Ciena Corporation

Ciena 6500 Packet-Optical Platform 4x10G

Hardware Version: 2.0
Firmware Version: 2.00

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 3
Document Version: 0.5

Prepared by/for:

Ciena Corporation
7035 Ridge Road
Hanover, Maryland 21076
United States of America

Phone: +1 (410) 694-5700
Contact: http://www.ciena.com/about/contact-us/?navi=top
http://www.ciena.com

Table of Contents

Table of Figures

List of Tables

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy (SP) for the Ciena 6500 Packet-Optical Platform 4x10G (Hardware Version: 2.0, Firmware Version: 2.00) from Ciena Corporation. This Security Policy describes how the Ciena 6500 Packet-Optical Platform 4x10G meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This module supports one FIPS-Approved module of operation. This policy was prepared as part of the Level 3 FIPS 140-2 validation of the module. The Ciena 6500 Packet-Optical Platform 4x10G is referred to in this document as the cryptographic module or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Ciena website (http://www.ciena.com/) contains information on the full line of products from Ciena Corporation.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model document
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were modified from originals produced by Corsec Security, Inc. in 2014 while under contract to Ciena. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Ciena and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Ciena.

2. Ciena 6500 Packet-Optical Platform 4x10G

2.1 Overview

The module is the Ciena 6500 Packet-Optical Platform 4x10G, which is a daughter/mezzanine card designed for use on the 4x10G Encryption OTR[1] circuit pack of the 6500 series Packet-Optical Platform. The module, also known as the Krypto Daughter Card, provides fully secure cryptographic functionality (including key generation and management, physical security, and identification and authentication of the module's operators) on the 6500 Packet-Optical Platform.

Architected for network modernization, Ciena's 6500 Packet-Optical Platform converges comprehensive Ethernet, TDM[2], and WDM[3] capabilities in one platform for delivery of emerging and existing services, from the access edge to the backbone core. By using the 4x10G Encryption OTR circuit pack, customers can deploy solutions for 10Gbps[4] client services with high capacity and offer differentiated service options including several path/equipment protection options.

The 4x10G Encryption OTR circuit pack is a single-slot card that supports wire-speed point-to-point encryption and decryption (see Figure 1 below). The card contains eight 10G[5] ports; four SFP[6]+/SFP-based client ports (ports 1, 2, 3, and 4) and four XFP[7]-based line ports (ports 5, 6, 7, and 8) , with full 10Gbps throughput for all client ports.

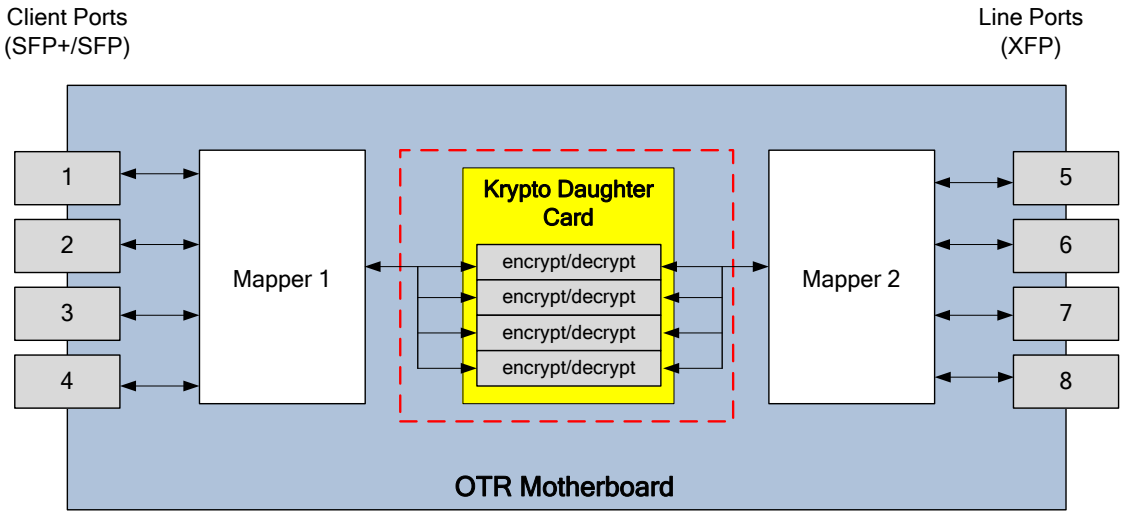

Figure 1 – The Module on Circuit Pack for Secure Communication

The circuit pack is composed of two primary components: the OTR motherboard and the module (shown as 'Krypto Daughter Card' above). The OTR motherboard contains two traffic-mapping devices, where 'Mapper 1' connects to the four client ports and 'Mapper 2' connects to the four line ports. The Krypto Daughter Card connects to the OTR motherboard via a mezzanine connector, and provides the bulk encryption and decryption capabilities.

[1] OTR – Optical Transponder
[2] TDM – Time-Division Multiplexing
[3] WDM – Wavelength-Division Multiplexing
[4] Gbps – Gigabits Per Second
[5] G – Gigabit
[6] SFP – Small Form Factor Pluggable
[7] XFP – (10 Gigabit) Small Form Factor Pluggable

This validation focuses on the Ciena 6500 Packet-Optical Platform 4x10G daughter card depicted in Figure 1 with red-colored dotted line. The module is housed in an aluminum enclosure with a heat sink lid secured with tamper-resistant screws. Any attempts to remove the lid will provide tamper evidence via two tamper evident labels and tamper-resistant screws, and additionally the module will immediately zeroize all keys and CSPs if the lid is removed.

