Non-Proprietary FIPS 140-2 Security Policy

Ciena® Corporation

Ciena Waveserver Ai WCS-2 Module

Hardware P/N: 186-1034-411-EB, Revision 002 with PCB P/N: 186-1034-210 Revision 001

Firmware Release 1.3.5, 1.3.6 or 1.3.61

And

Hardware P/N: 186-1034-411-EB Revision 003 with PCB P/N: 186-1034-210 Revision 001 or Hardware P/N: 186-1034-411-EB Revision 004 with PCB P/N: 186-1034-210 Revision 001

Firmware Release 1.3.6 or 1.3.61

Date: 07/29/2020

Prepared for:

ciena®

Ciena® Corporation
7035 Ridge Road
Hanover, Maryland 21076
United States of America
Phone: +1 410 694 5700
www.ciena.com

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: http://csrc.nist.gov/groups/STM/cmvp.

About this Document

This non-proprietary Cryptographic Module Security Policy for Ciena Waveserver Ai WCS-2 Module from Ciena® Corporation 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 Ciena Waveserver Ai WCS-2 Module may also be referred to as the “module” or “WCS2” in this document.

Disclaimer

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

Notices

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Ciena Corporation Ciena Waveserver Ai WCS-2 (WCS2) Module, Hardware P/N: 186-1034-411-EB, Revision 002 with PCB P/N: 186-1034-210 Revision 001 with firmware version 1.3.5, 1.3.6 or 1.3.61 and Hardware P/N: 186-1034-411-EB Revision 003 with PCB P/N: 186-1034-210 Revision 001 or Hardware P/N: 186-1034-411-EB Revision 004 with PCB P/N: 186-1034-210 Revision 001 with firmware version 1.3.6 or 1.3.61. 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

Waveserver Ai Platform is designed to address evolving density and power requirements for ultra-high-capacity interconnect applications.

The WCS2 module is implemented as components on a Waveserver Ai WCS2 circuit pack. It is the physical security boundary and is composed of FPGA, SSD, DDR4, Flash and the PCB-embedded wire connections between them, and all associated physical security mechanisms (defined in Section 6 and illustrated in Section 12.1). The WCS2 module provides fully secure cryptographic functionality, including key generation and management, physical security, and identification and authentication of the module's Crypto Officer (CO) and User.

2. Security Level

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	3
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	3
Mitigation of Other Attacks	N/A
Overall Level	2

Table 1 - Security Level

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The Ciena Waveserver Ai WCS-2 Module is a hardware module with a multiple-chip embedded embodiment. The module consists primarily of a Xilinx Zynq Ultrascale+ CPU mounted on the motherboard's PCB and covered by an aluminum enclosure. The module also contains integrated circuits, a SATA SSD component, Dynamic Random-Access Memory (DRAM), and Flash memory. The components communicate via wire connections embedded beneath multiple PCB layers.

The overall security level of the module is 2. The cryptographic boundary of the WCS2 surrounds the CPU, SSD, Flash and DRAM. The portion of the PCB under which the connecting wire traces are embedded, and all physical security mechanisms are described in Section 6.

