypt 2	BC-Auth	Encryption/Decryption of SSH session packets		AES-GCM: (A4261)
TLS Encrypt/Decrypt	BC-Auth	Encryption/Decryption of TLS session packets		AES-GCM: (A4261)
Client Data Encrypt/Decrypt 1	BC-Auth	Encryption/Decryption of Client Data (PL-4000M hardware block)		AES-CTR: (A4136) AES-GMAC: (A4136)
Client Data Encrypt/Decrypt 2	BC-Auth	Encryption/Decryption of Client Data (DCO transceiver hardware block, inserted into 4000T)		AES-GCM: (A2709) AES-ECB: (A2709)
TLS Key Pair/Certificate Generation	AsymKeyPair-KeyGen	Generation of certificate and keys for TLS server authentication		ECDSA KeyGen (FIPS186-5): (A4261) Counter DRBG: (A4261)
SSH Key Pair Generation	AsymKeyPair-KeyGen	Generation of keys for SSH server authentication		RSA KeyGen (FIPS186-5): (A4261) Counter DRBG: (A4261)
TLS Key Pair Verification	AsymKeyPair-KeyVer	TLS Key Pair Verification		ECDSA KeyVer (FIPS186-5): (A4261)
TLS Digital Signature Generation	DigSig-SigGen	TLS Digital Signature Generation		ECDSA SigGen (FIPS186-5): (A4261)
TLS Digital Signature Verification	DigSig-SigVer	TLS Digital Signature Verification		ECDSA SigVer (FIPS186-5): (A4261)
SSH Message Authentication 1	MAC	SSH Message Authentication		HMAC-SHA2-256: (A4261)
SSH Message Authentication 2	MAC	SSH Message Authentication		HMAC-SHA2-512: (A4261) SHA2-512: (A4261)
TLS Message Authentication 1	MAC	TLS Message Authentication		HMAC-SHA2-256: (A4261)

Name	Type	Description	Properties	Algorithms
TLS Message Authentication 2	MAC	TLS Message Authentication		HMAC-SHA2-384: (A4261) SHA2-384: (A4261)
SNMP Message Authentication 1	MAC	SNMP Message Authentication		HMAC-SHA2-256: (A4261)
SNMP Message Authentication 2	MAC	SNMP Message Authentication		HMAC-SHA2-384: (A4261) SHA2-384: (A4261)
SNMP Message Authentication 3	MAC	SNMP Message Authentication		HMAC-SHA2-512: (A4261) SHA2-512: (A4261)
Data Plane KEX Message Authentication	MAC	Data Plane KEX Message Authentication (prevents man-in-the-middle)		HMAC-SHA2-384: (A4261) SHA2-384: (A4261)
Verify Firmware Integrity	MAC	Verify Firmware Integrity		HMAC-SHA2-384: (A4261) SHA2-384: (A4261)
Verify Firmware Load	MAC	Verify Firmware Load		HMAC-SHA2-384: (A4261) SHA2-384: (A4261)
KAS 1	KAS-Full	Data exchange keys generation and distribution	IG:D.F Scenario 2 path (2) Bit Strength Caveat:provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4261) KDA OneStep SP800-56Cr2: (A4261)
KAS 2	KAS-Full	Key Agreement for SSH	IG:D.F Scenario 2 path (2) Bit Strength Caveat:provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4261) KDF SSH: (A4261)
KAS 3	KAS-Full	Key Agreement for SSH	IG:D.F Scenario 2 path (2) Bit Strength Caveat:provides between 112 and 152 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A4261) Domain Parameter Generation Methods: MODP-2048, MODP-3072 and MODP-4096 KDF SSH: (A4261)
KAS 4	KAS-Full	Key Agreement for TLSv1.2	IG:D.F Scenario 2 path (2) Bit Strength	KAS-ECC-SSC Sp800-56Ar3: (A4261)

Name	Type	Description	Properties	Algorithms
			Caveat:provides between 128 and 256 bits of encryption strength	TLS v1.2 KDF RFC7627: (A4261)
KAS 5	KAS-Full	Key Agreement for TLSv1.3	IG:D.F Scenario 2 path (2) Bit Strength Caveat:provides between 128 and 256 bits of encryption strength	KAS-ECC-SSC Sp800-56Ar3: (A4261) TLS v1.3 KDF: (A4261)
KAS 6	KAS-Full	Key Agreement for TLS v1.3	IG:D.F Scenario 2 path (2) Bit Strength Caveat:provides 112 or 128 bits of encryption strength	KAS-FFC-SSC Sp800-56Ar3: (A4261) Domain Parameter Generation Methods: ffdhe2048, ffdhe3072 TLS v1.3 KDF: (A4261)
SNMP Key Derivation	KAS-135KDF	Derives SNMPv3 Keys		KDF SNMP: (A4261)
SSH Key Derivation	KAS-135KDF	Derives SSH Keys		KDF SSH: (A4261)
TLS Key Derivation	KAS-135KDF	Derives TLS 1.2/3 Keys		TLS v1.2 KDF RFC7627: (A4261) TLS v1.3 KDF: (A4261)
Password Obfuscation	SHA	Operator Password obfuscation in config file		SHA2-256: (A4261)
Entropy Source	ENT-ESV	Entropy Source		
KAS Key Pair Generation 1	KAS-KeyGen	KAS Key Pair Generation (ECDH)		ECDSA KeyGen (FIPS186-5): (A4261) ECDSA KeyVer (FIPS186-5): (A4261) Counter DRBG: (A4261)
KAS Key Pair Generation 2	KAS-KeyGen	KAS Key Pair Generation (DH)		Safe Primes Key Generation: (A4261) Safe Primes Key Verification: (A4261) Counter DRBG: (A4261)
DRBG	DRBG	Deterministic Random Bit Generation		Counter DRBG: (A4261)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

The module's TLS v1.2 firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #1. The module is compatible with TLS v1.2 and provides support for the acceptable GCM ciphersuites from SP 800-52 Rev2, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key (in accordance with RFC 5246). In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

The module's TLS v1.3 firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #5. The TLS v1.3 protocol, and specifically the use of the AES-GCM encryption within the TLS v1.3 protocol is defined in RFC 8446. The module supports the acceptable GCM ciphersuites from SP 800-52 Rev2, Section 3.3.1. The IV is generated and used within this protocol's implementation.

The module's SSHv2 firmware AES-GCM implementation conforms to FIPS 140-3 IG C.H Scenario #1. The SSHv2 implementation is compliant with RFC 4252 and RFC 4253, and the IV generation of SSHv2 AES-GCM implementation is compliant with RFC 5647.

The module's hardware AES-GCM implementations conform to IG C.H, scenario #4. The module uses a 96-bit IV, which is constructed deterministically per SP 800-38D Section 8.2.1 from a nonce and counter.

PL-4000T - from a Frame Block Counter, Multi-Frame Index (MFI), Multi Frame Alignment Signal (MFAS) and nonce.

PL-4000M - from Frame Counter (which is comprised of MFAS and MFI-38 bits and 26 zero pads), and Frame Block Counter (32-bits).

Per the requirements specified in Section 8 in NIST SP 800-38D, the probability that the authenticated encryption function ever will be invoked with the same IV and the same key on two (or more) distinct sets of input data is no greater than 2^{-32}.

In all cases the module enforces FIPS 140-3 IG C.H, which states, "In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established."

2.8 RBG and Entropy

The tables below detail the modules ESV information.