Figure 2 below shows the top and bottom view of the module.

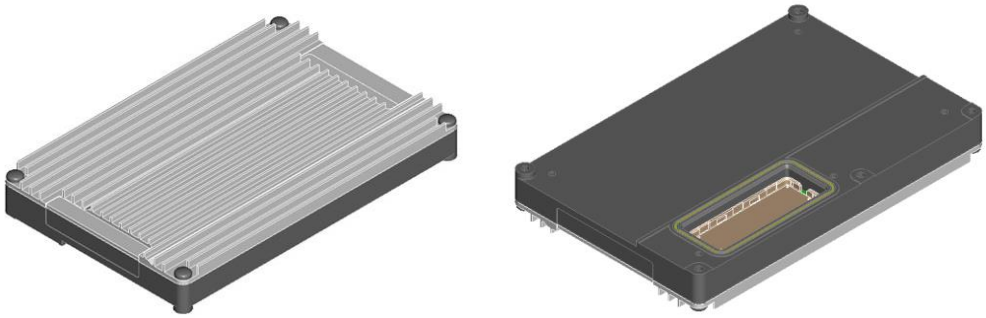

Figure 2 – Top and Bottom View of the Module

The module is validated at the FIPS 140-2 section levels as shown in Table 1 below.

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3
6	Operational Environment	N/A[8]
7	Cryptographic Key Management	3
8	EMI/EMC[9]	3
9	Self-tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The Ciena 6500 Packet-Optical Platform 4x10G is a hardware cryptographic module with a multiple-chip embedded embodiment. The module consists of firmware and hardware components enclosed in an aluminum metal enclosure. The main hardware components consist of integrated circuits, processors, Random Access Memories (SDRAM and BBRAM), flash memories (NOR and EEPROM), FPGAs[10], and

[8] N/A – Not Applicable
[9] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[10] FPGA – Field Programmable Gate Array

the enclosure. The overall security level of the module is 3. The cryptographic boundary of the module surrounds the module enclosure, which includes all the hardware components, firmware, and the metal case.

The Ciena 6500 Packet-Optical Platform 4x10G implements the FIPS-Approved algorithms as listed in Table 2 below.

Table 2 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number	
	FPGA	Firmware
AES[11] – CTR[12]and ECB[13] modes with 256-bit keys	#3600	
AES – CBC[14] mode with 128, 192, and 256-bit keys	-	#3599
AES–GCM mode with 128 and 256-bit keys	-	#3599
Triple-DES – CBC (3-key)	-	#2004
SHA[15]-1, SHA-256, SHA-384 and SHA-512	-	#2962
HMAC[16] with SHA-1, SHA-256, SHA-384 and SHA-512	-	#2297
NIST[17] SP[18]800-90A CTR_DRBG[19]	-	#933
RSA[20] Key generation (2048-bit) (FIPS 186-4)	-	#1851
RSA (PKCS[21] #1 v1.5) signature generation/verification (2048-bit)	-	#1851
ECDSA PKG[22] with NIST-defined P-curves P-224, P-256, P-384, and P-521 and PKV[23] with NIST defined P-curves P-192, P-224, P-384, and P-521.	-	#735
ECDSA signature generation with NIST-defined P-curves P-224, P-256, P-384 and P-521 with SHA-256, SHA-384, and SHA-512 ECDSA signature verification with NIST-defined P-curves P-192, P-224, P-256, P-384, and P-521 with SHA-1, SHA-256, SHA-384, and SHA-512	-	#735
Section 4.2 TLS[24] v1.2 (SP 800-135)	-	#623
Section 4.1.1 IKE[25] v1 (SP 800-135)	-	#623
Section 4.1.2 IKE v2 (SP 800-135)	-	#623

Note: The TLS and IKE protocols have not been reviewed or tested by the CAVP or CMVP.

[11] AES – Advanced Encryption Standard
[12] CTR – Counter
[13] ECB – Electronic Codebook
[14] CBC – Cipher Block Chaining
[15] SHA – Secure Hash Algorithm
[16] HMAC – (Keyed) Hash Message Authentication Code
[17] NIST – National Institute of Standards and Technology
[18] SP – Special Publication
[19] DRBG – Deterministic Random Bit Generator
[20] RSA – Rivest Shamir Adleman
[21] PKCS – Public-Key Cryptography Standards
[22] PKG – Public Key Generation
[23] PKV – Public Key Validation
[24] TLS – Transport Layer Security
[25] IKE – Internet Key Exchange

Additionally, the module implements the following algorithms that are allowed for use in a FIPS-Approved mode of operation:

- Non-Deterministic Random Number Generator (NDRNG)
- Diffie-Hellman[26] (2048-bit)
- Elliptic Curve Diffie-Hellman[27] (using NIST-defined P-curve P-384)

2.3 Module Interfaces

The module's design separates the physical ports into four logically distinct and isolated categories. They are:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Data input/output consists of the data utilizing the services provided by the module. This data enters and exits the module through the mezzanine connector of the module. Control input consists of configuration or administration data entered into the module through the mezzanine connector of the module remotely using the MyCryptoTool interface or locally using the Transport Control Subsystem (TCS) interface. Control input that enters the module through MyCryptoTool is secured with an HTTPS/TLS session. Status output consists of the signals output via the mezzanine connector that are then translated into alarms, LED[28] signals, and log information by the circuit pack.