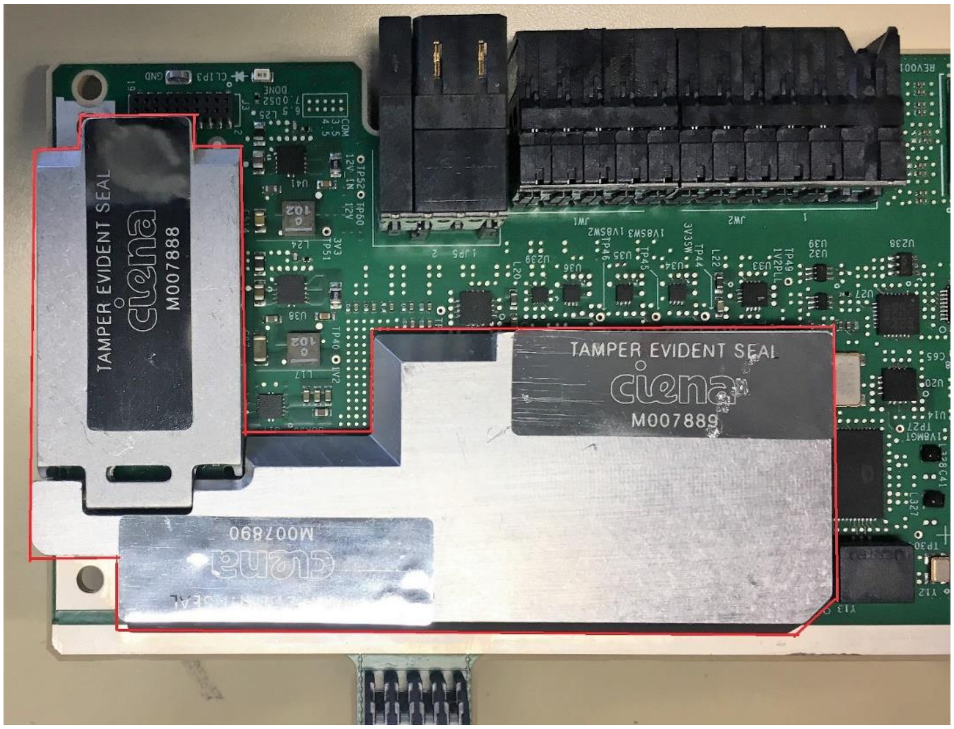

Figure 1- Top of module

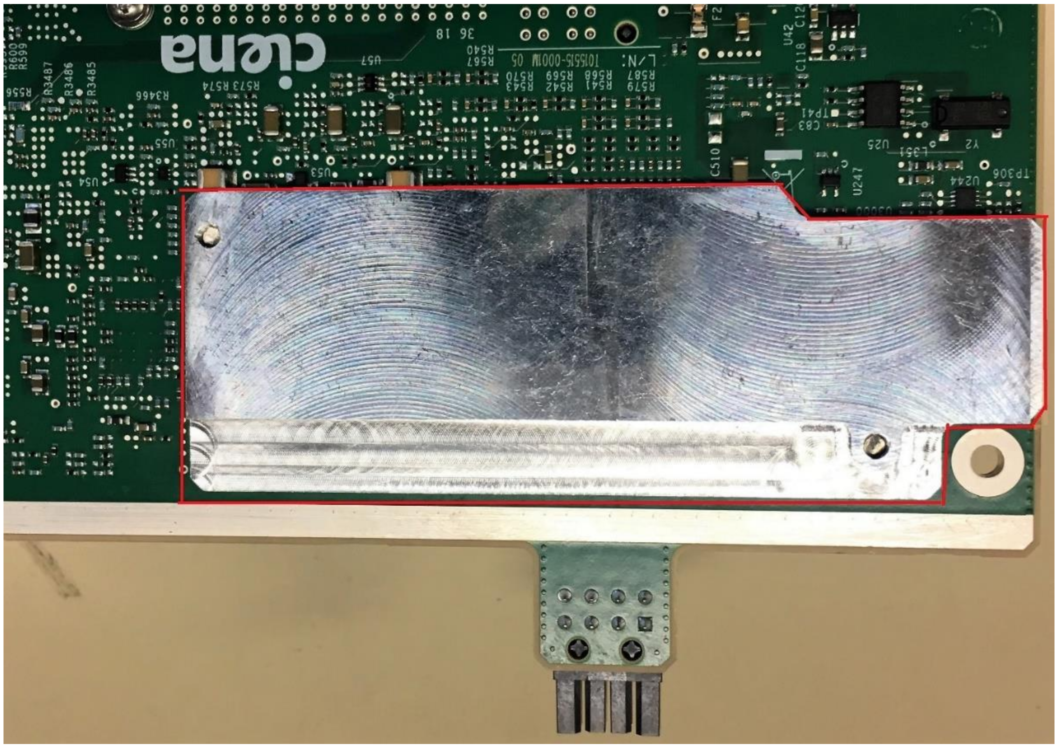

Figure 2- Bottom of module

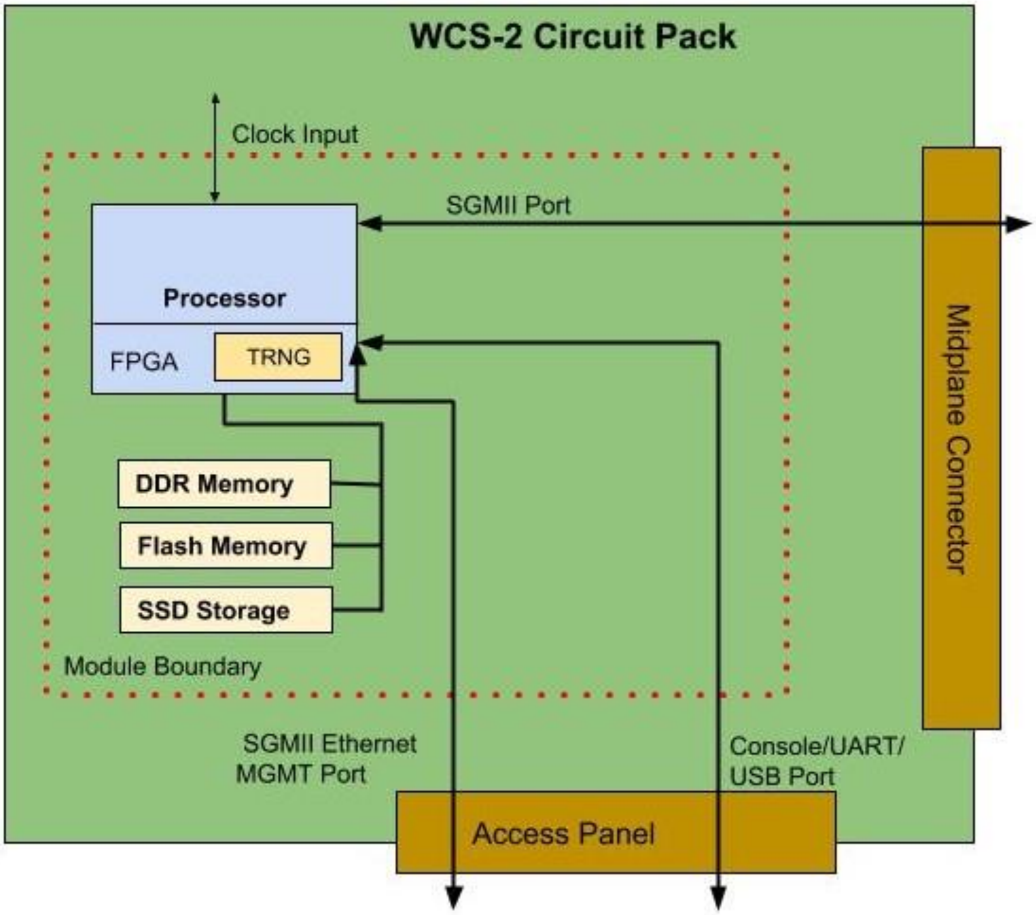

Figure 3 - Module Block Diagram

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.

