

# **FIPS 140-2 Non-Proprietary Security Policy**

---

**PacketLight Networks Ltd.**

**PL-2000M, PL-2000AD and PL-2000ADS**

**Hardware version: PL-2000M, PL-2000AD, PL-2000ADS**

**Firmware version: 1.3.12d**

**Date: 02/24/2023**

## Introduction

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at: <https://csrc.nist.gov/projects/cryptographic-module-validation-program>

## About this Document

This non-proprietary Cryptographic Module Security Policy for the PacketLight Networks, Ltd. PL-2000M, PL-2000AD and PL-2000ADS provides an overview of the product and a high-level description of how it meets the overall Level 2 security requirements of FIPS 140-2.

The PacketLight Networks, Ltd. PL-2000M, PL-2000AD and PL-2000ADS may also be referred to as the “module” in this document.

## Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. PacketLight Networks, Ltd. shall have no liability for any error or damages of any kind resulting from the use of this document.

## Notices

This document may be freely reproduced and distributed in its entirety without modification.

## Table of Contents

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Introduction .....                                                       | 2  |
| Disclaimer.....                                                          | 2  |
| Notices .....                                                            | 2  |
| 1. Introduction .....                                                    | 5  |
| 1.1 Scope.....                                                           | 5  |
| 1.2 Overview .....                                                       | 5  |
| 2. Security Levels.....                                                  | 7  |
| 3. Cryptographic Module Specification.....                               | 8  |
| 3.1 Cryptographic Boundary .....                                         | 8  |
| 4. Cryptographic Module Ports and Interfaces.....                        | 9  |
| 5. Roles, Services and Authentication.....                               | 13 |
| 5.1 Roles.....                                                           | 13 |
| 5.2 Services .....                                                       | 13 |
| 5.3 Authentication .....                                                 | 14 |
| 6. Physical Security.....                                                | 15 |
| 7. Operational Environment .....                                         | 15 |
| 8. Cryptographic Algorithms and Key Management.....                      | 16 |
| 8.1 Cryptographic Algorithms .....                                       | 16 |
| 8.1.1 Allowed Algorithms.....                                            | 17 |
| 8.1.2 Non-Approved but Allowed Algorithms with No Security Claimed ..... | 17 |
| 8.1.3 Non-Approved Mode of Operation.....                                | 18 |
| 8.1.4 Non-Approved Algorithms .....                                      | 18 |
| 8.2 Cryptographic Key Management .....                                   | 18 |
| 8.3 Key Generation and Entropy.....                                      | 24 |
| 8.4 Zeroization .....                                                    | 24 |
| 9. Self-tests.....                                                       | 24 |
| 9.1 Power-On Self-Tests.....                                             | 24 |
| 9.2 Conditional Self-Tests .....                                         | 25 |
| 9.3 Critical Function Tests .....                                        | 25 |
| 10. Guidance and Secure Operation .....                                  | 26 |
| 10.1 Initialization.....                                                 | 26 |
| 10.2 Usage of AES GCM in the module .....                                | 27 |
| 11. Glossary.....                                                        | 28 |

## List of Tables

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Table 1 - Security Level .....                                           | 7  |
| Table 2 - Physical Port and Logical Interface Mapping (PL-2000M) .....   | 10 |
| Table 3 - Physical Port and Logical Interface Mapping (PL-2000AD) .....  | 11 |
| Table 4 - Physical Port and Logical Interface Mapping (PL-2000ADS) ..... | 12 |
| Table 5 - Approved Services and Role allocation .....                    | 13 |
| Table 6 – Unauthenticated Services .....                                 | 14 |
| Table 7 - Non-Approved Services.....                                     | 14 |
| Table 8 - Authentication Types .....                                     | 15 |
| Table 9 - Hardware Implementation Algorithms .....                       | 16 |
| Table 10 - Firmware Algorithm Implementation .....                       | 17 |
| Table 11 - Allowed Algorithms.....                                       | 17 |
| Table 12 - Non-Approved Algorithms .....                                 | 18 |
| Table 13 - Approved Keys and CSPs .....                                  | 20 |
| Table 14 - Approved Service to Key/CSP Mapping .....                     | 24 |
| Table 15 - Power-up Self-tests .....                                     | 25 |
| Table 16 - Conditional Self-tests .....                                  | 25 |
| Table 17 – Critical Function Tests .....                                 | 25 |
| Table 18 - Glossary of Terms.....                                        | 28 |

## List of Figures

|                                                                         |    |
|-------------------------------------------------------------------------|----|
| Figure 1 - PL-2000M.....                                                | 8  |
| Figure 2 - PL-2000AD.....                                               | 8  |
| Figure 3 - PL-2000ADS.....                                              | 8  |
| Figure 4 - Right side of PL-2000M, PL-2000AD & PL-2000ADS modules ..... | 8  |
| Figure 5 - Left Side of PL-2000M, PL-2000AD & PL-2000ADS modules .....  | 8  |
| Figure 6 - Rear of PL-2000M, PL-2000AD & PL-2000ADS modules.....        | 8  |
| Figure 7: PL-2000M Ports.....                                           | 9  |
| Figure 8: PL-2000AD Ports .....                                         | 10 |
| Figure 9: PL-2000ADS Ports .....                                        | 11 |

# 1. Introduction

## 1.1 Scope

This document describes the cryptographic module security policy for the PacketLight Networks Ltd. PL-2000M, PL-2000AD and PL-2000ADS (Hardware versions: PL-2000M, PL-2000AD, PL-2000ADS) cryptographic module with Firmware 1.3.12d (also referred to as the “module” hereafter). It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

## 1.2 Overview

The PL-2000AD, PL-2000M and the PL-2000ADS are three product variations of the PL-2000x clone. The products run the same firmware and provide the same cryptographic security services.

The PL-2000x series are a 200G multi-protocol 1U MSPP transponder/muxponder device that provides a secure transport solution for long haul (PL-2000AD), metro (PL-2000M) and short-haul (PL-2000ADS) applications.

The PL-2000M has a single 200G uplink, composed of two multiplexed 100G OTU4 signals, while the PL-2000AD and PL-2000ADS have dual 100G uplinks. The PL-2000x serve as a multi-protocol, multi-rate, high-capacity optical transport platform for various types of client services with bit rates ranging from 10G to 100G. The supported services are:

- 10GbE-LAN, 40GbE-LAN, 100GbE-LAN
- 8G FC, 16G FC, 32G FC
- OC-192, STM-64
- OTU2, OTU2e, OTU3, OTU4

The PL-2000x can be configured to work in the following system modes:

- Transponder: Provides two 100G OTN transponders for 100G client services over a 200G uplink.
- 10G Muxponder mode: Provides two 100G muxponders for aggregation of 10G client services over a 200G uplink.
- 32G FC Muxponder: Provides two 100G muxponders for aggregation of 32G client services over a 200G uplink.
- 2x40G+12x10G Muxponder: Provides two 100G muxponders for aggregation of 40G and 10G client services over a 200G uplink.
- 4x40G+4x10G Muxponder: Provides two 100G muxponders for aggregation of 40G and 10G client services over a 200G uplink.
- 100G+10x10G: Provides one 100G OTN transponder for a 100G client service and one muxponder for aggregation of 10G client services over two 100G uplinks.
- 100G+40G+6x10G: Provides one 100G OTN transponder for a 100G client service and one muxponder for aggregation of 40G and 10G client services over two 100G uplinks.
- 2x32G+14x10G: Provides muxponder aggregation of 32G and 10G client services over two 100G uplinks.