Cert Number	Vendor Name
E63	ID QUANTIQUE SA

Table 7: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
IDQ Quantis IID QRNG	Physical	IDQ250C2	2 bits	1.75 bits	

Table 8: Entropy Sources

2.9 Key Generation

Please see SFI table.

2.10 Key Establishment

Please see SFI table.

The module implements the DH and ECDH key agreement schemes specified in NIST SP 800-56Arev3.

This specification requires that certain checks are performed to provide assurances regarding the keys being used.

The following assurance checks are performed by the cryptographic module:

- Assurances of domain parameter validity (section 5.5.2 of NIST SP 800-56Arev3)
- Assurances required by the key pair owner (section 5.6.2.1 of NIST SP 800-56Arev3)
- Assurances required by the public key recipient (section 5.6.2.2 of NIST SP 800-56Arev3)

2.11 Industry Protocols

No parts of the SSH protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

No parts of the SNMP protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

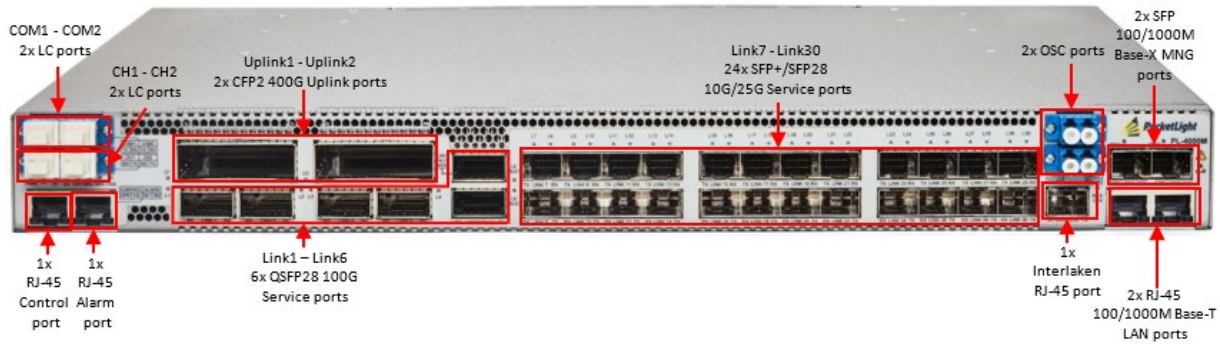


Figure 3: PL-4000M (Front)

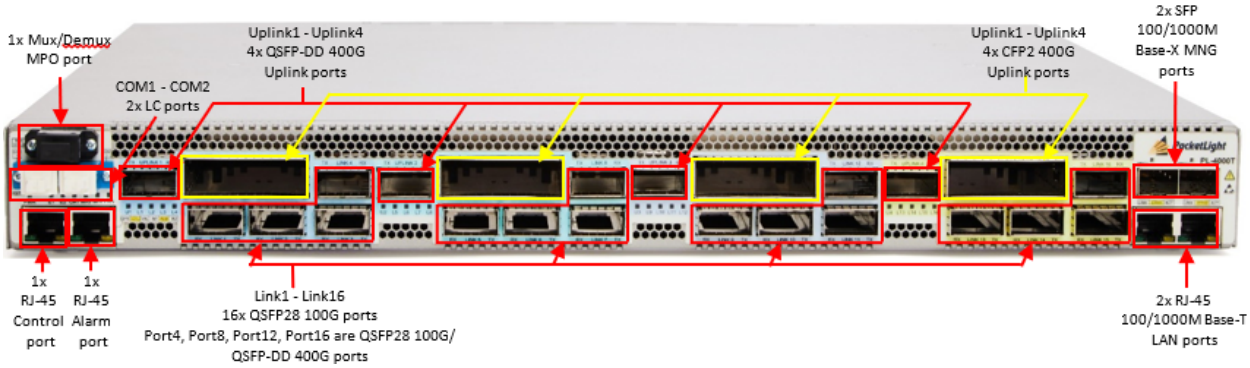


Figure 4: PL-4000T (Front)

Figure 5: PL-4000M and PL-4000T (Rear)

The table below details the modules Ports and Interfaces.

Physical Port	Logical Interface(s)	Data That Passes
LC ports (4000M)	None	Not in use
CFP2 400G Uplink ports (4000M)	Data Input Data Output Control Input Status Output	Muxponded/Transponded data, Inband management
SFP+/SFP28 10G/25G Service ports (4000M)	Data Input Data Output Status Output	Data
OSC ports (4000M)	None	Not in use

Physical Port	Logical Interface(s)	Data That Passes
SFP 100/1000M Base-X MNG ports (4000M)	Control Input Status Output	Management
RJ-45 Control port (4000M)	Control Input Status Output	Local CLI
RJ-45 Alarm port (4000M)	Status Output	External alarms dry contacts
QSFP28 100G Service ports (4000M)	Data Input Data Output Status Output	Data
Interlaken RJ-45 port (4000M)	None	Not in use
RJ-45 100/1000M Base-T LAN ports (4000M)	Control Input Status Output	Management
LEDs (4000M)	Status Output	Status
Power connectors (4000M)	Power	Power
Mux/Demux MPO port (4000T)	None	Not in use
LC ports (4000T)	None	Not in use
QSFP-DD 400G Uplink ports (4000T)	None	Not in use
CFP2 400G Uplink ports (4000T)	Data Input Data Output Control Input Status Output	Transponded data, Inband management
SFP 100/1000M Base-X MNG ports (4000T)	Control Input Status Output	Management
RJ-45 Control port (4000T)	Control Input Status Output	Local CLI
RJ-45 Alarm port (4000T)	Status Output	External alarms dry contacts
QSFP28 100G ports QSFP28 100G/ QSFP-DD 400G ports (4000T)	Data Input Data Output Control Input Status Output	Data
RJ-45 100/1000M Base-T LAN ports (4000T)	Control Input Status Output	Management
LEDs (4000T)	Status Output	Status

Physical Port	Logical Interface(s)	Data That Passes
Power connectors (4000T)	Power	Power

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

The table below details the modules Authentication Methods.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
WebGUI (HTTPS) Auth	Grants access to GUI according to role	Username and Password	Passwords are required to be at minimum 8 characters in length, and at maximum 20 bytes. Accepted characters are a-z, A-Z, 0-9, and [$@#&_!%^*]. An 8-character password allowing all legal characters (73) with repetition equates to a 1:(73^8), or 1: 806,460,091,894,081 chance of false acceptance.	Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/73^8, which is less than 1/100,000.
SSH/SFTP Auth	Grants access to CLI according to role	Username and Password	Passwords are required to be at minimum 8 characters in length, and at maximum 20 bytes. Accepted characters are a-z, A-Z, 0-9, and [$@#&_!%^*]. An 8-character password allowing all legal characters (73) with repetition equates to a 1:(73^8), or 1: 806,460,091,894,081 chance of false acceptance.	Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-minute period is 600/73^8, which is less than 1/100,000.
Console Auth	Grants access to CLI according to role	Username and Password	Passwords are required to be at minimum 8 characters in length, and at maximum 20 bytes. Accepted characters are a-z, A-Z, 0-9, and [$@#&_!%^*]. An 8-character password allowing all legal characters (73) with repetition equates to a 1:(73^8), or 1: 806,460,091,894,081 chance of false acceptance.	The fastest data rate for the serial port is 115,200 bps. Each ASCII character is 10 bits (1 Start, 8 data, 1 Stop), so that is (115,200 / 10 =) 115,20 characters per second or (115,20 * 60 =) 691,200 characters per minute. Running 100,000 trials in a minute will require a minimum of (4 * 10 * 100,000 =) 4,000,000 characters to be sent. This exceeds the 691,200 limit imposed by the data rate of the serial port. Therefore, the probability that a random attempt will succeed in one minute is less than 1/100,000.
SNMPv3 Auth	Verifying the rights of SNMP based processes to access for	Username and Password	Passwords are required to be at minimum 8 characters in length, and at maximum 20 bytes. Accepted characters are a-z, A-Z, 0-9, and [$@#&_!%^*]. An 8-character	Assuming 10 attempts per second via a scripted or automatic attack, the probability of a success with multiple attempts in a one-

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	monitoring and management		password allowing all legal characters (73) with repetition equates to a 1:(73^8), or 1: 806,460,091,894,081 chance of false acceptance.	minute period is 600/73^8, which is less than 1/100,000.