Data input/output consists of the data utilizing the services provided by the module. Control input consists of configuration or administration data entered into the module. Status output consists of signals output that are then translated into alarms and log information by the module.

The physical ports of the WCS2 Module are depicted in Figure 3.

Table 2 lists the physical ports and interfaces available in the WCS2 Module and provides the mapping from the physical ports and interfaces to logical interfaces as defined by FIPS 140-2. Interfaces are provided by the Midplane Connector, Console Port (line in the PCB) and Ethernet Management port (line in the PCB).

Physical Port	FIPS 140-2 Logical Interface Mapping
Midplane Connector (SGMII Port)	Data Input and Output Interface Status Output Interface Control Input Interface Power Input
Console UART/USB Port	Status Output Interface Control Input Interface
Ethernet Management Port (SGMII)	Data Input and Output Interface, Status Output Interface Control Input Interface
Clock Input Port	Data Input Interface

Table 2 - Physical Port and Logical Interface Mapping

5. Roles, Services and Authentication

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

5.1 Roles

The module supports two authorized roles: a CO role and a User role. The CO and User roles are responsible for module initialization and module configuration, including security parameters, key management, status activities, and audit review. The module enforces the separation of roles using either of the identity-based operator authentication methods in Section 5.3.

The CO and User roles configure and monitor the module via a console, HTTPS or SSH connection. As super-user, the CO and User have permission to view and edit secrets within the module. The CO and User configure and provision the directly connected Ciena Waveserver Ai Encryption Module over the mid-plane connector.

While operators must assume an authorized role to access most module services, there are a limited number of services for which the operator is not required to assume an authorized role. See Table 4 below for additional details on these services.

5.2 Services

The services that require operators to assume an authorized role are listed in Table 3 below. Please note that the keys and Critical Security Parameters (CSPs) listed in Tables 3 and 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.

The module provides the following Approved services which utilize the algorithms listed in Tables 6, 7 and 8:

Service	User	Crypto Officer	Description	Input	Output	CSP and Type of Access

Initialize the module	✓	✓	Initialize the module	Command	Status output	BKEK (X);
						MKEK (R/X);
						KEK (R/W/X);
						PKIX-KEK (R/W/X);

Configure the module	✓	✓	Configure the module settings and Import certificates over SSH or the Console
			Setup DP, Syslog, RADIUS, HTTPS, keys etc.
				Command and parameters	Command response	MKEK (R/X);
						KEK (R/W/X);
						PKIX-KEK (R/W/X);
						SSH CSPs (R/W/X);
						TLS CSPs (R/W/X);
						Password (R/W/X);
						Customer Enrollment Certificate (R/W/X);
						Customer Enrollment Pre-Shared Key or DP Customer Enrollment Certificate (R/W/X);

Monitor alarms (show status)	✓	✓	Monitor specific active alarm for diagnostic purposes	Command	Status output	SSH CSPs (R/W/X);
View system logs (show status)	✓	✓	View system status messages in local alarm log and provisioning log or via Syslog over TLS	Command	Status output	None; Or TLS CSPs (R/W/X);

Manage the Datapath Encryption Card	✓	✓	Manage the directly connected Encryption Card Module using SecureMPL	Command	SecureMPL CSPs	MKEK (R/X);
						KEK (R/X);
						Customer Enrollment Pre-Shared Key or DP Customer Enrollment Certificate(R/W/X);
						Ciena Device ID (R/W/X);
						SecureMPL CSPs (R/W/X)

Zeroize	✓	✓	Zeroize the keys and CSPs listed in the 'Zeroization' column in Table 9 below	Command	Command response	Please see the 'Zeroization' column in Table 9 below
Perform Secure Transfer	✓	✓	Transfer configuration file or firmware image to the module	Command and parameters	Command response	SSH CSPs (R/W/X); Password (R/W/X)

Service	User	Crypto Officer	Description	Input	Output	CSP and Type of Access
Upgrade application firmware	✓	✓	Upgrade the application firmware using RSA signature verification	Command and parameters	Command and response and status output	RSA Public Key (R/X)

Table 3 - Approved Services and Role allocation

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 4). None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

Service	Description	Input	Output	CSP and Type of Access
Perform operator authentication	Authenticate operators to the module local database or external RADIUS over TLS server	Command	Status output	TLS CSPs (R/W/X); SSH CSPs (R/W/X)
Perform on demand self-tests	Perform Power-up Self-Tests on demand via module restart	Power button on the host system or command	Status output	N/A
Factory Reset	A last resort factory reset is available via a signal.	Signal or command	Status output	Zeroizes all CSPs

Table 4- Additional Services

5.3 Authentication

The module supports identity-based authentication. Module operators must authenticate before being allowed access to services that require the assumption of an authorized role. The module authenticates an operator using a username and password or digital certificate containing the public key of the operator. Authentication is achieved by initiating a console, SSH, TLS/HTTPS, SSH or SecureMPL session. Digital certificates are for mutual authentication for SSH, TLS/HTTPS or SecureMPL sessions. The process of mutual authentication provides assurance to the module that it is communicating with an authenticated operator. The strength calculations below provide the minimum strength based on the public key size in the digital certificates.

The module employs the authentication methods described in Table 5 to authenticate COs and Users.

Authentication Type	Strength
Public Key Certificates (TLS/HTTPS and SSH)	The module supports ECDSA P-256, P-384 and P-521 bit and RSA 2048, 3072 and 4096-bit digital certificate authentication of COs and Users.