- 100G+2x32G+4x10G: Provides one 100G OTN transponder for a 100G client service and muxponder aggregation of 32G FC client services and 10G client services over two 100G uplinks.
- 10x10G (PL-2000M only): Provides muxponder for aggregation of 10G client services over 100G uplink.
- 100G (PL-2000M only): Provides 100G OTN transponder for a 100G client service over 100G uplink
- 40G+6x10G (PL-2000M only): Provides muxponder for aggregation of 40G and 10G client services over 100G uplink.
- 2x40G+2x10G (PL-2000M only): Provides muxponder for aggregation of 40G and 10G client services over 100G uplink.

The PL-2000x products provide several optional types of traffic fault protection:

- 1+1 optical fiber fault protection when an optional Optical Switch is installed (not available for PL-2000ADS)
- 1+1 service fault protection (not available for PL-2000M)
- Equipment fault protection per service port with two PL-2000x devices at each site.

The following management protocols are supported by the PL-2000x products<sup>1</sup>:

- Command Line Interface (CLI) over a serial interface or Telnet/Secure Shell (SSH) connection
- Web-based HTTP/HTTPS management
- SNMP protocol with support for SNMPv1, SNMPv2c, and SNMPv3 versions
- Remote Authentication Dial-In User Service (RADIUS) protocol for centralized remote user authentication
- Rapid Spanning Tree Protocol (RSTP) for loop prevention of management traffic
- File Transfer Protocols such as TFTP and SFTP for file transfer of system software, Log files, and Configuration files.
- Simple Network Time Protocol (SNTP) for network calendar timing
- Syslog protocol for monitoring device events by a remote server
- Virtual chassis configuration, using a single IP address for multiple nodes

The module supports the following Operations, Administration, and Maintenance (OAM) functions over management interfaces:

- Optical parameters monitoring
- Alarm and Event fault management
- Layer 1 and Layer 2 Performance monitoring (PM)
- Terminal loopback and Facility loopback for optical data ports
- Diagnostic Pseudo Random Binary Sequence (PRBS) for the optical data ports<sup>2</sup>
- Environmental (External) Alarms

---

<sup>1</sup> Plaintext protocols shall not be used. Please see Section 10 in this document for instructions on the secure configuration and operation of the module.

<sup>2</sup> Not utilized for any cryptographic functionality

## 2. Security Levels

The following table lists the level of validation for each area in FIPS 140-2:

| FIPS 140-2 Section Title                                     | Validation Level |
|--------------------------------------------------------------|------------------|
| Cryptographic Module Specification                           | 2                |
| Cryptographic Module Ports and Interfaces                    | 2                |
| Roles, Services, and Authentication                          | 2                |
| Finite State Model                                           | 2                |
| Physical Security                                            | 2                |
| Operational Environment                                      | N/A              |
| Cryptographic Key Management                                 | 2                |
| Electromagnetic Interference / Electromagnetic Compatibility | 2                |
| Self-Tests                                                   | 2                |
| Design Assurance                                             | 2                |
| Mitigation of Other Attacks                                  | N/A              |
| Overall Level                                                | 2                |

*Table 1 - Security Level*

### 3. Cryptographic Module Specification

#### 3.1 Cryptographic Boundary

The cryptographic boundary is classified as a multi-chip standalone device and is the entire boundary of the chassis as pictured below.



Figure 1 - PL-2000M



Figure 2 - PL-2000AD



Figure 3 - PL-2000ADS



Figure 4 - Right side of PL-2000M, PL-2000AD & PL-2000ADS modules<sup>3</sup>



Figure 5 - Left Side of PL-2000M, PL-2000AD & PL-2000ADS modules



Figure 6 - Rear of PL-2000M, PL-2000AD & PL-2000ADS modules

<sup>3</sup> The sides (right, left & rear) of the PL-2000M, PL-2000AD & PL-2000ADS are identical and all have similar surface topography.



## 4. Cryptographic Module Ports and Interfaces

The module provides the following number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The logical interfaces and their mapping are described in the following table:

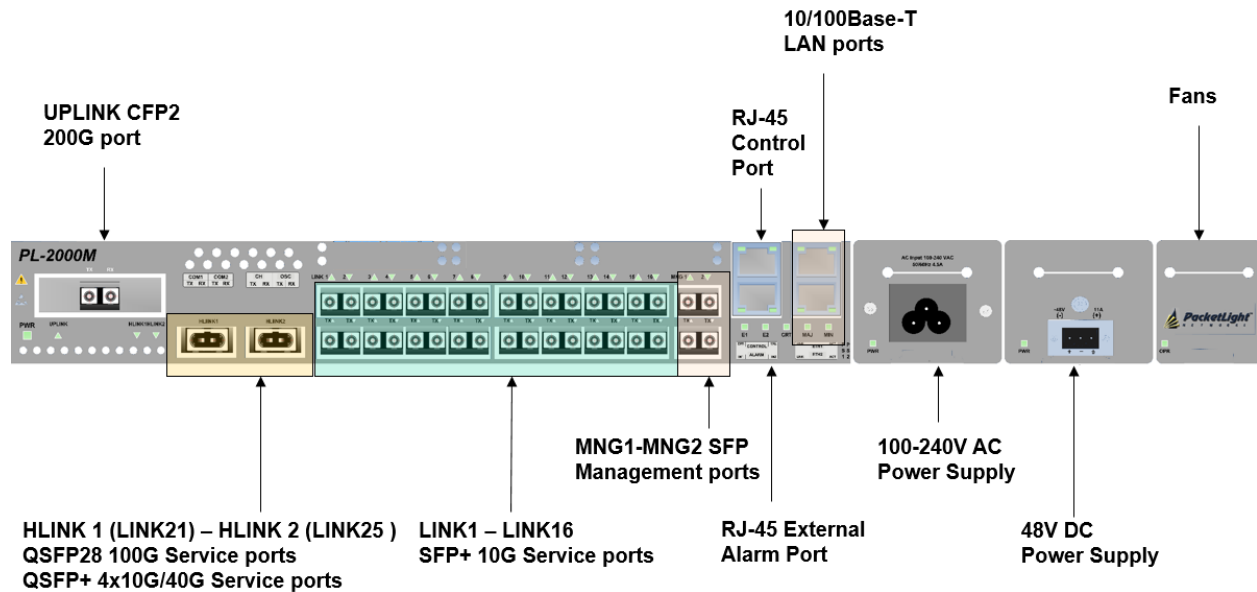


Figure 7: PL-2000M Ports

| Physical Port                               | Qty. | FIPS 140-2 Logical Interface Mapping               |
|---------------------------------------------|------|----------------------------------------------------|
| CFP2 200G port (uplink)                     | 1    | Data Input, Data Output, Control Input, Status out |
| RJ-45 Control Port                          | 1    | Control Input, Status out                          |
| 10/100 Base-T LAN Ports                     | 2    | Data Input, Data Output, Control Input, Status out |
| QSFP28 100G / QSFP+ 40G/4x10G Service ports | 2    | Data Input, Data Output, Control Input, Status out |
| SFP+ 10G Service ports                      | 16   | Data Input, Data Output, Control Input, Status out |
| SFP Management ports                        | 2    | Data Input, Data Output, Control Input, Status out |
| RJ-45 External Alarm port                   | 1    | Control Input, Status Output                       |
| 100-240V AC                                 | 1    | Power Input                                        |
| 48V DC Power Supply (Optional)              | 1    | Power                                              |