Table 10: Authentication Methods

4.2 Roles

The module supports four different roles: Admin, Crypto, Read-Write and Read-Only, which are detailed in the table below.

Name	Type	Operator Type	Authentication Methods
Admin	Role	CO	WebGUI (HTTPS) Auth SSH/SFTP Auth Console Auth SNMPv3 Auth
Crypto	Role	CO	WebGUI (HTTPS) Auth SSH/SFTP Auth Console Auth
Read-Write	Role	CO	WebGUI (HTTPS) Auth SSH/SFTP Auth Console Auth SNMPv3 Auth
Read-Only	Role	CO	WebGUI (HTTPS) Auth SSH/SFTP Auth Console Auth SNMPv3 Auth

Table 11: Roles

4.3 Approved Services

The table below lists all approved services supported by the module. The abbreviations of the access rights to keys and SSPs have the following interpretation:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialization	Initial Configuration	N/A	Command and parameters	Command response/ status	None	Admin

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Manage Accounts	Add, Edit, Delete, View user accounts	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command and parameters	Command response/ status	Password Obfuscation	Admin - Operator Passwords: W
Change Password	Admin to any except Crypto, each user its own	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command and parameters	Command response/ status	Password Obfuscation	Admin - Operator Passwords: W Crypto - Operator Passwords: W Read-Write - Operator Passwords: W Read-Only - Operator Passwords: W
Encryption Service	Transfer of encryption data	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command and parameters	Command response/ status	Client Data Encrypt/Decrypt 1 Client Data Encrypt/Decrypt 2 Data Plane KEX Message Authentication KAS 1 KAS Key Pair Generation 1	Admin - EC DH Key Pair for DEK: G,E - ECC CDH primitive for DEK: G,E - Data Encryption Key (DEK): G,E - Peer-Authentication Pre-Shared Secret: R,W,E Read-Write - EC DH Key Pair for DEK: G,E - ECC CDH primitive for DEK: G,E - Data Encryption Key (DEK): G,E - Peer-Authentication Pre-Shared Secret: R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Add/Change Pre-Shared Secret	Add/Changes the pre-shared secret used for the authentication of the key exchange messages.	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command and parameters	Command response/ status	Config File Encrypt/Decrypt	Crypto - Peer-Authentication Pre-Shared Secret: W
Lock Encrypted Service	Locks the encrypted uplink port.	N/A	Command	Command response/ status	None	Crypto
Change Provisioning Type	Provisions the service port or remove provisioning from the selected port	N/A	Command	Command response/ status	None	Admin Read-Write
View System Information	View system specific information	N/A	Command	Command response/ status	None	Admin Crypto Read-Write Read-Only
View Performance Monitoring	View port performance monitoring info	N/A	Command	Command response/ status	None	Admin Crypto Read-Write Read-Only
View Faults or Alarms	Used to localize and identify problems in the network	N/A	Command	Command response/ status	None	Admin Crypto Read-Write Read-Only
Configure Firewall	Configure Firewall rules/policies	N/A	Command and parameters	Command response/ status	None	Admin
Show Status	Outputs current module status	N/A	Command	Command response/ status	None	Admin Crypto Read-Write Read-Only
Show Versioning information	Returns module name/identifier and versioning information	N/A	Command	Module versioning information	None	Admin Crypto Read-Write Read-Only
Set Configuration data	Device configuration tool	N/A	Command and parameters	Command response/ status	None	Admin Read-Write
Establish SSH session	Establish an SSH session	Global ("FIPS Compliant Mode") in combination	Command	Command response/ status	Key File Encrypt/Decrypt SSH Encrypt/Decrypt	Admin - Operator Passwords: W - Diffie-Hellman

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		with successful completion of service			1 SSH Encrypt/Decrypt 2 SSH Key Pair Generation SSH Message Authentication 1 SSH Message Authentication 2 KAS 2 KAS 3 SSH Key Derivation KAS Key Pair Generation 1 KAS Key Pair Generation 2	(DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - SSH/SFTP Host Key Pair: G,E - SSH/SFTP Session Encryption Key: G,E - SSH/SFTP Session Authentication key: G,E Crypto - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - SSH/SFTP Host Key Pair: G,E - SSH/SFTP Session Encryption Key: G,E - SSH/SFTP Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication key: G,E Read-Write - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - SSH/SFTP Host Key Pair: G,E - SSH/SFTP Session Encryption Key: G,E - SSH/SFTP Session Authentication key: G,E Read-Only - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - SSH/SFTP Host Key Pair: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH/SFTP Session Encryption Key: G,E - SSH/SFTP Session Authentication key: G,E
Establish TLS session	Establish a web session using TLS protocol	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command	Command response/ status	Key File Encrypt/Decrypt TLS Encrypt/Decrypt TLS Key Pair/Certificate Generation TLS Key Pair Verification TLS Digital Signature Generation TLS Digital Signature Verification TLS Message Authentication 1 TLS Message Authentication 2 KAS 4 KAS 5 KAS 6 TLS Key Derivation KAS Key Pair Generation 1 KAS Key Pair Generation 2	Admin - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - TLS Key Pair: G,E - TLS Premaster Secret: G,E - TLS Master Secret: G,E - TLS Session Encryption Key: G,E - TLS Session Authentication Key: G,E Crypto - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - TLS Key Pair: G,E - TLS Premaster Secret: G,E - TLS Master Secret: G,E - TLS Session Encryption Key: G,E - TLS Session Authentication Key: G,E Read-Write - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - TLS Key Pair: G,E - TLS Premaster Secret: G,E - TLS Master Secret: G,E - TLS Session Encryption Key: G,E - TLS Session Authentication Key: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Read-Only - Operator Passwords: W - Diffie-Hellman (DH) Key Pair: G,E - Diffie-Hellman Shared Secret: G,E - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: G,E - EC Diffie-Hellman Shared Secret: G,E - TLS Key Pair: G,E - TLS Premaster Secret: G,E - TLS Master Secret: G,E - TLS Session Encryption Key: G,E - TLS Session Authentication Key: G,E
Configure SNMPv3	Configure SNMPv3 security profile, authentication, privacy, etc. settings	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command and parameters	Command response/ status	SNMPv3 Encrypt/Decrypt SNMP Message Authentication 1 SNMP Message Authentication 2 SNMP Message Authentication 3 SNMP Key Derivation	Admin - SNMP Privacy Key: G,E - SNMP Authentication Key: G,E - SNMPv3 Passwords (Privacy and Auth): W
SNMPv3 traps	Provide system condition information	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command	Command response/ status	None	Admin - SNMPv3 Passwords (Privacy and Auth): W Read-Write - SNMPv3 Passwords