	Using conservative estimates and equating the use of ECDSA with the P-256 elliptic curve to a 128-bit symmetric key, the probability for a random attempt to succeed is: 1:2^{128} or 1: 3.4 x 10^{38} which 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 1GB/s. Hence, at most (1 ×10^{9} × 60 = 6 × 10^{10}) 60,000,000,000 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: 1: (2^{128} possible keys / ((6 × 10^{10} bits per minute) / 128 bits per key)) 1: (2^{128} possible keys / 468,750,000 keys per minute) 1: 7.26 x 10^{29} which is less than 1:100,000 within one minute as required by FIPS 140-2. Using conservative estimates and equating the use of RSA with 2048 bits with 112 bits of security strength, the probability for a random attempt to succeed is: 1:2^{112} or 1: 5.19 x 10^{33} which 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 1 Gb/s. Hence, at most (1 ×10^{9} × 60 = 6 × 10^{10}) 60,000,000,000 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: 1: (2^{112} possible keys / ((6 × 10^{10} bits per minute) / 112 bits per key)) 1: (2^{112} possible keys / 535,714,285.7 keys per minute) 1: 9.69 × 1024 which is less than 1:100,000 within one minute as required by FIPS 140-2.
Ciena Device ID Public Key	The module supports ECDSA digital certificate authentication of COs and Users over the SecureMPL. Using conservative estimates and equating the use of ECDSA with P-521 elliptic curve to a 256-bit symmetric key, the probability for a random attempt to succeed is: 1:2^{256} or 1: 1.16 x 10^{77} which 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 1 Gb/s. Hence, at most 1 ×10^{9} × 60 = 6 × 10^{10} = 60,000,000,000 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: 1: (2^{256} possible keys / ((6 × 10^{10} bits per minute) / 256 bits per key)) 1: (2^{256} possible keys / 234,375,000 keys per minute) 1: 4.9 x 10^{68} which is less than 1:100,000 within one minute as required by FIPS 140-2.
Password-based	For HTTPS, SSH and Console the module enforces 8-character passwords (at minimum) chosen from the 96 human readable ASCII characters. The password can be a maximum of 128 characters.

	Based on the minimum password length, the probability for a random attempt to succeed is: 1:9^{68} or 1: 7.21 X 10^{15} Which is less than 1:1,000,000 as required by FIPS 140-2. A limit of 5 failed attempts is enforced by the module for SSH and HTTPS. Therefore, there can be at most 5:9^{68} attempts in a one-minute period, which is less than 1:100,000. For the Console, the probability of guessing a correct password is 1 in 7.21 x 10^{15}. Therefore the operator would have to make 60/(7.21 x 10^{15}) = 1.2 x 10^{14} attempts per second, which is beyond the operating capabilities of the module.

Table 5 - Authentication Mechanism

6. Physical Security

The physical boundary of the module can be seen in Figures 4 and 5 below. All CSPs are stored and protected within the WCS2 Module's components using the following physical security mechanisms, which provide opacity and tamper evidence:

The module is enclosed in a hard aluminum casing on the top and bottom of the PCB that is completely opaque within the visible spectrum.

The module uses three (3) tamper-evident labels to prevent the aluminum casings from being removed. They are applied at the factory; their locations can be seen in Figure 4.

Any attempt to remove the hard aluminum casing or tamper-evident labels will leave visual evidence of the attempt.