The physical ports and interfaces of the Ciena 6500 Packet-Optical Platform 4x10G are depicted below in Figure 3.

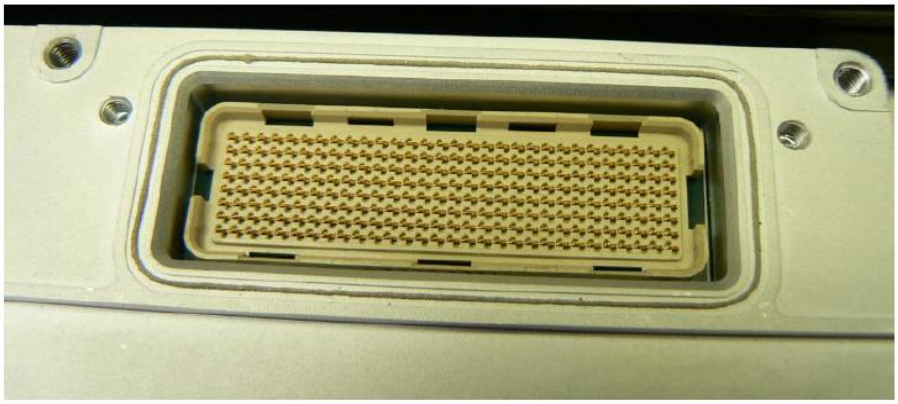

Figure 3 – Mezzanine Connector

Table 3 lists the physical ports and interfaces available in the module, and provides the mapping from the physical ports and interfaces to logical interfaces as defined by FIPS 140-2.

Table 3 – Logical Interface Mapping

FIPS 140-2 Logical Interface	Module Interface
Data Input Interface	Mezzanine Connector

[26] Caveat: Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength). Please see NIST Special Publication 800-131A for further details.
[27] Caveat: EC Diffie-Hellman (key agreement; key establishment methodology provides 192 bits of encryption strength). Please see NIST Special Publication 800-131A for further details.
[28] LED – Light Emitting Diode

FIPS 140-2 Logical Interface	Module Interface
Data Output Interface	Mezzanine Connector
Control Input Interface	Mezzanine Connector, tamper switch
Status Output Interface	Mezzanine Connector
Power Interface	Mezzanine Connector

2.4 Roles, Services, and Authentication

The following sections described the authorized roles supported by the module, the services provided for those roles, and the authentication mechanisms employed.

2.4.1 Authorized Roles

The module supports two authorized roles: a Crypto Officer (CO) role and a User role. The Crypto Officer and the User roles are responsible for module initialization and module configuration, including security parameters, key management, status activities, and audit review. All CO and User services (except the firmware upgrade service via the TCS interface) are provided through the MyCryptoTool. The MyCryptoTool interface is secured via an HTTPS/TLS session. The TCS interface is available to the CO only and is used for the firmware load.

Operators must assume an authorized role to access module services. Operators explicitly assume both the CO and User role by a mutually authenticated HTTPS/TLS session over MyCryptoTool using digital certificates. Operators explicitly assume the CO role over the TCS interface using a username and password credential.

2.4.2 Services

The services that require operators to assume an authorized role are listed in Table 4 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Table 4 use the following indicators to show the type of access required:

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, modified, or zeroized.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.

Table 4 – Authorized Operator Services

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Initialize the module	✓	✓	Initialize the module	Command	Status output	None
Configure the module using MyCryptoTool	✓	✓	Configure enterprise settings and import certificates	Command and parameter	Command response	Signing CA RSA/ ECDSA Public Key – R/X MKEK[29] – R/X KEK[30] – R/X