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(Privacy and Auth): W
Export Backup of Configuration file over HTTPS/SFTP	Save device and services configuration into file	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command	Command response/ status	Config File Encrypt/Decrypt Password Obfuscation	Admin - Operator Passwords: R - Peer-Authentication Pre-Shared Secret: R - SNMPv3 Passwords (Privacy and Auth): R
Restore Configuration file over HTTPS/SFTP	Restore device and services configuration into file	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command	Command response/ status	Config File Encrypt/Decrypt Password Obfuscation	Admin - Operator Passwords: W - Peer-Authentication Pre-Shared Secret: W - SNMPv3 Passwords (Privacy and Auth): W
View Network Topology	View the structure of a network	N/A	Command	Command response/ status	None	Admin Crypto Read-Write Read-Only
Random Number Generation	Random Number Generation	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command	Command response/ status	Entropy Source DRBG	Admin - SP 800-90A CTR_DRBG Entropy Input: E - SP 800-90A CTR_DRBG Seed: E - SP 800-90A CTR_DRBG key value: E - SP 800-90A CTR_DRBG V value: E Crypto - SP 800-90A CTR_DRBG Entropy Input: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SP 800-90A CTR_DRBG Seed: E - SP 800-90A CTR_DRBG key value: E - SP 800-90A CTR_DRBG V value: E Read-Write - SP 800-90A CTR_DRBG Entropy Input: E - SP 800-90A CTR_DRBG Seed: E - SP 800-90A CTR_DRBG key value: E - SP 800-90A CTR_DRBG V value: E Read-Only - SP 800-90A CTR_DRBG Entropy Input: E - SP 800-90A CTR_DRBG Seed: E - SP 800-90A CTR_DRBG key value: E - SP 800-90A CTR_DRBG V value: E
Perform Self-Tests On-Demand	Run self-tests	N/A	Command	Command response/ status	Verify Firmware Integrity	Admin Read-Write
Factory Reset	See Section 9.3	Status	Command	Command response/ status	None	Admin - Operator Passwords: Z - EC DH Key Pair for DEK: Z - ECC CDH primitive for DEK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- Data Encryption Key (DEK): Z - Peer-Authentication Pre-Shared Secret: Z - Diffie-Hellman (DH) Key Pair: Z - Diffie-Hellman Shared Secret: Z - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: Z - EC Diffie-Hellman Shared Secret: Z - SNMP Privacy Key: Z - SNMP Authentication Key: Z - SNMPv3 Passwords (Privacy and Auth): Z - TLS Key Pair: Z - TLS Premaster Secret: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - SSH/SFTP Host Key Pair: Z - SSH/SFTP Session Encryption Key: Z - SSH/SFTP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Authentication key: Z - Firmware Update Key: Z - SP 800-90A CTR_DRBG Seed: Z - SP 800-90A CTR_DRBG Entropy Input: Z - SP 800-90A CTR_DRBG key value: Z - SP 800-90A CTR_DRBG V value: Z Read-Write - Operator Passwords: Z - EC DH Key Pair for DEK: Z - ECC CDH primitive for DEK: Z - Data Encryption Key (DEK): Z - Peer-Authentication Pre-Shared Secret: Z - Diffie-Hellman (DH) Key Pair: Z - Diffie-Hellman Shared Secret: Z - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: Z - EC Diffie-Hellman Shared Secret: Z - SNMP Privacy Key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SNMP Authentication Key: Z - SNMPv3 Passwords (Privacy and Auth): Z - TLS Key Pair: Z - TLS Premaster Secret: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - SSH/SFTP Host Key Pair: Z - SSH/SFTP Session Encryption Key: Z - SSH/SFTP Session Authentication key: Z - Firmware Update Key: Z - SP 800-90A CTR_DRBG Seed: Z - SP 800-90A CTR_DRBG Entropy Input: Z - SP 800-90A CTR_DRBG key value: Z - SP 800-90A CTR_DRBG V value: Z
Zeroization	See Section 9.3 (Zeroization)	Status	Command	Command response/ status	None	Admin - Operator Passwords: Z - EC DH Key Pair

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						for DEK: Z - ECC CDH primitive for DEK: Z - Data Encryption Key (DEK): Z - Peer-Authentication Pre-Shared Secret: Z - Diffie-Hellman (DH) Key Pair: Z - Diffie-Hellman Shared Secret: Z - Elliptic Curve Diffie-Hellman (ECDH) Key Pair: Z - EC Diffie-Hellman Shared Secret: Z - SNMP Privacy Key: Z - SNMP Authentication Key: Z - SNMPv3 Passwords (Privacy and Auth): Z - TLS Key Pair: Z - TLS Premaster Secret: Z - TLS Master Secret: Z - TLS Session Encryption Key: Z - TLS Session Authentication Key: Z - SSH/SFTP Host Key Pair: Z - SSH/SFTP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Encryption Key: Z - SSH/SFTP Session Authentication key: Z - Firmware Update Key: Z - SP 800-90A CTR_DRBG Seed: Z - SP 800-90A CTR_DRBG Entropy Input: Z - SP 800-90A CTR_DRBG key value: Z - SP 800-90A CTR_DRBG V value: Z
Firmware Update	Upload and deploy firmware	Global ("FIPS Compliant Mode") in combination with successful completion of service	Command	Command response/ status	Verify Firmware Load	Admin - Firmware Update Key: G,E Read-Write - Firmware Update Key: G,E

Table 12: Approved Services

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

N/A for this module.

4.5 External Software/Firmware Loaded

The version signature is verified by HMAC-SHA-384. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Bypass Actions and Status

The Bypass capability is the ability of a service to partially or wholly circumvent a cryptographic function or process.

The following two independent internal actions are required to activate the bypass capability, to prevent the inadvertent bypass of plaintext data due to a single error:

1. The admin shuts down the interface.

2. Then switches the interface to non-encrypted mode.

*Both actions are accompanied by a service impact warning

The module shows status to indicate that the bypass capability is alternately activated and deactivated, and that the module is providing some services with cryptographic processing and some services without cryptographic processing, as follows: If the bypass service indicator is “Bypass is in effect”, it means that at least one active service is not encrypted. If the bypass service indicator is “Bypass in not in effect”, it means that all active services are encrypted.

4.7 Cryptographic Output Actions and Status

The Self-initiated cryptographic output capability is the ability of the module to perform cryptographic operations and other approved security functions or SSP management techniques without external operator request.

The following two independent internal actions are required to activate the self-Initiated cryptographic output capability to prevent the inadvertent output due to a single error:

1. The admin selects the service type and turns on the interface.
2. The admin confirms the changes.

The module shows status to indicate whether the self-Initiated cryptographic output capability is activated through the Admin Status of the respective channel. If the self-Initiated cryptographic output service indicator is “Up” for a respective channel, it means that the capability is activated. If the self-Initiated cryptographic output service indicator is “Down” for a respective channel, it means that the capability is not activated.

5 Software/Firmware Security

5.1 Integrity Techniques

The firmware is delivered as an executable file and the module implements a HMAC-SHA2-384 keyed hash firmware integrity test.