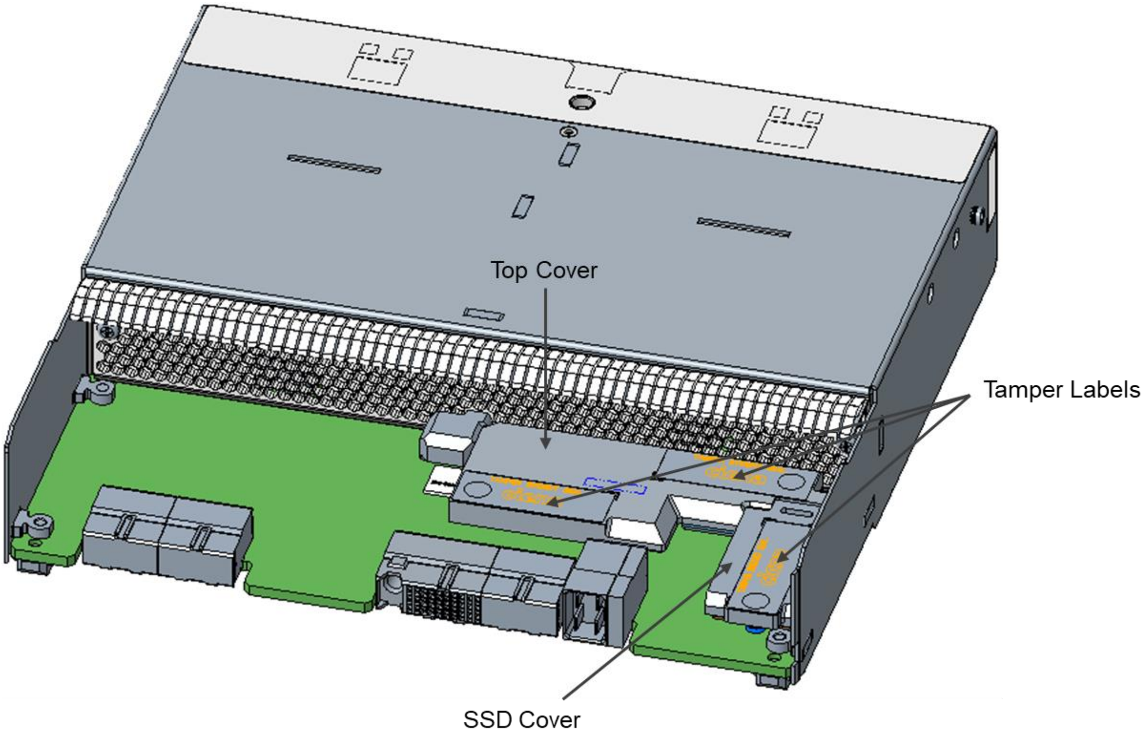

Figure 4- Top View with 3x Tamper Evident Label Locations

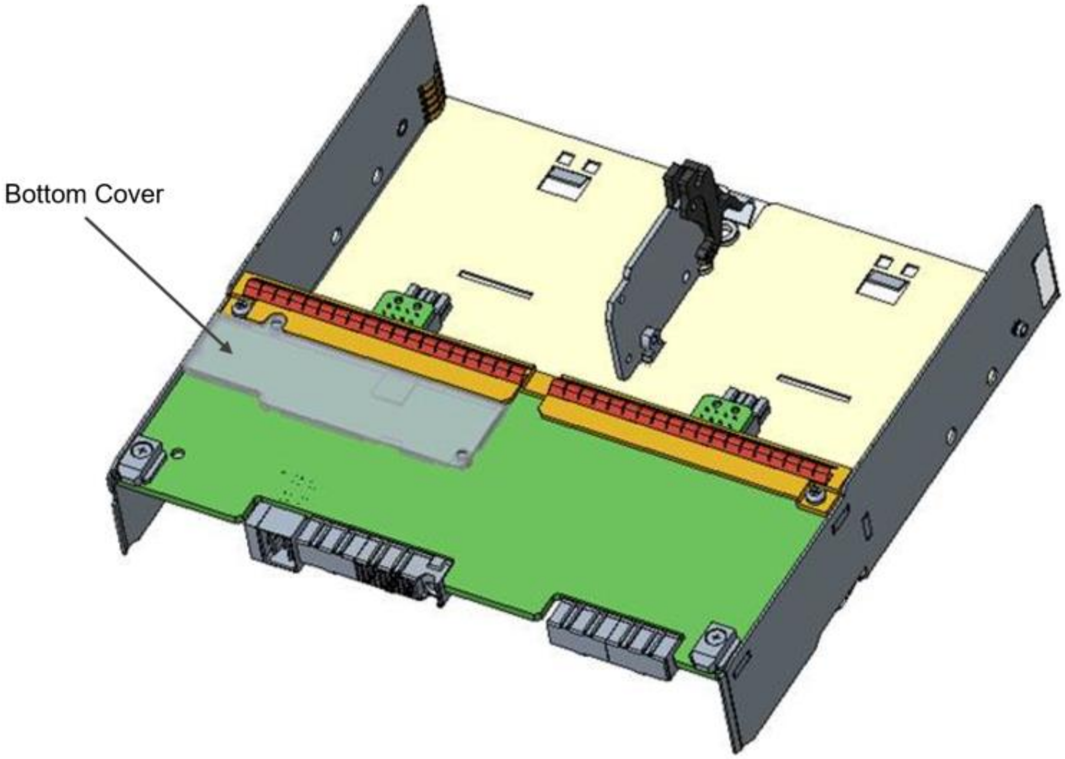

Figure 5 - Bottom View

7. Operational Environment

The operational environment of the WCS2 Module is considered a limited operational environment and does not provide the module operator access to a general-purpose operating system (OS).

All firmware downloads are digitally signed, and a conditional self-test (RSA signature verification) per Section 10.2 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.

8. Cryptographic Algorithms and Key Management

8.1 Cryptographic Algorithms

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

Xilinx CPU (Hardware Algorithm Implementation)					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
4438	AES KTS	256-bits	SP 800-38A FIPS 197 SP 800-38D	ECB, GCM	Encryption, Decryption, Authentication Key Transport per IG D.9

Table 6 – Xilinx CPU Hardware Implementation Algorithms

Crypto Library 1					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
C125	AES	256-bits	SP 800-38A FIPS 197 SP 800-38D	CBC	Encryption, Decryption
	DRBG	256-bits	SP 800-90Arev1	AES CTR_DRBG	Random Bit Generation
	HMAC	256	FIPS 198-1	HMAC-SHA-256	Message Authentication
	SHA	256	FIPS 180-4	SHA-256	Hashing, Keyed-Hash, Signature Generation, Signature Verification
Vendor Affirmed	CKG	N/A	SP 800-133	N/A	Key Generation

Table 7 – Crypto Library 1 Firmware Implementation Algorithms

Crypto Library 2					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
C193	AES	128, 256	SP 800-38A FIPS 197 SP 800-38D	CBC, GCM, CTR	Encryption, Decryption, Authentication
	DRBG	AES-128 and AES-256	SP 800-90A	CTR_DRBG	Random Bit Generation
	ECDSA	P-256, P-384, P-521	FIPS 186-4	PKG, PKV, Signature Generation using SHA-256, SHA-384 and SHA-512, Signature Verification using SHA-256, SHA-384 and SHA-512	Key Generation, Signature Generation, Signature Verification
	HMAC	256, 384, 512	FIPS 198-1	HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Message Authentication
	KAS	256, 384, 512	SP 800-56A	ECC component testing	Key Agreement
	KTS	AES-CBC 256 and HMAC-SHA-256	SP 800-38A FIPS 198-1	Symmetric Encryption with Approved Authentication	Key Transport per IG D.9
	KDF		SP 800-135	SSH KDF, TLS 1.2 KDF	Key Derivation
	RSA	2048, 3072, 4096	FIPS 186-4	Key Generation 2048 and 3072, Sig Gen PKCS 1.5 using mod 2048, 3072 and 4096 with SHA-256, SHA-384 and SHA-512 Signature Ver PKCS 1.5 using mod 2048 and 3072 with SHA-256, SHA-384 and SHA-512	Key Generation, Signature Generation, Signature Verification
	SHA	160, 256, 384, 512	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512	Hashing, Keyed-Hash, Signature Verification
Vendor Affirmed	CKG	N/A	SP 800-133	N/A	Key Generation

Table 8 - Crypto Library 2 Firmware Implementation Algorithms

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

Note: Additional algorithms were CAVP tested but are not being utilized by the module.