|                       |                                                                                            |               |
|-----------------------|--------------------------------------------------------------------------------------------|---------------|
| Fan Module (Optional) | 1                                                                                          | N/A           |
| Status LEDs           | Power: 1<br>Uplink: 1<br>Clients: 18<br>MNG: 2<br>System: 5<br>PS: 2<br>Fan: 1<br>Total=30 | Status Output |

Table 2 - Physical Port and Logical Interface Mapping (PL-2000M)

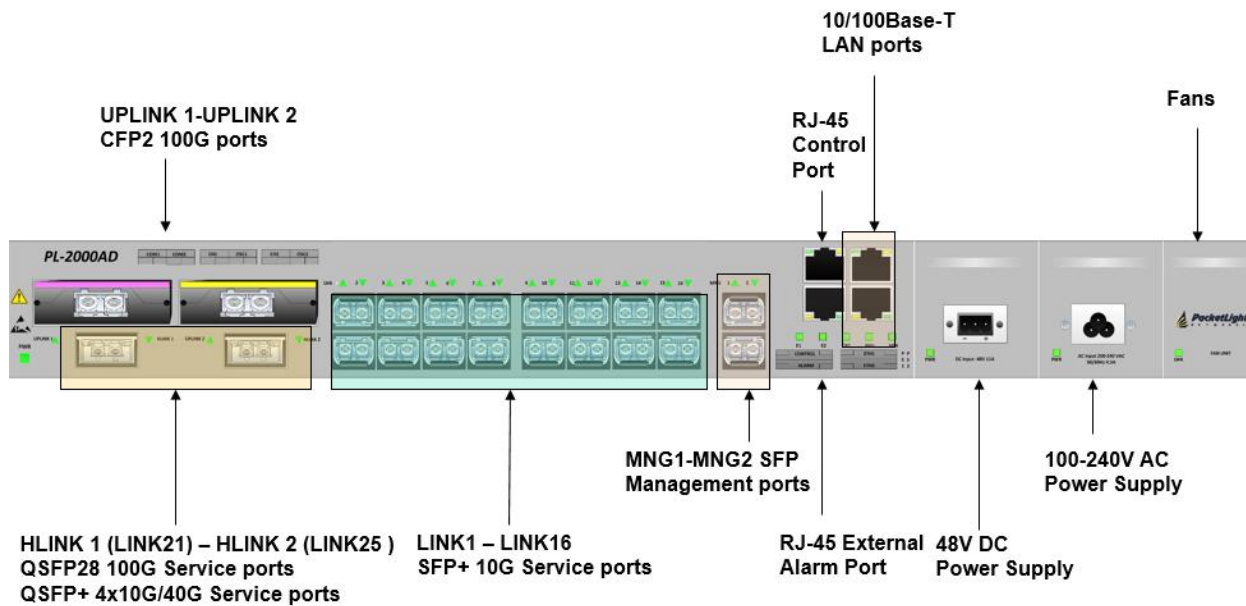


Figure 8: PL-2000AD Ports

| Physical Port                               | Qty. | FIPS 140-2 Logical Interface Mapping               |
|---------------------------------------------|------|----------------------------------------------------|
| CFP2 100G ports (uplink)                    | 2    | Data Input, Data Output, Control Input, Status out |
| RJ-45 Control Port                          | 1    | Control Input, Status out                          |
| 10/100 Base-T LAN Ports                     | 2    | Data Input, Data Output, Control Input, Status out |
| QSFP28 100G / QSFP+ 40G/4x10G Service ports | 2    | Data Input, Data Output, Control Input, Status out |
| SFP+ 10G Service ports                      | 16   | Data Input, Data Output, Control Input, Status out |

|                                     |                                                                                            |                                                    |
|-------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------|
| SFP Management ports                | 2                                                                                          | Data Input, Data Output, Control Input, Status out |
| RJ-45 External Alarm port           | 1                                                                                          | Control Input, Status Output                       |
| 48V DC Power Supply                 | 1                                                                                          | Power                                              |
| 100-240V AC Power Supply (Optional) | 1                                                                                          | Power                                              |
| Fan Module (Optional)               | 1                                                                                          | N/A                                                |
| Status LEDs                         | Power: 1<br>Uplink: 1<br>Clients: 18<br>MNG: 2<br>System: 5<br>PS: 2<br>Fan: 1<br>Total=30 | Status Output                                      |

Table 3 - Physical Port and Logical Interface Mapping (PL-2000AD)