5.2 Initiate on Demand

The Firmware Integrity Test can be invoked by rebooting the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

The table below details the Physical Security Mechanisms supported by the module.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-evident Seals	Minimum of every 30 days.	The CO shall inspect the enclosure and tamper-evident seals for physical signs of tampering or attempted access to the cryptographic module. The physical security of the module is intact if there is no evidence of tampering with the tamper-evident seals.

Table 13: Mechanisms and Actions Required

The module has a multi-chip standalone embodiment and is made of commercially available, production grade components meeting commercial specifications for power, temperature, reliability, shock and vibration. All production-grade components include standard passivation techniques, in the form of a coating applied over the module's circuitry to protect against environmental and other physical damage. The production grade metal enclosure is opaque to the visible spectrum, and all openings are designed in such a way to obscure visual access to the security relevant innards of the module.

7.2 User Placed Tamper Seals

Number: The PL-4000M is sealed with 4-5 tamper-evident seals, and the PL-4000T is sealed with 4-7 tamper-evident seals.

Placement: The locations of the tamper-evident seals are indicated by the red rectangles in Figures 6 and 7.

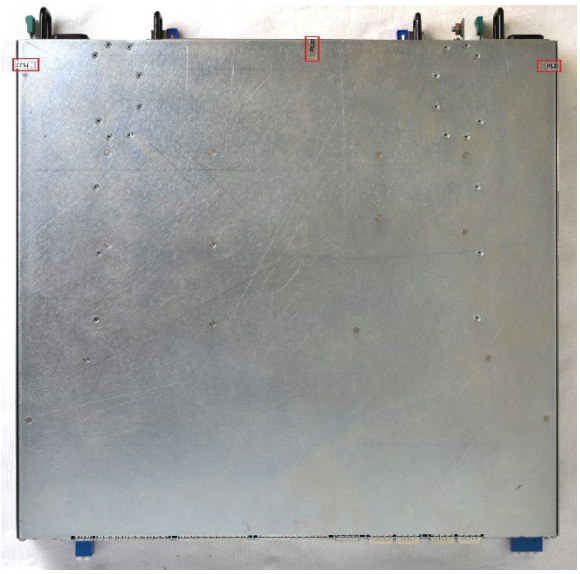
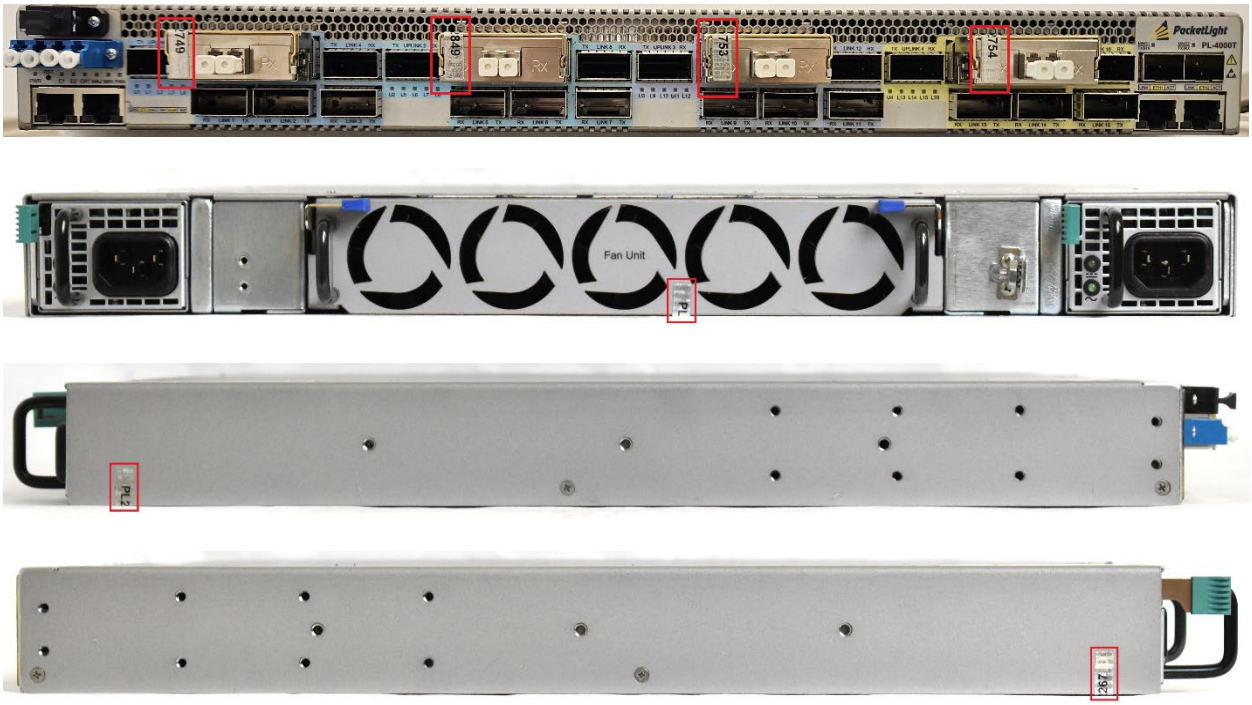


Figure 6: PL-40000M (Front, Rear, Left, Right, Bottom)



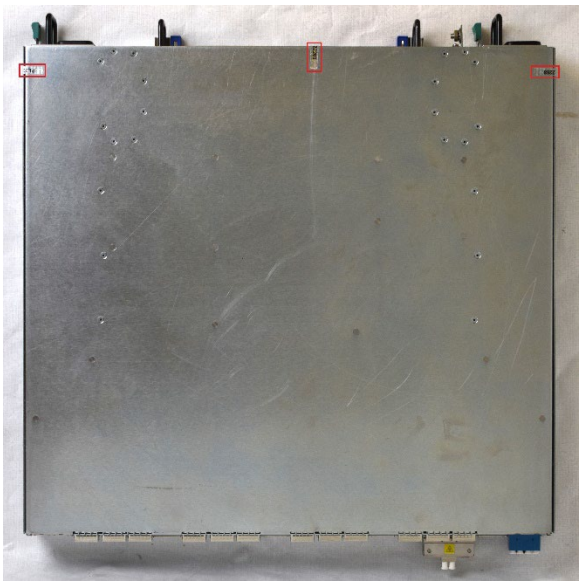


Figure 7: PL-40000T (Front, Rear, Left, Right, Bottom)

Surface Preparation:

For optimum adhesion, surfaces must be cleaned with alcohol to remove surface contaminants before affixing the tamper-evident seals:

- Use 90% (or higher) Isopropyl Alcohol
- Apply alcohol to a clean paper towel and wipe the intended surface to remove contaminants.
- Dry the surface with another clean paper towel (some contaminants will remain on the surface if the alcohol is allowed to air dry)
- Apply the label to the clean surface. NOTE: The adhesive side of the label must not be touched during the label placement. If it is inevitable, tweezer must be used for handling.

Operator Responsible for Securing Unused Seals: Crypto-Officer

Part Numbers: Holo-Guard FIPS

8 Non-Invasive Security

Currently, the ISO/IEC 19790:2012 non-invasive security area is not required by FIPS 140-3 (see NIST SP 800-140F). The requirements of this area are not applicable to the module.

9 Sensitive Security Parameters Management

9.1 Storage Areas

The table below lists Sensitive Security Parameters (SSPs) storage areas for the module. Section 9.4 below selects from the storage areas listed and specifies the appropriate parameter in the "Storage" column if applicable to a specific SSP.