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)
- Elliptic Curve Diffie-Hellman with NIST-defined P-curves P-256, P-384 and P-521 for key agreement (CVL Cert. #C193, key agreement; key establishment methodology provides between 128 bits and 256 bits of encryption strength);

- Diffie-Hellman (CVL Cert. #C193, key agreement; key establishment methodology provides 112 bits of encryption strength); and
- RSA (key wrapping; key establishment methodology provides 112 bits or 128 bits of encryption strength).

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

- SNMPv2 and SNMPv3 is used for status output only. The SNMP implementation does not process sensitive information and is not being used to meet any FIPS 140-2 requirements.

8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 9:

Keys and CSPs	Use	CSP Type	Generation/Input	Output Method	Storage	Zeroization
Base Key Encryption Key (BKEK)	Used for decrypting the MKEK and Ciena Device ID	AES GCM 256-bit key	Preloaded at the factory	Never exits the module	Stored in plaintext in the CPU's non-readable, write once eFuse	N/A
Master Key Encryption Key (MKEK)	Used for encrypting or decrypting KEK and PKIX-KEK	AES GCM 256-bit key	Preloaded at the factory	Never exits the module	Stored encrypted with the BKEK in non-volatile memory	N/A
Key Encryption Key (KEK)	Used for encrypting the encryption card's PSK and the private key of the customer.	AES CBC 256-bit key	Initial value is preloaded at the factory and run-time values are generated internally	Never exits the module	Encrypted with MKEK and stored in non-volatile memory	Clear CSP
Public Key Infrastructure X.509 Key Encryption Key (PKIX-KEK)	Used for encrypting and decrypting the customer enrolled X.509 certificates	AES CBC 256-bit key	Initial value is preloaded at the factory and run-time values are generated internally	Never exits the module	Encrypted with MKEK and stored in non-volatile memory	Clear CSP
SecureMPL Encryption Key	Used for encryption/ decryption for SecureMPL	AES CBC 256-bit value	Derived from the EC DH shared secret during key establishment	Never exits the module	Stored in plaintext in RAM	Reboot or power removal
SecureMPL Integrity Key	Used for the integrity for SecureMPL	HMAC-SHA-256	Derived from the EC DH shared secret during key establishment	Never exits the module	Stored in plaintext in RAM	Reboot or power removal
SecureMPL EC DH Key Pair	Used for SecureMPL authentication	ECDSA P-256 with SHA-256	Generated internally during session negotiation	Public: exits in plaintext. Private: never exits the module	Stored in plaintext in RAM	Reboot or power removal

Keys and CSPs	Use	CSP Type	Generation/Input	Output Method	Storage	Zeroization
Ciena Device ID Key Pair	Used for end point authentication of SecureMPL	ECDSA P-521	Loaded at the factory	Public: exits in plaintext. Private: never exits the module	Read-Only. Stored encrypted in non-volatile memory with the BKEK	N/A
TLS Session Key	Used for encrypting/decrypting TLS messages	AES CBC, GCM 256-bit keys	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, or power removal
TLS Authentication Key	Used for authenticating TLS messages	HMAC SHA-256, HMAC-SHA-384	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, or power removal
TLS Pre-Master Secret	Establish the 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, or power removal
TLS Master Secret	Establish the TLS Session Key	384-bit random value	Generated internally during session negotiation	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, or power removal
SSH Session Authentication Key	It is used to authenticate all SSH data traffic between the SSH Client and SSH Server	HMAC-SHA-256, HMAC-SHA-512	Derived via key derivation function defined in SP 800-135 KDF (SSH)	Never exits the module	Stored in plaintext in RAM	By session termination, reboot, or power removal
SSH Encryption Key	It is used to encrypt all SSH data traffic between the SSH Client and SSH Server	AES CBC, AES-GCM, CTR256-bit keys	Derived via key derivation function defined in SP 800-135 KDF (SSH)	Exits in encrypted form during protocol handshake	Stored in plaintext in RAM	By session termination, reboot, or power removal
SSH Server Host Key	Used to identify the host	RSA 2048, 3072, 4096 ECDSA P-256, P-384, P-521	Generated internally using the Approved DRBG	Never exits the module	Stored in plaintext in RAM	By session termination, reboot or power removal
Module Web Access ECDSA Key Pair	Used with certificates in mutual authentication	ECDSA P-256, P-384, P-521	Either generated internally using the Approved DRBG or imported in encrypted form	Public: Never exits the module Private: Exits the module in encrypted form	Stored encrypted with KEK in non-volatile memory	Secure Erase
DH Key Pair	Public and Private keys used for establishing TLS/SSH sessions	DH Public: 2048-bit Private: 224-bit	Generated internally	Private: Never exits the module Public exits the module in plaintext;	Stored in plaintext in RAM	By session termination, reboot, or power removal