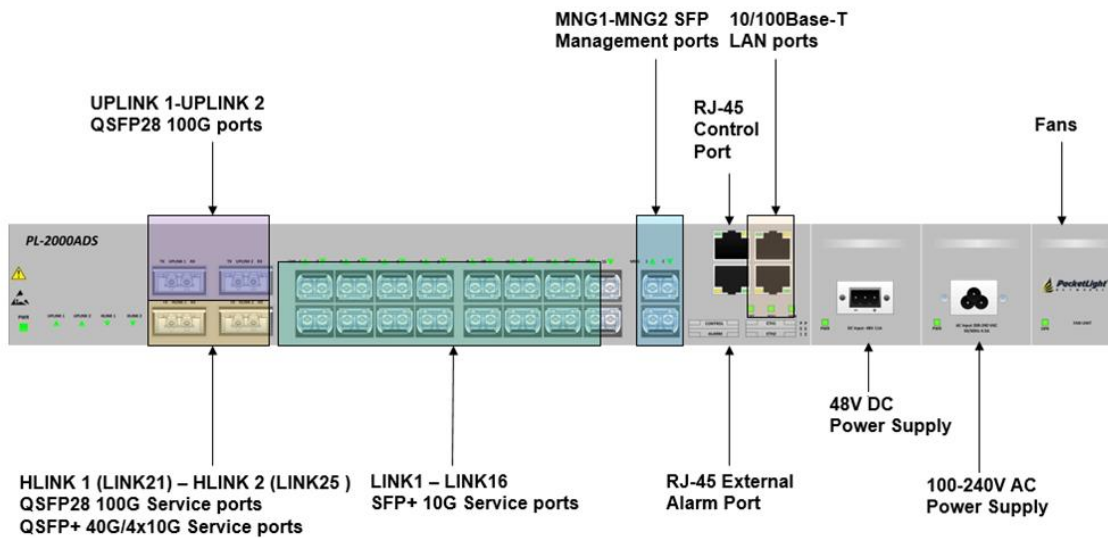


Figure 9: PL-2000ADS Ports

| Physical Port                               | Qty.                                                                                       | FIPS 140-2 Logical Interface Mapping               |
|---------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------|
| QSFP28 100G ports (uplink)                  | 2                                                                                          | Data Input, Data Output, Control Input, Status out |
| RJ-45 Control Port                          | 1                                                                                          | Control Input, Status out                          |
| 10/100 Base-T LAN Ports                     | 2                                                                                          | Data Input, Data Output, Control Input, Status out |
| QSFP28 100G / QSFP+ 40G/4x10G Service ports | 2                                                                                          | Data Input, Data Output, Control Input, Status out |
| SFP+ 10G Service ports                      | 16                                                                                         | Data Input, Data Output, Control Input, Status out |
| SFP Management ports                        | 2                                                                                          | Data Input, Data Output, Control Input, Status out |
| RJ-45 External Alarm port                   | 1                                                                                          | Control Input, Status Output                       |
| 100-240V AC Power Supply                    | 1                                                                                          | Power                                              |
| 48V DC Power Supply (Optional)              | 1                                                                                          | Power                                              |
| Fan Module (Optional)                       | 1                                                                                          | N/A                                                |
| Status LEDs                                 | Power: 1<br>Uplink: 1<br>Clients: 18<br>MNG: 2<br>System: 3<br>PS: 2<br>Fan: 1<br>Total=28 | Status Output                                      |

Table 4 - Physical Port and Logical Interface Mapping (PL-2000ADS)

#### Management Interfaces:

- RJ-45 Control port
- Two 10M/100M LAN ports
- Two Remote or local management by two 100/1000M management channels based on pluggable (SFP) optics for out-of-band Optical Supervisory Channels (OSCs)
- Remote management via in-band channels embedded in the OTN uplink signals

## 5. Roles, Services and Authentication

### 5.1 Roles

The module supports five different roles, Super-User, Administrator (Admin), Crypto-Officer (CO), Read-Write and Read-Only.

There are 21 unique Crypto-Officer users. Each service port on the module can be assigned a different CO user.

Admin user can access and edit permissions for all functions such as adding and deleting users, changing access levels and resetting/changing passwords. Admin user cannot manage the Super-User or the CO users.

The Crypto-Officer user can manage their own password. The assigned CO user has access to the “Encryption tab” on the WebGUI where they may enter pre-shared-secret information, change the locking of encrypted service, and set the Key Exchange Period for the encryption service for the associated service port.

The Read-Write role can view and manage the module and can manage its own password.

The Read Only User is restricted to only viewing the status of the module and does not have any edit permissions except to change its own password. Both the Read-Write User and Read Only User have no access to any cryptographic functions.

### 5.2 Services

The module provides the following Approved services which utilize algorithms listed in Table 9 and 10:

| Service                                             | Super-User Role | Read-Write Role | Read Only Role | Crypto Officer Role | Admin Role |
|-----------------------------------------------------|-----------------|-----------------|----------------|---------------------|------------|
| Initialization                                      |                 | X               |                |                     | X          |
| Manage Accounts                                     |                 |                 |                |                     | X          |
| Change Password                                     | X               | X               | X              | X                   | X          |
| Encryption Service                                  | X               |                 |                | X                   |            |
| Add/Change Pre-Shared Secret                        | X               |                 |                | X                   |            |
| Lock Encrypted Service <sup>4</sup>                 | X               |                 |                | X                   |            |
| Change Provisioning Type                            | X               | X               |                |                     | X          |
| View Performance Monitoring                         | X               | X               | X              | X                   | X          |
| View Faults or Alarms                               | X               | X               | X              | X                   | X          |
| Configure Firewall                                  | X               | X               | X              | X                   | X          |
| Request Status Information                          | X               | X               | X              | X                   | X          |
| Set Configuration data                              | X               | X               |                |                     | X          |
| Export Backup of Configuration file over HTTPS/SFTP | X               |                 |                |                     | X          |
| View Network Topology                               | X               | X               | X              | X                   | X          |
| On-Demand Self-test                                 | X               | X               | X              | X                   | X          |
| Zeroization/Factory Reset                           | X               |                 |                |                     | X          |
| Firmware Update                                     | X               | X               |                |                     | X          |

Table 5 - Approved Services and Role allocation

<sup>4</sup> The Lock Encrypted Service will prevent changing service type, firmware update and Zeroization/Factory Reset

The below table provides a full description of the unauthenticated services provided by the module:

| Unauthenticated Services |
|--------------------------|
| Request Authentication   |
| On-Demand Self-test      |

Table 6 – Unauthenticated Services

The module provides the following non-Approved services which utilize algorithms listed in Table 12:

| Service                      |
|------------------------------|
| Non-Conformant Key Agreement |

Table 7 - Non-Approved Services

Services listed in Table 7 make use of non-compliant cryptographic algorithms. Use of these algorithms are prohibited in a FIPS-approved mode of operation.

### 5.3 Authentication

The module supports role-based authentication. Users must authenticate using a user ID and password, SSH client key (SSH only), or certificates associated with the correct protocol in order to set up the secure session. Secure sessions that authenticate Users have no interface available to access other services (such as Crypto Officer services). Each User SSH session remains active (logged in) and secured until the operator logs out or inactivity for a configurable amount of time has elapsed. Each User Management Console session remains active until the operator logs out or inactivity for a configurable amount of time has elapsed.

| Type of Authentication     | Authentication Strength                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WebGUI (HTTPS)<br>Password | <p>Passwords are required to be at minimum 8 characters in length, and at maximum 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1:(95<sup>8</sup>), or 1:6,634,204,312,890,625 chance of false acceptance. The Crypto-Officer may connect locally using the serial port or remotely after establishing a HTTPS session.</p> <p>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 600/95<sup>8</sup>, which is less than 1/100,000.</p> |
| SSH/SFTP<br>Password       | <p>Passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95<sup>8</sup>), or 1:6,634,204,312,890,625 chance of false acceptance.</p> <p>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 600/95<sup>8</sup>, which is less than 1/100,000.</p>                                                                                                                |

| Type of Authentication | Authentication Strength                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Console Password       | <p>For password authentication done by the modules, passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95<sup>8</sup>), or 1:6,634,204,312,890,625 chance of false acceptance.</p> <p>The fastest data rate for the serial port is 9,600 bps. Each ASCII character is 10 bits (1 Start, 8 data, 1 Stop), so that is (9600 / 10 =) 960 characters per second or (960 * 60 =) 57,600 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 greatly exceeds the 57,600 limit imposed by the data rate of the serial port. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute to be less than 1:100,000 as required by FIPS 140-2.</p> |
| Public keys            | <p>A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is 1/2<sup>112</sup>, which is less than 1/1,000,000.</p> <p>The module supports RSA certificates for authentication of roles during TLS, HTTPS or SSH/SFTP. Using conservative estimates and equating a 2048-bit RSA key to 112-bits of strength, the probability for a random attempt to succeed during a one-minute period is 1:2<sup>112</sup> or 1: 5.19 x 10<sup>33</sup>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SNMPv3 Passwords       | <p>Passwords are required to be at least 8 characters in length and maximum of 64 bytes (number of characters is dependent on the character set used by system). An 8-character password allowing all printable American Standard Code for Information Interchange (ASCII) characters (95) with repetition equates to a 1: (95<sup>8</sup>), or 1:6,634,204,312,890,625 chance of false acceptance.</p> <p>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 600/95<sup>8</sup>, which is less than 1/100,000.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 8 - Authentication Types