Storage Area Name	Description	Persistence Type
DDR4 SDRAM	Random memory access	Dynamic
QSPI FLASH	Flash file system	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

The table below lists SSP input and output methods for the module. Section 9.4 below selects from the input and output methods listed and specifies the appropriate parameter in the "Inputs/Outputs" column if applicable to a specific SSP.

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
SSP Input 1	External	QSPI FLASH	Plaintext	Manual	Electronic	
SSP Input 2	External	QSPI FLASH	Encrypted	Manual	Electronic	
SSP Input 3	External	DDR4 SDRAM	Plaintext	Automated	Electronic	
SSP Output 1	QSPI FLASH	External	Encrypted	Manual	Electronic	
SSP Output 2	DDR4 SDRAM	External	Plaintext	Automated	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

The table below lists SSP zeroization methods for this module. Section 9.4 below selects from the zeroization methods listed and specifies the appropriate parameter in the "Zeroization" column if applicable to a specific SSP.

Zeroization Method	Description	Rationale	Operator Initiation
Session Termination	All session ephemeral keys are zeroized.	Loss of contents	By closing of HTTPS/SSH session.
Key Lifetime	Data Plane ephemeral keys are zeroized.	Loss of contents	N/A
Power Cycle	All session ephemeral keys are zeroized.	Loss of contents	Power cycle
Zeroization Command	All SSPs are zeroized. System IP is restored to default.	Loss of contents	Input zeroization command in console.
Factory Reset	All SSPs are zeroized. System IP is kept.	Loss of contents	Input factory reset command in console.

Table 16: SSP Zeroization Methods

9.4 SSPs

The following table summarizes the keys and Sensitive Security Parameters (SSPs) that are used by the cryptographic services implemented in the module:

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Operator Passwords	Authentication for the Admin, Crypto, Read-Write and Read-Only roles	Minimum of 8 bytes (64 bits) and maximum of 20 bytes (160 bits) string value - Minimum of 8 bytes (64 bits) and maximum of 20 bytes (160 bits) string value	Authentication string - CSP			
EC DH Key Pair for DEK	Key pair used in NIST SP 800-56Arev3 (Section 5.7.1.2) ECC CDH Primitive computation	P-384 - 192 bits	Public/Private - CSP	KAS Key Pair Generation 1		KAS 1
ECC CDH primitive for DEK	Shared Secret (Z) value that will be used to derive the DEK	384-bit string - 192 bits	Key Material - CSP		KAS 1	KAS 1
Data Encryption Key (DEK)	Used for encrypting or decrypting payload data	256-bit - 256 bits	Symmetric key - CSP		KAS 1	Client Data Encrypt/Decrypt 1 Client Data Encrypt/Decrypt 2
Peer-Authentication Pre-Shared Secret	Entered by Crypto. Parameter used for Peer-Authentication during key exchange	384-bit string - 384 bits	Authentication hex string - CSP			Data Plane KEX Message Authentication
Diffie-Hellman (DH) Key Pair	Negotiating TLS/HTTPS or SSH/SFTP sessions	Public: 2048-bit, 3072-bit, 4096-bit / Private: 224-bit, 256-bit, 325-bit - 112	Public/Private - CSP	KAS Key Pair Generation 2		KAS 3 KAS 6

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		bits, 128 bits, 152 bits				
Diffie-Hellman Shared Secret	Diffie-Hellman Shared Secret	2048-bit, 3072-bit, 4096-bit - 112 bits, 128 bits, 152 bits	Shared Secret - CSP		KAS 3 KAS 6	KAS 3 KAS 6
Elliptic Curve Diffie-Hellman (ECDH) Key Pair	Negotiating TLS/HTTPS or SSH/SFTP sessions	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Public/Private - CSP	KAS Key Pair Generation 1		KAS 2 KAS 4 KAS 5
EC Diffie-Hellman Shared Secret	EC Diffie-Hellman Shared Secret	P-256, P-384, P-521 - 128 bits, 192 bits, 256 bits	Shared Secret - CSP		KAS 2 KAS 4 KAS 5	KAS 2 KAS 4 KAS 5
SNMP Privacy Key	Encryption / Decryption of SNMP traffic	128-bit, 192-bit, 256-bit - 128 bits, 192 bits, 256 bits	Symmetric key - CSP	SNMP Key Derivation		SNMPv3 Encrypt/Decrypt
SNMP Authentication Key	Message authentication and verification in SNMP	HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 - 256 bits, 384 bits, 512 bits	Symmetric key - CSP	SNMP Key Derivation		SNMP Message Authentication 1 SNMP Message Authentication 2 SNMP Message Authentication 3
SNMPv3 Passwords (Privacy and Auth)	SNMPv3 Passwords	Minimum of 8 bytes (64 bits) and maximum of 20 bytes (160 bits) string value - Minimum of 8 bytes (64 bits) and maximum of 20 bytes (160 bits) string value	Authentication string - CSP			SNMP Key Derivation
TLS Key Pair	Key Pair used for TLS authentication	P-384 - 192 bits	Public/Private - CSP	TLS Key Pair/Certificate Generation		TLS Digital Signature Generation TLS Digital

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Signature Verification
TLS Premaster Secret	Establish the TLS Master Secret	384-bit string - 192 bits	Key material - CSP		KAS 4 KAS 5 KAS 6	TLS Key Derivation
TLS Master Secret	Establish the TLS Session Keys	384-bit string - 192 bits	Key material - CSP	TLS Key Derivation		TLS Key Derivation
TLS Session Encryption Key	Used for encrypting/ decrypting TLS messages	128-bit, 256-bit - 128 bits, 256 bits	Symmetric Key - CSP	TLS Key Derivation		TLS Encrypt/Decrypt
TLS Session Authentication Key	Used for authenticating TLS messages	HMAC SHA2-256, HMAC SHA2-384 - 256 bits, 384 bits	Symmetric Key - CSP	TLS Key Derivation		TLS Message Authentication 1 TLS Message Authentication 2
SSH/SFTP Host Key Pair	Key Pair used for SSH/SFTP authentication	2048-bit - 112 bits	Public/Private - CSP	SSH Key Pair Generation		
SSH/SFTP Session Encryption Key	Used for Encrypting SSH/SFTP messages	128-bit, 192-bit, 256-bit - 128 bits, 192 bits, 256 bits	Symmetric Key - CSP	SSH Key Derivation		SSH Encrypt/Decrypt 1 SSH Encrypt/Decrypt 2
SSH/SFTP Session Authentication key	Data authentication for SSH/SFTP sessions	HMAC SHA2-256, HMAC SHA2-512 - 256 bits, 512 bits	Symmetric Key - CSP	SSH Key Derivation		SSH Message Authentication 1 SSH Message Authentication 2
Firmware Update Key	Firmware Update Key	HMAC SHA2-384 - 384 bits	Symmetric Key - CSP	Factory		Verify Firmware Load
SP 800-90A CTR_DRBG Seed	Seeding material for the SP800-90A CTR_DRBG	384-bit value - 384-bit value	Key material - CSP	Entropy Source		DRBG
SP 800-90A CTR_DRBG Entropy Input	Entropy Input for the SP800-90A CTR_DRBG	384-bit value - 384-bit value	Key material - CSP	Entropy Source		DRBG
SP 800-90A CTR_DRBG key value	Used for the SP 800-90A CTR_DRBG	Internal state value - Internal state value	Internal state value - CSP	DRBG		DRBG
SP 800-90A CTR_DRBG V value	Used for the SP 800-90A CTR_DRBG	Internal state value -	Internal state value - CSP	DRBG		DRBG