[29] MKEK – Master Key Encryption Key
[30] KEK – Key Encryption Key

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Monitor alarms	✓	✓	Monitor specific alarms for diagnostic purposes	Command	Status output	None
Manage data encryption certificate	✓	✓	Manage data encryption certificate enrollment, signing CA certificate information, trusted CA certificates, import CA certificate and CRL, and clear CSPs	Command and parameters	Command response	DEK[31] – R/W BKEK[32] – R/X MKEK – R/X KEK – R/X Signing CA RSA/ ECDSA Public Key – R/X X
Manage web access certificate and import CRL	✓	✓	Manage web access certificate and import CRL	Command and parameters	Command response	BKEK – R/X MKEK – R/X KEK – R/X Signing CA RSA/ ECDSA Public Key – R/X
Show FIPS status and statistics	✓	✓	Show the system status, FIPS-Approved mode, configuration settings, and active alarms.	Command	Status output	None
View system logs	✓	✓	View system status messages in historical alarm log and provisioning log.	Command	Status output	None
Zeroize using MyCryptoTool	✓	✓	Zeroize the keys and CSPs listed in the 'Zeroization' column in Table 7 below	Command	Command response	Please see the 'Zeroization' column in Table 7 below.
Employ encryption / decryption service	✓	✓	Encrypt or decrypt user data, keys, or management traffic	Command and parameters	Command response	BKEK – R/X MKEK – X DEK – X TLS Session Key – X
Message Authentication service	✓	✓	Authenticate management traffic	Command and parameters	Command response	TLS Authentication Key – X
Generate asymmetric key pair (data path)	✓	✓	Generate the asymmetric key pair (RSA/ECDSA)	Command and parameters	Key pair	Module Data Path RSA/ ECDSA Private Key – W Module Data Path RSA/ ECDSA Public Key – W
Generate asymmetric key pair (web access)	✓	✓	Generate the asymmetric key pair (RSA/ECDSA)	Command and parameters	Key pair	Module Web Access RSA/ ECDSA Private Key – W Module Web Access RSA/ ECDSA Public Key – W
Generate signature (CSR)	✓	✓	Generate a signature for the supplied message using specified key and RSA/ECDSA algorithm	Command and parameters	Status, signature	Module RSA/ ECDSA Private Key – R/X

[31] DEK – Data Encryption Key
[32] BKEK – Base Key Encryption Key

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Verify signature	✓	✓	Verify the signature on the supplied message using the specified key and RSA/ECDSA algorithm	Command and parameters	Status	Module RSA/ ECDSA Public Key – R/X
Perform device diagnostics	✓	✓	Test the module during operation, and monitor the module	Command and parameters	Command response and status via log and LEDs	None
Upgrade KM application firmware	✓		Upgrade the KM application firmware using ECDSA signature verification	Command and parameters	Command response and status output	ECDSA Public Key – R/X
Upgrade KM FPGA	✓		Upgrade the KM FPGA using ECDSA signature verification	Command and parameters	Command response and status output	ECDSA Public Key – R/X

In FIPS-Approved mode, the module provides a limited number of services for which the operator is not required to assume an authorized role (see Table 5). None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

Table 5 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Perform operator authentication	Authenticates operators to the module	Command	Status output	CO RSA/ECDSA Public key – R/X User RSA/ECDSA Public key – R/X CA RSA/ECDSA Public Key – R/X Preshared Authentication String – R/X
Perform peer authentication	Authenticates peer devices to the module	Command	Status output	Peer RSA/ECDSA Public key – R/X
Zeroize using TCS	Zeroize certificates and KEK	Command	Command response	Please see the 'Zeroization' column in Table 7 below.
Perform on-demand self-tests	Performs Power-up Self-Tests on demand via module restart	Use power button on the host system, Command	Status output	All plaintext keys and CSPs – W
Show system status and statistics using TCS	Show the system status, system identification, and configuration settings of the module	Command	Status output	None
Configure the module using TCS	Configure and manage the carrier provisioning	Command	Response and status output	None

Service	Description	Input	Output	CSP and Type of Access
Process data traffic	Encrypt and decrypt data traffic	None	Status output	DEK – W/X Entropy Input string – R DRBG seed – W/R

2.4.3 Authentication Mechanisms

The module supports identity-based authentication. Module operators must authenticate to the module before being allowed access to services that require the assumption of an authorized role. The module authenticates an operator using digital certificates containing public key of the operator. The authentication is achieved via the process of initiating a TLS session and using digital certificates towards mutual authentication. The process of mutual authentication provides assurance to the module that it is communicating with an authenticated operator. The strength calculation below provides minimum strength based on the public key size in the digital certificates.

The module employs the authentication methods described in Table 6 to authenticate Crypto Officers and Users.

Table 6 – Authentication Mechanism

Authentication Type	Strength
Public Key Certificates	The module supports RSA digital certificate authentication of Crypto Officers and Users during MyCryptoTool access. Using conservative estimates and equating a 2048-bit RSA key to a 112-bit symmetric key, the probability for a random attempt to succeed is $1:2^{112}$ or $1: 5.19 \times 10^{33}$. Alternately the module can be configured to support ECDSA digital certificate authentication of COs and Users during MyCryptoTool access. Using conservative estimates and equating the use of ECDSA with the P-384 elliptic curve to a 192-bit symmetric key, the probability for a random attempt to succeed is: $1:2^{192}$ or $1: 6.28 \times 10^{51}$ For either mode this is less than 1:1,000,000 as required by FIPS 140-2 The fastest network connection supported by the modules over Management interfaces is 5 Mbps. Hence, at most ($5 \times 10^6 \times 60 = 3 \times 10^8$ =) 300,000,000 bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed or a false acceptance will occur in one minute is In RSA Mode: 1: (2^{112} possible keys / ((3×10^8 bits per minute) / 112 bits per key)) 1: (2^{112} possible keys / 2,678,572 keys per minute) $1: 19.38 \times 10^{26}$; which is less than 1:100,000 as required by FIPS 140-2. In ECC Mode: 1: (2^{192} possible keys / ((3×10^8 bits per minute) / 192 bits per key)) 1: (2^{192} possible keys / 1,562,500 keys per minute) $1: 4.02 \times 10^{51}$ which is less than 1:100,000 within one minute as required by FIPS 140-2.
Preshared Key	The module supports the use of Preshared authentication string for the TCS interface accessing the module on behalf of the Crypto Officer. An HMAC-SHA-256 operation with a 512-bit key is performed on the Preshared authentication string. The 256-bit output value of the HMAC-SHA-256 value will have an equivalent symmetric key strength of 128 bits, Using conservative estimates, the probability for a random attempt to succeed is $1:2^{128}$ or $1: 3.40 \times 10^{38}$. The module implements a 200 ms delay between authentication attempts yielding a rate of five (5) attempts per second, and therefore 300 attempts per minute. Given that an attacker will have at most, 300 attempts in one minute, and there are $1: 3.40 \times 10^{38}$ possibilities, the probability that a random attempt will succeed or a false acceptance will occur in one minute is: $1: 3.40 \times 10^{38}$ / 300 attempts per minute $1: 1.13 \times 10^{36}$ which is less than 1:100,000 as required by FIPS 140-2.