## 6. Physical Security

The module is a multi-chip standalone cryptographic module made with production grade components and standard passivation. The cover of all the modules are sealed with two tamper-evident seals, applied during manufacturing. The physical security of the module is intact if there is no evidence of tampering with the seal. The locations of the tamper-evident seals are indicated by the red rectangles in Figures 1 through 4<sup>5</sup>.

## 7. Operational Environment

The module's operational environment is considered a limited operational environment under FIPS 140-2.

<sup>5</sup> Depicted on Page 8 of this document.

## 8. Cryptographic Algorithms and Key Management

### 8.1 Cryptographic Algorithms

The module implements the following approved algorithms in the firmware and hardware:

| Hardware Algorithm Implementation |           |          |                                      |               |                                        |
|-----------------------------------|-----------|----------|--------------------------------------|---------------|----------------------------------------|
| CAVP Cert #                       | Algorithm | Sizes    | Standard                             | Mode/Method   | Use                                    |
| C221                              | AES       | 256-bits | SP 800-38A<br>FIPS 197<br>SP 800-38D | ECB, GCM, CTR | Encryption, Decryption, Authentication |
|                                   | KTS       | 256-bits | IG D.9                               | KTS (AES GCM) | Key Transport                          |

Table 9 - Hardware Implementation Algorithms

| Firmware Algorithm Implementation      |                  |                                  |                                      |                                    |                                                                                                      |
|----------------------------------------|------------------|----------------------------------|--------------------------------------|------------------------------------|------------------------------------------------------------------------------------------------------|
| CAVP Cert #                            | Algorithm        | Sizes                            | Standard                             | Mode/Method                        | Use                                                                                                  |
| C416                                   | AES              | 128, 192, 256-bits               | SP 800-38A<br>FIPS 197<br>SP 800-38D | CBC, CFB, ECB, GCM, CTR            | Encryption, Decryption, Authentication                                                               |
| Vendor Affirmed                        | CKG              | N/A                              | SP 800-133                           | N/A                                | Key Generation                                                                                       |
| C416                                   | CVL <sup>6</sup> | SHA-1, SHA-256, SHA-384, SHA-512 | SP 800-135                           | TLS <sup>7</sup> , SSH, SNMPv3 KDF | Key Derivation                                                                                       |
| C416                                   | CVL              | Partial Public Key Validation    | SP 800-56A                           | ECC CDH Component Testing          | Key Agreement                                                                                        |
| C416                                   | KTS              | 128, 192, 256-bits               | IG D.9                               | KTS (AES GCM)                      | Key Transport key establishment methodology provides between 128 and 256 bits of encryption strength |
| C416                                   | DRBG             | 256-bits                         | SP 800-90Arev1                       | AES CTR_DRBG                       | Random Bit Generation                                                                                |
| C416                                   | HMAC             | 160, 256, 384, 512-bits          | FIPS PUB 198                         | SHA-1, SHA-256, SHA-384, SHA-512   | Message Authentication                                                                               |
| KAS-SSC Cert. #A3304, KDA Cert. #A3304 | KAS              | ECC: P-256, P-384, P-521         | SP 800-56Arev3                       | Ephemeral Unified                  | Key Agreement                                                                                        |
|                                        |                  | KDA: SHA-384                     | SP 800-56Crev2                       | One Step KDA                       |                                                                                                      |

<sup>6</sup> No parts of the TLS, SSH or SNMP protocol, other than the KDF, have been tested by the CAVP and CMVP per FIPS 140-2 IG D.11.

<sup>7</sup> Note: TLS only supports SHA-256 and SHA-384



|                                       |                  |                                             |                              |                                                                                                                                                                                                                    |                                                                                                                                                                                                    |
|---------------------------------------|------------------|---------------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| KAS-SSC Cert. #A3304, CVL Cert. #C416 | KAS              | FFC: FB, FC<br>KDF: SHA-1, -256, -384, -512 | SP 800-56Arev3<br>SP 800-135 | dhEphem<br>TLS KDF, SSH KDF                                                                                                                                                                                        | Key Agreement                                                                                                                                                                                      |
| A3304                                 | KAS-SSC          | ECC: P-256, P-384, P-521<br><br>FFC: FB, FC | SP 800-56Arev3               | Ephemeral Unified<br><br>dhEphem                                                                                                                                                                                   | Key Agreement; Key establishment methodology provides between 128 and 256 bits of encryption strength<br><br>Key Agreement; Key establishment methodology provides 112 bits of encryption strength |
| A3304                                 | KDA              | SHA-384                                     | SP 800-56Crev2               | One Step KDA                                                                                                                                                                                                       | Key Derivation                                                                                                                                                                                     |
| A3304                                 | DSA <sup>8</sup> | (2048, 224), (2048, 256), (3072, 256)       | FIPS 186-4                   | KeyGen                                                                                                                                                                                                             | Key Generation                                                                                                                                                                                     |
| C416                                  | SHS              | SHA-1, SHA-256, SHA-384, SHA-512            | FIPS PUB 180-4               | SHA-1, SHA-256, SHA-384, SHA-512                                                                                                                                                                                   | Message Digest Generation                                                                                                                                                                          |
| C416                                  | RSA              | 2048, 3072 (Key Generation Only)            | FIPS PUB 186-4               | Key Generation, Signature Generation <sup>9.31</sup> , Signature Verification <sup>9.31</sup> , Signature Generation PKCS1.5, Signature Verification PKCS1.5, Signature Generation PSS, Signature Verification PSS | Key Generation, Signature Generation, Signature Verification                                                                                                                                       |

Table 10 - Firmware Algorithm Implementation

Note: Not all algorithms/modes tested on the CAVP validation certificates are implemented in the module.

### 8.1.1 Allowed Algorithms

The module implements the following allowed cryptographic algorithms:

| Algorithm | Use                       |
|-----------|---------------------------|
| NDRNG     | To seed the Approved DRBG |

Table 11 - Allowed Algorithms

### 8.1.2 Non-Approved but Allowed Algorithms with No Security Claimed

The module supports the following non-Approved but allowed algorithms with no security claimed:

- 256-bit AES CTR (no security claimed) is used to obfuscate a configuration file while stored on the module<sup>9</sup>.

<sup>8</sup> CAVP tested as a pre-requisite for KAS-SSC-FFC only. Not used by the module.