Keys and CSPs	Use	CSP Type	Generation/Input	Output Method	Storage	Zeroization
ECDH Key Pair	Public and Private keys used for establishing TLS/SSH sessions	ECDSA P-256, P-384 and P-521	Generated internally	Private: Never exits the module Public: Exits the module in plaintext	Stored in plaintext in RAM	By session termination, reboot, or power removal
DRBG Seed	Used for random number generation	384-bit value	Generated internally using entropy input	Never exits the module	Stored in plaintext in RAM	By reboot or power removal
Entropy Input	Used for random number generation	512-bit value	Generated internally using NDRNG	Never exits the module	Stored in plaintext in RAM	By power removal
DP Customer Enrollment Certificate	Used for remote device peer authentication	ECDSA P-256, P-384, P-521	Input encrypted via SFTP/SCP	Never exits the module	Stored encrypted with KEK in non-volatile memory	Clear CSP
Customer Enrollment Certificate	Used to establish identity prior to a TLS session (RADIUS and Syslog)	RSA 2048, 3072, 4096 ECDSA P-256, P-384, P-521	Input encrypted via SFTP/SCP	Never exits the module	Stored encrypted with PKIX-KEK in non-volatile memory	Secure Erase
Customer Enrollment Pre-Shared Key	Used for remote device and peer authentication	128 – 2048 bit string	Input encrypted via SFTP/SCP	Never exits the module	Stored encrypted with KEK in non-volatile memory	Secure Erase
Password	Used to authenticate the CO and User	8 – 128 characters	Input by the operator	N/A	Stored in plaintext in non-volatile memory.	Secure Erase

Table 9 – Approved Keys and CSPs Table

No parts of the TLS or protocols other than the KDF, have been tested by the CAVP and CMVP per FIPS 140-2 IG D.11.

8.3 Key Generation and Entropy

The module generates keys as described in SP 800-133 Section 5, Option #1. It uses a FIPS-Approved CTR_DRBG (as specified in SP 800-90A) to generate cryptographic keys, RSA and ECDSA key pairs. The DRBG is seeded from seeding material provided by a hardware-based NDRNG, which provides an entropy source and whitening circuitry to supply a uniformly-distributed unbiased random sequence of bits to the DRBG.

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. A total of 512-bits of entropy is requested by the module. From this 384-bits is used as direct input into the module's Approved DRBG.

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

All ephemeral keys used by the module are zeroized on reboot, loss of power or session termination. The "Clear CSP (Critical Security Parameter)" command also allows an operator to clear certificates' public keys, private keys, and the KEK. The BKEK, MKEK and KEK CSPs reside in non-volatile memory.

The other CSPs are stored in the volatile and non-volatile memories of the module. The zeroization of the KEK, which encrypts all other CSPs, renders all the other CSPs stored in non-volatile memory 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 firmware load image files cannot be zeroized.

Secure Erase (RTFD) provides a means to securely remove all sensitive configuration data from the module's SSD storage (e.g. IP address, hostname, user names, user passwords, Pre-Shared Keys, Certificates, KEK and PKIX-KEK. Etc) before it gets de-commissioned (e.g. return to Ciena for RMA). The module shall reset all user provisioned datapath encryption parameters to default values if the user performs a RTFD operation.

9. EMI/EMC

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

10. 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.

10.1 Power-On Self-Tests

The Ciena WCS2 Module performs the following self-test at power-up to verify the integrity of the firmware images and the correct operation of the FIPS-Approved algorithms implemented in the module:

Type	Test Description
Integrity Test	• Firmware image (Zone A) EDC Integrity Test using SHA-384 • Firmware image (Zone B) EDC Integrity Test using SHA-384
Xilinx CPU Known Answer Tests	• AES GCM Encryption KAT • AES GCM Decryption KAT

Crypto Library 1 Known Answer Tests	• AES CBC Encryption KAT • AES CBC Decryption KAT • SHA-256 KAT • HMAC SHA-256 KAT • SP 800-90A CTR_DRBG KAT
Crypto Library 2 Known Answer Tests	• AES CBC Encryption KAT • AES CBC Decryption KAT • AES GCM Encryption KAT • AES GCM Decryption KAT • SP 800-90A CTR_DRBG KAT • SHA-1 KAT • SHA-256 KAT • SHA-384 KAT • SHA-512 KAT • HMAC-SHA-256 KAT • HMAC-SHA-384 KAT • HMAC-SHA-512 KAT • RSA Sign/Verify KATs • ECDSA Sign/Verify KATs • Diffie-Hellman Primitive Z Computation KAT • EC Diffie-Hellman Primitive Z Computation KAT

Table 10- 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 power-cycling the module.

10.2 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
Continuous RNG Tests on Entropy Input	• Performed on entropy input provided to the SP 800-90A CTR_DRBG
ECDSA Pairwise Continuous Test	• Performed on ECDSA Key generation
RSA Pairwise Continuous Test	• Performed on RSA Key generation
Firmware Load Test	• RSA 4096-bit Signature Verification operation performed prior to a firmware upgrade.

Table 11 – Conditional Self-tests

10.3 Critical Function Tests

Each of the module's DRBGs perform the following critical function tests:

Type	Test Description
DRBG Health Tests	• Performed on DRBG, per SP 800-90A Section 11.3. Required per IG C.1.

Table 12 – Critical Function Tests

10.4 Self-Test Failure Handling

Upon the failure of any power-up self-test (except the Zone A firmware Integrity test or Zone B firmware integrity test), conditional self-test (except the firmware load tests), or critical functions tests, the module goes into “Critical Error” state and disables all access to cryptographic functions and CSPs. A permanent error status will be relayed via the status output interface, which then raises an alarm and adds an entry to the system 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 the Zone A Soft Error state where it will proceed with the Zone B firmware integrity test.