The module also performs authentication of Peers using public key certificates but the module does not provide any authenticated services to the Peer.

2.5 Physical Security

All CSPs are stored and protected within the module's hard aluminum enclosure. The enclosure is completely opaque within the visible spectrum. The enclosure is secured using tamper-resistant screws, tamper-evident labels, and tamper switches with tamper-response circuitry. Any attempts to defeat or bypass the tamper-response mechanism on the enclosure to access the module's internal components would result in zeroization of all the plaintext keys and CSPs.

Once the module is commissioned and the tamper-response circuitry is activated, it continuously monitors the enclosure via the tamper switches. On removal of the cover, detection of unauthorized access, or tamper event, the tamper-response circuitry inside the enclosure immediately erases all the plaintext keys and CSPs stored within the module.

Further, the enclosure of the module has been tested for hardness at a temperature of 74°F; no assurance is provided for Level 3 hardness conformance at any other temperature.

2.6 Operational Environment

The operational environment of the module does not provide access to a general-purpose operating system (OS) to the module operator. The module's Xilinx XC7Z045 processor runs an embedded Linux Kernel in a non-modifiable operational environment. The operating system is not modifiable by the operator, and only the module's signed image can be executed. All firmware downloads are digitally signed, and a conditional self-test (ECDSA signature verification) is performed during each download. If the signature test fails, the new firmware is ignored and the current firmware remains loaded. Only FIPS validated firmware may be loaded into the module to maintain the module's validation.

2.7 Cryptographic Key Management

The module generates keys as described in example #1 of FIPS 140-2 Implementation Guidance 7.8. It uses the FIPS-Approved CTR_DRBG (as specified in SP 800-90A) to generate cryptographic keys and RSA/ECDSA key pairs. The DRBG is seeded from seeding material provided by a hardware-based Non-Deterministic Random Number Generator (NDRNG), which provides an entropy source and whitening circuitry to supply a uniform distributed unbiased random sequence of bits to the DRBG.

The module supports the CSPs described in Table 7.

Table 7 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization[33]	Use
Base Key Encryption Key (BKEK)	AES 256-bit key	Preloaded at the factory	Never exits the module	Stored in plaintext in battery backed (BB) RAM[34] in the module	Power is removed from BB RAM	Used for decrypting MKEK
Master Key Encryption Key (MKEK)	AES 256-bit key	Preloaded at the factory	Never exits the module	Encrypted with BKEK and stored in the non-volatile memory	Power is removed from BB RAM	Used for encryption/decrypting KEK
Key Encryption Key (KEK)	AES 256-bit key	Generated internally	Never exits the module	Encrypted with MKEK and stored in non-volatile memory	Power is removed from BB RAM or by command via MyCryptoTool and TCS interface	Used for encrypting/decrypting private key of an entity key pair
Data Encryption Key (DEK)	AES 256-bit key	Generated internally	Never exits the module	Plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for encrypting or decrypting payload data between an authorized external entity and the module
Initialization Vector (IV)	128-bit value	Generated internally	Never exits the module	Plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for encrypting or decrypting payload data between an authorized external entity and the module
Preshared Authentication String	256-bit value	Hardcoded at the factory	Never exits the module	Stored plaintext in non-volatile memory (embedded in code)	N/A	Used for authenticating a CO for the Firmware Load service

[33] Zeroization – Upon the detection of a tamper event, the module zeroizes all keys and CSPs listed in Table 7.
[34] RAM – Random Access Memory

Key	Key Type	Generation / Input	Output	Storage	Zeroization[33]	Use
IKE DH[35] Private Component	224-bit DH key	Generated internally during IKE negotiation	Never exits the module	Plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for exchanging shared secret to derive session keys during IKE
IKE DH Public Component	2048-bit DH key	The module's public key is generated internally during IKE negotiation; public key of a peer enters the module in plaintext	The module's public key exits the module in plaintext; public key of the a peer never exits the module	Plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for exchanging shared secret to derive session keys during IKE
IKE Session Encryption Key	AES 256-bit key	Generated internally during DH key negotiation	Never exits the module	Plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for encrypting/decrypting IKE messages
IKE Session Authentication Key	HMAC SHA-256	Generated internally during DH key negotiation	Never exits the module	Plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating IKE messages