<sup>9</sup> The configuration file can only be exported or imported over HTTPS or SFTP.

The operator shall consult FIPS 140-2 IG 1.23 for further understanding of the use of functions where no security is claimed.

### 8.1.3 Non-Approved Mode of Operation

The Crypto Officer is responsible for configuration of the module. When configured according to Section 10 in this Security Policy, the modules only support the non-Approved services listed in Table 7. The non-Approved algorithms or plaintext protocols in Section 10 are disabled.

### 8.1.4 Non-Approved Algorithms

The module implements the following algorithms which are considered non-Approved:

| Algorithm      | Use                                                     |
|----------------|---------------------------------------------------------|
| Diffie-Hellman | Key Agreement less than 112 bits of encryption strength |

Table 12 - Non-Approved Algorithms

## 8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 13:

| Keys and CSPs                  | Description                                                                          | Key/CSP Type                                                           | Generation /Input                                                                                                                                                                      | Output Method                                         | Storage                             | Zeroization                                 |
|--------------------------------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-------------------------------------|---------------------------------------------|
| Operator Passwords             | Authentication for the Admin, Crypto-Officers, Read-Write Users and Read Only Users  | Minimum of 8 (64 bits) and maximum of 20 bytes (160 bits) string value | Externally generated. Enters the module in encrypted form via a secure TLS or SSH/SFTP session.<br><br>Enters the module in plaintext via a directly attached cable to the serial port | Exits encapsulated (SSH/SFTP) in configuration backup | Hashed in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| EC DH Key Pair for DEK         | Key pair used in NIST SP 800-56Arev3 (Section 5.7.1.2) ECC CDH Primitive computation | EC DH private component 384-bits<br><br>EC DH public key (P-384)       | Generated internally using the SP 800-90A CTR_DRBG<br><br>Public key of a peer enters the module in plaintext                                                                          | Private never exits the module                        | Plaintext in volatile memory        | Session termination or power cycle          |
| ECC CDH primitive for DEK      | Shared Secret (Z) value that will be used to derive the DEK                          | 384-bit string                                                         | Computed per SP 800-56Arev3 (Section 5.7.1.2)                                                                                                                                          | Never exits the module                                | Plaintext in volatile memory        | Session termination or power cycle          |
| Data Encryption Key (DEK)      | Used for encrypting or decrypting payload data                                       | AES-GCM 256 bit                                                        | Derived per NIST SP 800-56Crev2 (Section 4.1)                                                                                                                                          | Never exits the module                                | Plaintext in volatile memory        | Power Cycle                                 |
| Peer-Authentication Pre-Shared | Entered by Crypto-Officer. Parameter                                                 | 384-bit string                                                         | Externally generated. Enters the module in                                                                                                                                             | Exits encapsulated (SSH/SFTP) in                      | Encrypted in non-volatile           | Invoke Factory Reset or Zeroization         |

| Keys and CSPs                                 | Description                                      | Key/CSP Type                                                                            | Generation /Input                                                                                             | Output Method                                         | Storage                                | Zeroization                                 |
|-----------------------------------------------|--------------------------------------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------------------------|---------------------------------------------|
| Secret                                        | used for Peer-Authentication during key exchange |                                                                                         | encrypted form via HTTPS                                                                                      | configuration backup                                  | Flash memory                           | command                                     |
| Diffie-Hellman (DH) Key Pair                  | Negotiating TLS/HTTPS or SSH/SFTP sessions       | Diffie-Hellman private component<br>160 – 512 bits<br><br>Public component<br>2048 bits | Generated internally using the SP 800-90A CTR_DRBG<br><br>Public key of a peer enters the module in plaintext | Private never exits the module                        | Plaintext in volatile memory           | Session termination or power cycle          |
| Elliptic Curve Diffie-Hellman (ECDH) Key Pair | Negotiating TLS/HTTPS or SSH/SFTP sessions       | EC DH private component<br>384-bits<br><br>EC DH public key (P-256, P-384 and P-521)    | Generated internally using the SP 800-90A CTR_DRBG<br><br>Public key of a peer enters the module in plaintext | Private never exits the module                        | Plaintext in volatile memory           | Session termination or power cycle          |
| SNMP Privacy Key                              | Encryption / decryption of SNMP session traffic  | AES CFB 128, 192, 256-bit                                                               | Derived using SP 800-135 Key derivation (SNMP)                                                                | Exits encapsulated (SSH/SFTP) in configuration backup | Encrypted in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| SNMP Authentication Key                       | Message authentication and verification in SNMP  | HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512                                 | Derived using SP 800-135 Key derivation (SNMP)                                                                | Exits encapsulated (SSH/SFTP) in configuration backup | Encrypted in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| SNMPv3 Password                               | Password                                         | Minimum of 8 (64 bits) and maximum of 20 bytes (160 bits) string value                  | Externally generated. Enters the module in encrypted form via a secure TLS or SSH session.                    | Exits encapsulated (SSH/SFTP) in configuration backup | Plaintext in non-volatile Flash memory | Invoke Factory Reset or Zeroization command |
| SSH/SFTP Host Key Pair                        | Key Pair used for SSH/SFTP authentication        | RSA 2048-bit                                                                            | Internally generated via FIPS-Approved DRBG upon first system power-up                                        | Private never exits the module                        | Plaintext in non-volatile Flash memory | Zeroization command                         |
| Premaster Secret                              | Establish the TLS Master Secret                  | 384-bit string                                                                          | Generated internally with the SP 800-90A CTR_DRBG<br><br>Input during TLS negotiation                         | Exits in encrypted form during protocol handshake     | Plaintext in volatile memory           | Session termination or power cycle          |

| Keys and CSPs                       | Description                                 | Key/CSP Type                                   | Generation /Input                                    | Output Method                                     | Storage                      | Zeroization                        |
|-------------------------------------|---------------------------------------------|------------------------------------------------|------------------------------------------------------|---------------------------------------------------|------------------------------|------------------------------------|
| TLS Master Secret                   | Establish the TLS Session Key               | 384-bit string                                 | Derived <sup>10</sup> from the TLS Pre-Master Secret | Never exits the module                            | Plaintext in volatile memory | Session termination or power cycle |
| TLS Session Key                     | Used for encrypting/decrypting TLS messages | AES CBC, CTR, or GCM 128 or 256-bit key        | Generated internally during session negotiation      | Exits in encrypted form during protocol handshake | Plaintext in volatile memory | Session termination or power cycle |
| TLS Authentication Key              | Used for authenticating TLS messages        | HMAC SHA-1-, 256-, 384- or 512-bit key         | Generated internally during session negotiation      | Never exits the module                            | Plaintext in volatile memory | Session termination or power cycle |
| SSH/SFTP Session Encryption Key     | Used for Encrypting SSH/SFTP messages       | AES CBC, CTR, or GCM 128-, 192, or 256-bit key | Internally generated via FIPS-Approved DRBG          | Exits in encrypted form during protocol handshake | Plaintext in volatile memory | Session termination or power cycle |
| SSH/SFTP Session Authentication key | Data authentication for SSH/SFTP sessions   | HMAC SHA-1-, 256-, 384- or 512-bit key         | Derived via in SP800-135 KDF (SSH)                   | Never exits the module                            | Plaintext in volatile memory | Session termination or power cycle |
| SP 800-90A CTR_DRBG Seed            | Seeding material for the SP800-90A CTR_DRBG | 384-bit value                                  | Internally generated by the NDRNG                    | Never exits the module                            | Plaintext in volatile memory | Power cycle                        |
| SP 800-90A CTR_DRBG Nonce           | Entropy material for the SP800-90A CTR_DRBG | 128-bit value                                  | Internally generated by the NDRNG                    | Never exits the module                            | Plaintext in volatile memory | Power cycle                        |
| SP 800-90A CTR_DRBG key value       | Used for the SP 800-90A CTR_DRBG            | Internal state value                           | Internally generated                                 | Never exits the module                            | Plaintext in volatile memory | Power cycle                        |
| SP 800-90A CTR_DRBG V value         | Used for the SP 800-90A CTR_DRBG            | Internal state value                           | Internally generated                                 | Never exits the module                            | Plaintext in volatile memory | Power cycle                        |