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		Internal state value				

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Operator Passwords	SSP Input 1 SSP Input 2 SSP Output 1	QSPI FLASH:Obfuscated		Zeroization Command Factory Reset	
EC DH Key Pair for DEK	SSP Input 3 SSP Output 2	DDR4 SDRAM:Plaintext		Key Lifetime Power Cycle	ECC CDH primitive for DEK:Derives
ECC CDH primitive for DEK		DDR4 SDRAM:Plaintext		Key Lifetime Power Cycle	EC DH Key Pair for DEK:Derived From
Data Encryption Key (DEK)		DDR4 SDRAM:Plaintext		Key Lifetime Power Cycle	ECC CDH primitive for DEK:Derived From
Peer-Authentication Pre-Shared Secret	SSP Input 1 SSP Input 2 SSP Output 1	QSPI FLASH:Encrypted		Zeroization Command Factory Reset	
Diffie-Hellman (DH) Key Pair	SSP Input 3 SSP Output 2	DDR4 SDRAM:Plaintext		Session Termination Power Cycle	Diffie-Hellman Shared Secret:Derives
Diffie-Hellman Shared Secret		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	Diffie-Hellman (DH) Key Pair:Derived From
Elliptic Curve Diffie-Hellman (ECDH) Key Pair	SSP Input 3 SSP Output 2	DDR4 SDRAM:Plaintext		Session Termination Power Cycle	EC Diffie-Hellman Shared Secret:Derives
EC Diffie-Hellman Shared Secret		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	Elliptic Curve Diffie-Hellman (ECDH) Key Pair:Derived From
SNMP Privacy Key		DDR4 SDRAM:Plaintext		Power Cycle	SNMPv3 Passwords (Privacy and Auth):Derived From
SNMP Authentication Key		DDR4 SDRAM:Plaintext		Power Cycle	SNMPv3 Passwords (Privacy and Auth):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SNMPv3 Passwords (Privacy and Auth)	SSP Input 1 SSP Input 2 SSP Output 1	QSPI FLASH:Encrypted		Zeroization Command Factory Reset	SNMP Privacy Key:Derives SNMP Authentication Key:Derives
TLS Key Pair		QSPI FLASH:Encrypted		Zeroization Command Factory Reset	
TLS Premaster Secret		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	TLS Master Secret:Derives
TLS Master Secret		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	TLS Premaster Secret:Derived From TLS Session Encryption Key:Derives TLS Session Authentication Key:Derives
TLS Session Encryption Key		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	TLS Master Secret:Derived From
TLS Session Authentication Key		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	TLS Master Secret:Derived From
SSH/SFTP Host Key Pair		QSPI FLASH:Encrypted		Zeroization Command Factory Reset	
SSH/SFTP Session Encryption Key		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	
SSH/SFTP Session Authentication key		DDR4 SDRAM:Plaintext		Session Termination Power Cycle	
Firmware Update Key		QSPI FLASH:Encrypted		N/A	
SP 800-90A CTR_DRBG Seed		DDR4 SDRAM:Plaintext		Power Cycle	SP 800-90A CTR_DRBG Entropy Input:Derived From
SP 800-90A CTR_DRBG Entropy Input		DDR4 SDRAM:Plaintext		Power Cycle	
SP 800-90A CTR_DRBG key value		DDR4 SDRAM:Plaintext		Power Cycle	SP 800-90A CTR_DRBG Seed:Derived From
SP 800-90A CTR_DRBG V value		DDR4 SDRAM:Plaintext		Power Cycle	SP 800-90A CTR_DRBG Seed:Derived From

Table 18: SSP Table 2

10 Self-Tests

This section specifies the pre-operational and conditional self-tests performed by the module. The pre-operational and conditional self-tests ensure that the module is not corrupted and that the cryptographic algorithms work as expected.

10.1 Pre-Operational Self-Tests

Pre-operational Self-Tests are run upon the power up/initialization of the module. The module transitions to the operational state only after the pre-operational self-tests (and the cryptographic algorithm self-tests (CASTs)) are passed successfully. The design of the modules ensures that all data output, via the data output interface, is inhibited whenever the module is in a pre-operational self-test condition. The Pre-Operational Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-384 (A4261)	384-bit	Integrity Test	SW/FW Integrity	Status	Keyed message authentication code-based firmware integrity verification
SHA2-384 (A4261)	384-bit	Bypass Test	Bypass	Status	Ensures the correct operation of the logic governing activation of the bypass capability.

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Conditional Self-Tests are run when an applicable security function or process is invoked. The Conditional Self-Tests are detailed in the table below.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A4136)	256-bit	KATs	CAST	Status	Separate Encrypt and Decrypt	Power Up
AES-GMAC (A4136)	256-bit	KATs	CAST	Status	Separate Encrypt and Decrypt	Power Up
AES-ECB (A2709)	256-bit	KATs	CAST	Status	Separate Encrypt and Decrypt	Power Up
AES-GCM (A2709)	256-bit	KATs	CAST	Status	Separate Encrypt and Decrypt	Power Up
AES-ECB (A4261)	128-bit	KATs	CAST	Status	Separate Encrypt and Decrypt	Power Up
AES-GCM (A4261)	256-bit	KATs	CAST	Status	Separate Encrypt and Decrypt	Power Up
Counter DRBG (A4261)	128-bit	KAT	CAST	Status	SP 800-90 A Section 11.3	Power Up
ECDSA KeyGen (FIPS186-5) (A4261)	P-384, SHA2-384	PCT	PCT	Status	-	Key Pair Generation
ECDSA SigGen (FIPS186-5) (A4261)	P-384, SHA2-384	KAT	CAST	Status	Sign	Power Up
ECDSA SigVer (FIPS186-5) (A4261)	P-384, SHA2-384	KAT	CAST	Status	Verify	Power Up
HMAC-SHA2-384 (A4261)	384-bit	KAT	CAST	Status	-	Power Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
KAS-ECC-SSC Sp800-56Ar3 (A4261)	P-256	KAT	CAST	Status	Ephemeral Unified Shared Secret (Z) Computation	Power Up
KAS-FFC-SSC Sp800-56Ar3 (A4261)	2048-bit	KAT	CAST	Status	Ephemeral Unified Shared Secret (Z) Computation	Power Up
KDA OneStep SP800-56Cr2 (A4261)	SHA2-384	KAT	CAST	Status	-	Power Up
KDF SNMP (A4261)	-	KAT	CAST	Status	-	Power Up
KDF SSH (A4261)	SHA2-256	KAT	CAST	Status	-	Power Up
RSA KeyGen (FIPS186-5) (A4261)	2048-bit	PCT	PCT	Status	-	Key Pair Generation
Safe Primes Key Generation (A4261)	MODP-2048, MODP-3072, MODP-4096, ffdhe2048, ffdhe3072	PCT	PCT	Status	-	Key Pair Generation
SHA2-256 (A4261)	256-bit	KAT	CAST	Status	-	Power Up
SHA2-512 (A4261)	512-bit	KAT	CAST	Status	-	Power Up
TLS v1.2 KDF RFC7627 (A4261)	SHA2-256	KAT	CAST	Status	-	Power Up
TLS v1.3 KDF (A4261)	SHA2-256	KAT	CAST	Status	-	Power Up
Firmware Load Test (HMAC-SHA2-384 (A4261)	HMAC-SHA2-384	-	SW/FW Load	Status	-	Firmware Loading
SHA2-384 (A4261)	384-bit	-	Bypass	Status	-	Bypass modification
Adaptive Proportion Test (APT)	-	FD	CAST	Status	SP 800-90B Section 4	Continuous
Repetition Count Test (RCT)	-	FD	CAST	Status	SP 800-90B Section 4	Continuous