[35] DH – Diffie-Hellman

Key	Key Type	Generation / Input	Output	Storage	Zeroization[33]	Use
IKEv2 ECDH[36] Private Component	384-bit value	Generated internally during IKEv2 negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for exchanging shared secret to derive session keys during IKEv2
IKEv2 ECDH Public Component	384-bit value	The module's public component is generated internally during IKEv2 negotiation; public component of a peer enters the module in plaintext	The module's public component exits the module in plaintext; public key of the a peer never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for exchanging shared secret to derive session keys during IKEv2
IKEv2 Session Encryption Key	AES 256-bit key	Generated internally during EC DH key negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for encrypting/decrypting IKEv2 messages using AES-GCM
IKEv2 Session Authentication Key	HMAC SHA-384	Generated internally during EC DH key negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating IKEv2 messages

[36] ECDH – Elliptic Curve Diffie-Hellman

Key	Key Type	Generation / Input	Output	Storage	Zeroization[33]	Use
TLS Session Key	AES 128 or 256-bit or Triple-DES 168-bit key	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for encrypting/decrypting TLS messages
TLS Authentication Key	HMAC SHA-256, HMAC SHA-384	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating TLS messages
TLS Pre-Master Secret	384-bit random value	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Establish the TLS Master Secret
TLS Master Secret	384-bit random value	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Establish the TLS Session Key
Peer RSA Public Key	2048-bit key	Enters the module in encrypted form	Never exits the module	Stored in plaintext in RAM	By reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating the peers
CA RSA Public Key	2048 or 4096-bit key	Enters the module in encrypted form	Never exits the module	Stored plaintext in non-volatile memory	By Command via MyCryptoTool and TCS interface	Used for authenticating the operator
CO RSA Public Key	2048-bit key	Enters the module in encrypted form	Never exits the module	Stored in plaintext in RAM	By reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating the CO

Key	Key Type	Generation / Input	Output	Storage	Zeroization[33]	Use
User RSA Public Key	2048-bit key	Enters the module in encrypted form	Never exits the module	Stored in plaintext in RAM	By reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating the User
Module RSA Private Key	2048-bit key	Generated internally using approved DRBG; imported in encrypted form	Never exits the module	Stored encrypted with KEK in non-volatile memory	By command via MyCryptoTool and TCS interface	Used for signature generation
Module RSA Public Key	2048-bit key	Generated internally using approved DRBG; imported in encrypted form	Exits the module encrypted	Stored plaintext in non-volatile memory	By command via MyCryptoTool and TCS interface	Used for mutual authentication
Peer ECDSA Public Key	384-bit key	Enters the module in encrypted form	Never exits the module	Stored in plaintext in RAM	By reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating the peers
CA ECDSA Public Key	384-bit key	Enters the module in encrypted form	Never exits the module	Stored plaintext in non-volatile memory	By command via MyCryptoTool and TCS interface	Used for authenticating the operator
CO ECDSA Public Key	384-bit key	Enters the module in encrypted form	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating the CO
User ECDSA Public Key	384-bit key	Enters the module in encrypted form	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for authenticating the User
Module ECDSA Private Key	384-bit key	Generated internally using approved DRBG; imported in encrypted form	Never exits the module	Stored encrypted with KEK in non-volatile memory	By command via MyCryptoTool and TCS interface	Used for signature generation

Key	Key Type	Generation / Input	Output	Storage	Zeroization[33]	Use
Module ECDSA Public Key	384-bit key	Generated internally using approved DRBG; imported in encrypted form	Exits the module encrypted	Stored plaintext in non-volatile memory	By command via MyCryptoTool and TCS interface	Used for mutual authentication
ECDH Private Component	384-bit value	Generated internally during TLS negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for establishing TLS session for MyCryptoTool.
ECDH Public Component	384-bit value	The module's public component is generated internally during TLS negotiation; public component of a peer enters the module in plaintext	The module's Public Component exits the module in plaintext; Public Key Component of the a peer never exits the module	Stored in plaintext in RAM	By session termination, reboot, power removal, or command via MyCryptoTool and TCS interface	Used for establishing TLS session for MyCryptoTool
DRBG seed	384-bit value	Generated internally using entropy input	Never exits the module	Stored in plaintext in RAM	By reboot, power removal or command via MyCryptoTool and TCS interface	Used for random number generation
Entropy Input string	512-bit value	Generated internally using NDRNG	Never exits the module	Stored in plaintext in RAM	By reboot, power removal or command via MyCryptoTool and TCS interface	Used for random number generation

2.8 EMI/EMC

The module was tested and found to be conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

2.9 Self-Tests

The module performs various Self-Tests (Power-Up Self-Tests, Conditional Self-Tests, and Critical Function Self-Tests) on the cryptographic algorithm implementations to verify their functionality and correctness.