Table 13 - Approved Keys and CSPs

<sup>10</sup> Derived via NIST SP 800-135 TLS 1.2 KDF

The module implements the following access control policy on keys and CSPs in the module shown in the following table. The Access Policy is noted by R=Read, W=Write and X=Execute.

| Module Service     | CSP Access                                                                                                                                                                                                                                                                                                                                                      | Rights (R/W/X) |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| Initialization     | Diffie-Hellman (DH) Key Pair, Elliptic Curve Diffie-Hellman (ECDH) Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key, SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication Key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X          |
| Manage Accounts    | Operator Passwords                                                                                                                                                                                                                                                                                                                                              | R/W/X          |
|                    | DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value                                                  | R/W/X          |
| Change Password    | Operator Passwords                                                                                                                                                                                                                                                                                                                                              | R/W/X          |
|                    | DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value                                                  | R/W/X          |
| Encryption Service | EC DH Key Pair for DEK; ECC CDH primitive for DEK; DEK; Peer-Authentication Pre-Shared Secret; SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value                                                                                                                                                           | R/W/X          |
|                    | DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A                                                                                                                    | R/W/X          |

|                              |                                                                                                                                                                                                                                                                                                                                                                            |       |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                              | CTR_DRBG Nonce, SP 800-90A<br>CTR_DRBG key value, SP 800-90A V<br>value                                                                                                                                                                                                                                                                                                    |       |
| Add/Change Pre-Shared Secret | Peer-Authentication Pre-Shared Secret                                                                                                                                                                                                                                                                                                                                      | R/W   |
|                              | DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value                                                             | R/W/X |
| Lock Encrypted Service       | DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value                                                             | R/W/X |
| View Performance Monitoring  | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Password, DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| View Faults or Alarms        | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Password, DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Configure Firewall           | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Password; DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret,                                                                                                                                                                                                                                               | R/W/X |

|                            |                                                                                                                                                                                                                                                                                                                                                                            |       |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
|                            | TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value                                                                                                                              |       |
| Request Status Information | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Password; DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| Set Configuration data     | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Password; DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| View Network Topology      | SNMP Privacy Key, SNMP Authentication Key, SNMPv3 Password; DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key; SSH/SFTP Host Key Pair, SSH/SFTP Session Encryption Key, SSH/SFTP Session Authentication key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V value | R/W/X |
| On-Demand Self-test        | N/A                                                                                                                                                                                                                                                                                                                                                                        | N/A   |
| Zeroization/Factory Reset  | All CSPs                                                                                                                                                                                                                                                                                                                                                                   | R/W/X |
| Firmware Update            | DH Key Pair, ECDH Key Pair, Premaster Secret, TLS Master Secret, TLS Session Key, TLS Authentication Key, SP 800-90A CTR_DRBG Seed, SP 800-90A CTR_DRBG Nonce, SP 800-90A CTR_DRBG key value, SP 800-90A V                                                                                                                                                                 | R/W/X |

|  |       |  |
|--|-------|--|
|  | value |  |
|--|-------|--|

Table 14 - Approved Service to Key/CSP Mapping

### 8.3 Key Generation and Entropy

The module is a hardware module with an entropy-generating NDRNG inside the module’s cryptographic boundary consistent with Scenario 1 (a) described in FIPS 140-2 IG 7.14. The module performs a CRNGT on the entropy input it receives. The module’s firmware requests 512-bits from the entropy buffer (which is filled by the NDRNG). The firmware will use 384 bits as seed for the Approved CTR\_DRBG. Therefore, the 384-bits used to seed the DRBG will contain ~307-bits of actual entropy which is more than 256-bits of entropy required for the CTR\_DRBG, per NIST SP 800-90A.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (vendor affirmed). The resulting generated symmetric keys are the unmodified output from the SP 800-90A DRBG.

### 8.4 Zeroization

Ephemeral secret keys are zeroized either at session termination or by power-cycling the module. Persistently stored CSPs can also be zeroized by issuing a factory reset. This changes all values back to zero or the default values.

In the case SSH/SFTP Host Key Pair, the zeroization command must be invoked by the Admin role at the CLI.

If the module transitions from the non-Approved to the Approved mode or vice versa, the module shall be zeroized prior to switching modes.

The output data path is provided by the data interfaces and is logically disconnected from processes performing key generation or zeroization. No key information will be output through the data output interface when the module zeroizes keys.

## 9. Self-tests

FIPS 140-2 requires the module to perform self-tests to ensure the module integrity and the correctness of the cryptographic functionality at start-up. Some functions require conditional tests during normal operation of the module.

If any of the tests fail, the module will return an error code and transition to an error state where no functions can be executed. An operator can attempt to reset the state by cycling the power. However, the failure of a self-test may require the module to be replaced.

### 9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run. If any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the operator.

The module implements the following power-on self-tests:

| Type           | Test Description                                                                                                |
|----------------|-----------------------------------------------------------------------------------------------------------------|
| Integrity Test | <ul style="list-style-type: none"> <li>HMAC-SHA-384 keyed hash integrity test on the module firmware</li> </ul> |



|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Known Answer Tests | <ul style="list-style-type: none"> <li>● Hardware AES ECB KAT (Encryption and Decryption. Size 256)</li> <li>● Hardware AES GCM KAT (Encryption and Decryption. Size 256)</li> <li>● Firmware SHS KAT (SHA-1, SHA-256, SHA-384 and SHA-512)</li> <li>● Firmware HMAC KAT (HMAC-SHA-384)</li> <li>● Firmware AES ECB KAT (Encryption and Decryption. Size 256)</li> <li>● Firmware AES GCM KAT (Encryption and Decryption. Size 256)</li> <li>● Firmware SP 800-90A CTR_DRBG KAT</li> <li>● Firmware RSA (Sign and Verify. Size 2048)</li> <li>● Firmware Diffie-Hellman Primitive "Z" Computation KAT (56Aev3)</li> <li>● Firmware EC Diffie-Hellman Primitive "Z" Computation KAT (56Aev3)</li> <li>● Firmware One-step KDF KAT (56Crev2)</li> <li>● Firmware SSH KDF KAT (SP 800-135)</li> <li>● Firmware TLS KDF KAT (SP 800-135)</li> <li>● Firmware SNMP KDF KAT (SP 800-135)</li> </ul> |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Table 15 - Power-up Self-tests

The module performs all power-on self-tests automatically when it is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation. Should any of the above tests fail, the device enters an error state. In an error state no traffic is allowed In/Out of the device.