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Pre-operational self-tests can be run on-demand, for periodic testing, by rebooting the module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-384 (A4261)	Integrity Test	SW/FW Integrity	On Demand	Power Cycle
SHA2-384 (A4261)	Bypass Test	Bypass	On Demand	Power Cycle

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CTR (A4136)	KATs	CAST	On Demand	Power Cycle
AES-GMAC (A4136)	KATs	CAST	On Demand	Power Cycle
AES-ECB (A2709)	KATs	CAST	On Demand	Power Cycle
AES-GCM (A2709)	KATs	CAST	On Demand	Power Cycle
AES-ECB (A4261)	KATs	CAST	On Demand	Power Cycle
AES-GCM (A4261)	KATs	CAST	On Demand	Power Cycle
Counter DRBG (A4261)	KAT	CAST	On Demand	Power Cycle
ECDSA KeyGen (FIPS186-5) (A4261)	PCT	PCT	On Demand	Power Cycle
ECDSA SigGen (FIPS186-5) (A4261)	KAT	CAST	On Demand	Power Cycle
ECDSA SigVer (FIPS186-5) (A4261)	KAT	CAST	On Demand	Power Cycle
HMAC-SHA2-384 (A4261)	KAT	CAST	On Demand	Power Cycle
KAS-ECC-SSC Sp800-56Ar3 (A4261)	KAT	CAST	On Demand	Power Cycle
KAS-FFC-SSC Sp800-56Ar3 (A4261)	KAT	CAST	On Demand	Power Cycle
KDA OneStep SP800-56Cr2 (A4261)	KAT	CAST	On Demand	Power Cycle
KDF SNMP (A4261)	KAT	CAST	On Demand	Power Cycle
KDF SSH (A4261)	KAT	CAST	On Demand	Power Cycle
RSA KeyGen (FIPS186-5) (A4261)	PCT	PCT	On Demand	Power Cycle
Safe Primes Key Generation (A4261)	PCT	PCT	On Demand	Power Cycle
SHA2-256 (A4261)	KAT	CAST	On Demand	Power Cycle
SHA2-512 (A4261)	KAT	CAST	On Demand	Power Cycle
TLS v1.2 KDF RFC7627 (A4261)	KAT	CAST	On Demand	Power Cycle
TLS v1.3 KDF (A4261)	KAT	CAST	On Demand	Power Cycle
Firmware Load Test (HMAC-SHA2-384 (A4261)	-	SW/FW Load	On Demand	Provided Service
SHA2-384 (A4261)	-	Bypass	On Demand	Provided Service
Adaptive Proportion Test (APT)	FD	CAST	On Demand & Continuous	Power Cycle
Repetition Count Test (RCT)	FD	CAST	On Demand & Continuous	Power Cycle

Table 22: Conditional Periodic Information

10.4 Error States

If any of the Pre-operational Self-Tests or Cryptographic Algorithm Self-Tests fail, the module will output an error status and enter a critical error state, where all data output is inhibited. Upon entering a critical error state, an operator can attempt to clear the critical error state by rebooting the module. If the critical error state cannot be cleared, the module must be returned to the manufacturer. The action taken upon failure of a conditional self-test is context dependent. The table below shows the different causes that lead to the Error States and the status indicators reported.

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	-	Pre-Operational, A4261 CAST, A4136 CAST or 4261 PCT fails	Attempt reboot, if reboot does not clear error return to manufacturer.	"...Self-Test FAILED"
Data Plane Critical Error	-	A2709 CAST or Conditional Bypass self-test fails	Attempt reboot, if reboot does not clear error return to manufacturer.	"...Self-Test FAILED"
Soft Error	-	RCT or APT self-test fails	Module returns to operational state once error is logged.	"...Self-Test FAILED"

Table 23: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The secure delivery of the modules is guaranteed by the trusted courier (DHL). Upon receipt of the module, the Crypto-Officer is responsible for verifying the packaging information slip and checking the delivery packaging for any irregularities (such as openings or tears). If the Crypto-Officer suspects any tampering, they should immediately contact PacketLight Networks Ltd. If the Crypto-Officer does not suspect tampering upon delivery of the module, they shall follow the steps defined in the Installation section of the PacketLight PL-4000M/PL-4000T Security Guides (shipped with the cryptographic module).

The operator shall set up the device as defined in the PacketLight PL-4000M/PL-4000T Security Guides

11.2 Administrator Guidance

The following steps are required to enable the secure operation of the Module:

- Verify that the firmware version of the module is 2.1.0.
- The default password of the Admin and Crypto shall be changed upon first use.
- All operator passwords shall be a minimum of 8 characters in length.
- The default Pre-Shared Secret for Data Plane Encryption shall be changed by Crypto prior to enabling the Data Plane Encryption Service.
- Admin shall configure firewall to only allow secure protocols.
    - Ensure HTTPS is enabled.
    - Ensure SSH/SFTP is enabled.
    - Ensure that SNMPv3 is enabled, and Authentication is not set to use “No Auth” or “No Priv”.
- Telnet shall be disabled and not be used in the Approved mode of operation.
- HTTP shall be disabled and not be used in the Approved mode of operation.
- SNMPv1 and SNMPv2 shall be disabled and not be used in the Approved mode of operation.
- RADIUS shall be disabled and not be used in the Approved mode of operation.
- TACACS+ shall be disabled and not be used in the Approved mode of operation.
- FTP shall be disabled and not be used in the Approved mode of operation.
- TFTP shall be disabled and not be used in the Approved mode of operation.
- Ensure Encryption License is installed.
- The Crypto-Officer shall be aware that performing the “Lock Encrypted Service” command will prevent the module from zeroizing SSPs.
- RSA keys shall be at least 2048-bits.
- The Crypto Officer shall ensure the Key Exchange Period for OTU4 traffic does not exceed 24 hours.
- Ensure all traffic is encapsulated in a TLS tunnel as appropriate. Ensure use of Approved algorithms for TLS:

    1.2:

    - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

    1.3:

    - TLS_AES_128_GCM_SHA256
    - TLS_AES_256_GCM_SHA384
    - Curves: P-256:P-384:P-521: ffdehe3072: ffdhe2048

- Ensure use of Approved algorithms for SSH:
    - Key Exchange Algorithms:
        - ecdh-sha2-nistp256
        - ecdh-sha2-nistp384
        - ecdh-sha2-nistp521
        - diffie-hellman-group-exchange-sha256 (use modulus size 2048 or greater)
    - Encryption Algorithms:
        - AES128-CTR
        - AES192-CTR
        - AES256-CTR
        - AES128-GCM
        - AES256-GCM
    - Mac Algorithms:
        - HMAC-SHA2-256
        - HMAC-SHA2-512

- Ensure use of Approved algorithms for SNMP:
    - Authentication Algorithms:
        - SHA-256
        - SHA-384
        - SHA-512
    - Privacy Algorithms:
        - AES-CFB128-128
        - AES-CFB128-192
        - AES-CFB128-256

11.3 Non-Administrator Guidance

12 Mitigation of Other Attacks

The module does not claim mitigation of other attacks.