2.9.1 Power–Up Self–Tests

The Ciena 6500 Packet-Optical Platform 4x10G module performs the following self-tests at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithms implemented in the module:

- Integrity test for the KM application firmware image (Zone A) using ECDSA signature verification
- Integrity test for the KM application firmware image (Zone B) using ECDSA signature verification
- Integrity test for the KM FPGA (Zone B) image using ECDSA signature verification
- Following algorithm self-tests have been implemented for FIPS-Approved algorithms:
    - o KM
        - AES CBC Encryption Known Answer Test (KAT)
        - AES CBC Decryption KAT
        - AES GCM Encryption KAT
        - AES GCM Decryption KAT
        - Triple-DES Encryption KAT
        - Triple-DES Decryption KAT
        - SHA-1 KAT
        - SHA-256, 384, 512 KAT
        - HMAC SHA-1 KAT
        - HMAC SHA-256, 384, 512 KAT
        - SP 800-90A CTR_DRBG KAT
        - RSA 186-4 Signature Generation KAT
        - RSA 186-4 Signature Verification KAT
        - ECDSA 186-4 Signature Generation Pairwise Consistency Test (PCT)
        - ECDSA 186-4 Signature Verification PCT
    - o FPGA
        - AES Encryption KAT
        - AES Decryption KAT

The power-up self-tests can be performed at any time by power-cycling the module or via TCS command.

2.9.2 Conditional Self-Tests

The Ciena 6500 Packet-Optical Platform 4x10G implements the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for the SP 800-90A CTR_DRBG
- CRNGT for the NDRNG
- Pair-wise Consistency Test for RSA key pair generation and verification
- Pair-wise Consistency Test for ECDSA key pair generation and verification
- Firmware Load Test for the KM Application using ECDSA signature verification

- Firmware Load Test for the KM FPGA using ECDSA signature verification

2.9.3 Critical Function Self-Tests

The Ciena 6500 Packet-Optical Platform 4x10G performs the following critical function self-tests:

- SP 800-90 CTR_DRBG Instantiate Health Test
- SP 800-90 CTR_DRBG Generate Health Test
- SP 800-90 CTR_DRBG Reseed Health Test
- SP 800-90 CTR_DRBG Uninstantiate Health Test

2.9.4 Self-Test Failure Handling

Upon the failure of any power-up self-test (except the Zone A application firmware integrity test, Zone B application firmware integrity test, or the Zone B FPGA integrity test), conditional self-test (except firmware load test), or critical function test, the module goes into "Critical Error" state and disables all access to cryptographic functions and CSPs. All data output via data output interfaces are inhibited upon any self-test failure. A permanent error status will be relayed via the status output interface, which then is interpreted either in the illumination of an LED or as a recorded entry to the system log file or alarm history log file.

During the integrity tests at start up, the module first checks the Zone A firmware image. If this test fails, the module transitions to a Zone A Soft Error state where it will skip Zone A and proceed with Zone B application firmware and FPGA integrity test. If the Zone A firmware image passes the integrity check, the module checks the firmware and FPGA within Zone B. If the Zone B firmware integrity check fails, the module transitions to either Critical Error state if Zone A firmware integrity check also fails or Zone B Soft Error state if Zone A firmware integrity check passes. If the Zone B firmware integrity check passes, but the Zone B FPGA integrity check fails, the module transitions to a Zone B Soft Error state where a new firmware image can be loaded from TCS interface followed by a reboot.

Upon failure of the firmware load test, the module enters "Soft Error" state. The soft error state is a non-persistent state wherein the module resolves the error by rejecting the loading of the new firmware. Upon rejection, the error state is cleared, and the module resumes its services using the previously-loaded firmware.

While the error state persists, the module replies to all cryptographic service requests with a pre-defined error message to indicate the error status. The management interface does not respond to any commands until the module is operational. The module requires rebooting or power-cycling to come out of the error state and resume normal operations. In the case of firmware or FPGA load corruption in Zone B that cannot be corrected by TCS interface, the module will not be able to resume normal operation and the Crypto Officer should contact Ciena.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any other attacks.

3. Secure Operation

The Ciena 6500 Packet-Optical Platform 4x10G meets overall Level 3 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-Approved mode of operation.

3.1 Initial Setup

The Ciena 6500 Packet-Optical Platform 4x10G module does not require any installation activities as it is delivered to the customer pre-installed on the circuit pack from the factory. Either the Crypto Officer or the User can perform the Secure Operation responsibilities and tasks listed here; however, this Security Policy places this responsibility solely on the Crypto Officer. On receipt of the circuit pack, the Crypto Officer must check that the tamper evident labels are in place as well as the battery in the battery holder. After the circuit pack is removed from the shipping package and prior to use, the Crypto Officer must perform a physical inspection of the unit for signs of damage. If damage is found, the Crypto Officer shall immediately contact Ciena.

The module is shipped from the factory with the required physical security mechanisms (tamper-evident labels, tamper-resistant screws, and tamper switches with tamper-response circuitry) installed. The Crypto Officer should check the package for any irregular tears or opening. If tampering is suspected, the Crypto Officer should immediately contact Ciena. The module is contained in a strong, hard metal enclosure, and is protected by tamper-evident labels, tamper-resistant screws, tamper switches, and tamper-response circuitry. See Figure 4 below for tamper-evident label locations.