## 9.2 Conditional Self-Tests

Conditional self-tests are tests that run during operation of the module. Each module performs the following conditional self-tests:

| Type                      | Test Description                                                                  |
|---------------------------|-----------------------------------------------------------------------------------|
| CRNGT on NDRNG            | Continuous RNG test (CRNGT) performed on entropy input from the TRNG              |
| CRNGT on the DRBG         | Continuous RNG test (CRNGT) for the SP800-90A DRBG                                |
| DRBG Health Tests         | Performed on DRBG, per SP 800-90A Section 11.3. Required per IG W.3.              |
| Pairwise Consistency Test | RSA Key Generation                                                                |
| Bypass Test               | SHA-384 hash on service table                                                     |
| Firmware Load Test        | HMAC-SHA-384 based integrity test to verify firmware to be loaded into the module |

Table 16 - Conditional Self-tests

## 9.3 Critical Function Tests

The module implements the following critical function tests which execute at start-up or during operation of the module.

| Type                        | Test Description                                                                                |
|-----------------------------|-------------------------------------------------------------------------------------------------|
| Hardware TRNG Health checks | The hardware-based entropy source performs health checking functions prior to providing output. |
| DRBG Health Tests           | Performed on DRBG, per SP 800-90A Section 11.3. Required per IG W.3.                            |

Table 17 – Critical Function Tests

## 10. Guidance and Secure Operation

This section describes the configuration, maintenance, and administration of the cryptographic module. The Crypto Officer is responsible for ensuring none of the plaintext protocols or non-Approved ciphers in Section 10 are enabled. When configured according to Section 10 in this Security Policy, the modules only run in their FIPS-Approved mode of operation, with the exception of the Services in Table 7. Services listed in Table 7 make use of non-compliant cryptographic algorithms. Use of these algorithms are prohibited in a FIPS-approved mode of operation.

When the module is powered on, its power-up self-tests are executed without any operator intervention.

### 10.1 Initialization

The operator shall set up the device as defined in the PacketLight PL-2000M\_AD\_ADS Security Guide (the Security Guide is shipped with the cryptographic module). The Crypto-Officer shall also:

- Verify that the firmware version of the module is 1.3.12d.
- The default password of the Admin and Crypto-Officer shall be changed upon first use.
- All operator passwords must be a minimum of 8 characters in length.
- The default Pre-Shared Secret for Data Plane Encryption must be changed by the Crypto-Officer prior to enabling the Data Plane Encryption Service.
- RADIUS shall be disabled and not used the Approved mode of operation.
- Syslog shall be disabled and not used the Approved mode of operation.
- The Crypto-Officer shall be aware that performing the “Lock Encrypted Service” command will prevent the module from zeroizing CSPs.
- Enable HTTPS and configure the web server certificate prior to connecting to the WebUI over TLS.
- Ensure that SNMPv1 and SNMPv2c are disabled.
- Ensure the SNMP V3 Authentication is not set to use “No Auth” or “No Priv”. HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 or HMAC-SHA-512 shall be used for Authentication. AES-128, AES-192 and AES-256 shall be used for Privacy.
- For SSH/SFTP, ensure modulus sizes of 2048-bits of strength or use group 14 selected for Diffie-Hellman.
- Ensure that SSH is configured to use RSA for authentication.
- Ensure RSA keys are at least 2048-bit keys. No 512-bit or 1024-bit keys shall be used in FIPS mode of operation.
- The Crypto Officer shall ensure the Key Exchange Period for OTU4 traffic does not exceed 80 hours.
- Ensure all traffic is encapsulated in a TLS tunnel as appropriate. Ensure use of FIPS-approved algorithms for TLS:
  - DHE-RSA-AES256-GCM-SHA384;
  - DHE-RSA-AES128-GCM-SHA256;
  - ECDHE-RSA-AES256-GCM-SHA384;
  - ECDHE-RSA-AES128-GCM-SHA256;
  - DHE-RSA-AES256-SHA256;
  - DHE-RSA-AES128-SHA256;
  - ECDHE-RSA-AES256-SHA384;

- ECDHE-RSA-AES128-SHA256;
- ECDHE-RSA-AES256-SHA;
- ECDHE-RSA-AES128-SHA;
- DHE-RSA-AES256-SHA; and
- DHE-RSA-AES128-SHA.

Use of the non-conformant algorithms listed in Section 8.1.4 will place the module in a non-approved mode of operation.

## 10.2 Usage of AES GCM in the module

The module's software AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module is compatible with TLS v1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, 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 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 hardware AES-GCM implementation conforms to IG A.5, scenario #4. The module uses a 128-bit IV which is constructed deterministically per SP 800-38D Section 8.2.1 from a Frame Block Counter, Multi-Frame Index (MFI), Multi Frame Alignment Signal (MFAS) and a nonce.

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 140-2 IG A.5, which states that 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.

## 11. Glossary

| Term  | Description                                    |
|-------|------------------------------------------------|
| AES   | Advanced Encryption Standard                   |
| CAVP  | Cryptographic Algorithm Validation Program     |
| CFP   | C Form-factor Pluggable                        |
| CKG   | Cryptographic Key Generation                   |
| CMVP  | Cryptographic Module Validation Program        |
| COM   | Communication                                  |
| CRNGT | Continuous Random Number Generator Test        |
| CSP   | Critical Security Parameter                    |
| CTR   | Counter                                        |
| DRBG  | Deterministic Random Bit Generator             |
| ECB   | Electronic Codebook                            |
| FIPS  | Federal Information Processing Standards       |
| GCM   | Galois/Counter Mode                            |
| IG    | Implementation Guidance                        |
| IV    | Initialization vector                          |
| KAT   | Known answer test                              |
| KDF   | Key-Derivation Function                        |
| MFAS  | Multi-Frame Alignment Signal                   |
| MFI   | Multi-Frame Index                              |
| NIST  | National Institute of Standards and Technology |
| NDRNG | Non-Deterministic Random Number Generator      |
| OSC   | Open Sound Control                             |
| OTN   | Optical Transport Network                      |
| QSFP  | Quad Small Form-factor Pluggable               |
| RSA   | Rivest Shamir Adleman                          |
| SFP   | Small Form-factor Pluggable                    |
| SHA   | Secure Hash Algorithm                          |
| SHS   | Secure Hash Standard                           |
| TRNG  | True Random Number Generator                   |

*Table 18 - Glossary of Terms*