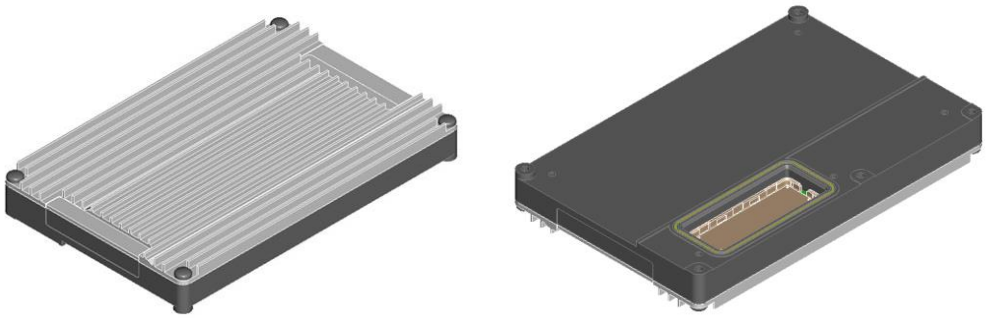

Figure 4 – Top and Bottom View of the Module

The Crypto Officer is responsible for configuring the module, which includes the configuration of the data path parameters and the security parameters for the data path. The Crypto Officer must install the web server certificate, one or more CA Certificates in order for the module to be able to verify the submitted CO and User RSA/ECDSA Public keys during TLS mutual authentication for the MyCryptoTool interface. Please refer to Chapter 4, "Provisioning Certificate Management using MyCryptoTool" in Ciena's *MyCryptoTool User's Guide* document for more information. Once the module's web server certificate has been configured, the web server software will restart for the certificate change to take effect and begin enforcing TLS mutual authentication. When the web server has completed the restart process, the module operates only in FIPS-Approved mode of operation. At any point of time, the "FIPS mode" status of the module can be viewed using the MyCryptoTool interface.

The module comes provisioned into FIPS mode from the factory, and the module will remain and operate in FIPS-Approved mode of operation unless decommissioned by the CO or the physical security has been breached.

3.2 Secure Management

The Crypto Officer is responsible for maintaining and monitoring the status of the module to ensure that it is running in its FIPS-Approved mode. For additional details regarding the management of the module, please refer to Ciena's *User's Guide and Technical Practices* document.

3.2.1 Management

When configured according to the Crypto Officer guidance in this Security Policy, the module only runs in an Approved mode of operation. The Crypto Officer is able to monitor and configure the module via MyCryptoTool. Detailed instructions for monitoring and troubleshooting the module are provided in the Ciena's *User's Guide and Technical Practices* document.

3.2.2 Physical Inspection

As the labels are applied at the factory, the CO shall inspect the module to ensure that the labels are applied correctly. The CO shall periodically inspect the module for evidence of tampering at six-month intervals. The CO shall visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of tampering. The CO shall also inspect the module's enclosure for any signs of damage. If evidence of tampering is found during periodic inspection, the Crypto Officer should send the module back to Ciena Corporation for repair or replacement.

3.2.3 Monitoring Status

The Crypto Officer should monitor the module's status regularly. The operational status of the module can be viewed using MyCryptoTool. At any point of time, the "FIPS mode" status of the module can be viewed by accessing the "Encryption Details", "Data Encryption Certificate Management", "Web Access Certificate Management", "Active Alarms", or "Historical Logs" web page of the MyCryptoTool interface. The line at the top of these pages indicates "FIPS mode" of the module.

3.2.4 Zeroization

All ephemeral keys used by the module are zeroized on reboot, session termination, factory reset, or tamper event. The "Clear CSP (Critical Security Parameter)" button on MyCryptoTool and via the Zeroize command via TCS also allows an operator to clear certificates and the KEK. CSPs reside in SDRAM and Flash memory.

The BKEK is stored in battery-backed RAM. Other keys and CSPs are stored in the volatile and non-volatile memories of the module. The BKEK can be zeroized by removing power to the BB RAM or in response to tamper events. The zeroization of the BKEK renders other keys and CSPs, including MKEK and KEK stored in non-volatile memory of the module useless, thereby, effectively zeroizing them. The zeroization of KEK renders asymmetric private keys inaccessible, thereby, rendering them unusable. The only public key that is stored in a file is embedded in code and is used for verifying the integrity of the image files cannot be zeroized. Resetting the module to factory state (software-controlled erasure) also erases all the volatile and non-volatile keys and CSPs from the module. Additionally, all keys and CSPs are also zeroized or become inaccessible when the module detects a tamper event.

3.3 User Guidance

The User shall follow all the instructions and guidelines provided for the Crypto Officer in Section 3 of this Security Policy document in order to ensure the secure operation of the module.

4. Acronyms

Table 8 below describes the acronyms used in this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BB	Battery Backed
BKEK	Base Key Encryption Key
CA	Certificate Authority
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
DCC	Data Communication Channel
DEK	Data Encryption Key
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
Gb/s	Gigabit Per Second
GbE	Gigabit Ethernet
GCC	General Communication Channel
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IKE	Internet Key Exchange
IV	Initialization Vector
KAT	Known Answer Test

Acronym	Definition
KEK	Key Encrypting Key
LED	Light Emitting Diode
MKEK	Master Key Encrypting Key
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
OS	Operating System
OTN	Optical Transport Network
OTR	Optical Transponder
PKCS	Public-Key Cryptography Standards
PRNG	Pseudo Random Number Generator
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest, Shamir, and Adleman
SDRAM	Synchronous Dynamic Random Access Memory
SHA	Secure Hash Algorithm
SP	Special Publication
TLS	Transport Layer Security