If the Zone B firmware integrity check fails, the module transitions to the Critical Error state (if the Zone A firmware integrity check also failed).

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.

In the case of a firmware integrity failure in both Zone A and Zone B, the module will not be able to resume normal operation and the Crypto Officer should contact Ciena.

11. Mitigation of Other Attacks

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

12. Guidance and Secure Operation

The WCS2 Module meets Level 2 requirements for FIPS 140-2. The following sections describe how to place and keep the module in the FIPS-Approved mode of operation.

12.1 Delivery of the Module

The WCS-2 is shipped as part of the Waveserver Ai circuit pack. The module is always delivered via commercial bounded carrier. The shipment will contain a packing slip with the serial numbers of all shipped devices. Prior to deployment the receiver shall verify that the hardware serial numbers match the serial numbers listed in the packing slip.

12.2 Initial Setup

The 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 CO or the User can perform the Secure Operation responsibilities and tasks listed here; however, this Security Policy places this responsibility solely on the CO.

The module is shipped from the factory with the required physical security mechanisms (tamper-evident labels, metal covers and PCB layers) installed. The CO must perform a physical inspection of the unit for signs of damage and to ensure that all physical security mechanisms are in place. Additionally, the CO should check the package for any irregular tears or openings. If damage is found or tampering is suspected, the CO should immediately contact Ciena.

12.3 Secure Management

The CO is responsible for configuring, 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.

The CO is responsible for the configuration the module, which includes configuring the Datapath parameters and certificates. The CO must:

- Configure a password for the default account. The CO can optionally create additional accounts.
- All operator passwords must be a minimum of 8 characters in length.
- Install the web server certificate and at least one CA certificate for the module to be able to verify the submitted CO and User ECDSA Public Keys during HTTPS mutual authentication.
- Ensure use of FIPS-approved algorithms for TLS:

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
```

- Ensure all management traffic is encapsulated within a trusted session
- For SSH, ensure Group 14 or stronger is selected for Diffie-Hellman
- Install the PSK or X.509 certificate authentication material
- Set up Syslog (over TLS) and RADIUS over TLS

- Either local or RADIUS over TLS shall be used for user authentication purposes. TACACS+ and plaintext RADIUS shall not be used in the FIPS Approved mode.
- The system server GRPC shall be disabled.
- The configuration shall be saved once completed

When configured according to the CO guidance in this Security Policy, the module only runs in a FIPS Approved mode of operation. The Crypto Officer should monitor the module's status regularly. The CO can monitor and configure the module via the console port or SSH. The module will operate in FIPS-Approved mode of operation until it is decommissioned by the CO or the physical security is breached. Detailed instructions for monitoring and troubleshooting the module are provided in the Ciena's *User's Guide and Technical Practices* document.

12.3.1 Usage of AES-GCM in the Waveserver Ai WCS-2 Cryptographic Module

The module supports multiple implementations of GCM, all of which comply with a scenario in FIPS 140-2 IG A.5. The module's BKEK GCM key is used for decryption only therefore it does not need to comply to the IV generation/construction requirements.

For the TLS Session GCM key, the key and IV generation conform to IG A.5 scenario #1 following RFC 5288 for TLS. 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.

The module's Xilinx CPU Hardware AES-GCM implementation conforms to IG A.5 scenario #2. The IVs are generated randomly by an internal Approved DRBG. The MKEK IV used for Datapath Encryption uses the Crypto Library 1 DRBG (Cert. #C125). The MKEK IV used for Certificate management uses the Crypto Library 2 DRBG (Cert. #C193). Both DRBGs are seeded by the internal NDRNG.

For the GCM key used for the SSH Encryption Key, it is only used as part of the SSHv2 cipher suites conformant to the Draft IG A.5 and RFCs 4252, 4253 and RFC 5647. When the invocation counter reaches its maximum value 2^{64} -1 the next AES GCM encryption is performed with the invocation counter set to 1. A counter is set so that no more than 2^{64}-1 AES GCM encryptions may be performed in the same session. When a session is terminated for any reason, a new key and new initial IV shall be derived.

In each of the use cases above, if the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

12.4 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 inspect the module for evidence of tampering at six-month intervals. The CO shall visually inspect the tamper-evident labels for tears, rips, dissolved adhesive, and other signs of tampering. The CO shall also inspect the PCB, the enclosure, and tamper-evident labels 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.

12.5 User Guidance

The User shall follow all the instructions and guidelines provided for the Crypto Officer in Section 12 of this Security Policy document to ensure the secure operation of the module.

12.6 SecureMPL Protocol

The MPL is a communication layer protocol servicing Waveserver application needs for message exchange in-process (between threads), inter-process (within the same module) and process between modules. The Secure MPL layer was introduced to facilitate privacy and data security communication needs between WCS2 and Encryption Card through the midplane. For example, Secure MPL is used for the secure transport of customer enrolled Datapath Encryption authentication materials from WCS2 module to Encryption module.

13. Glossary

Term	Description
AES	Advanced Encryption Standard
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CRL	Certificate Revocation List
CRNGT	Continuous Random Number Generator Test
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter
DH	Diffie-Hellman
DRAM	Dynamic Random-Access Memory
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
FPGA	Field Programable Gate Array
GCM	Galois/Counter Mode
GRPC	gRPC Remote Procedure Call
HMAC	(Keyed) Hashed Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IG	Implementation Guidance
I/O	Input/Output
IV	Initialization vector
KAT	Known answer test
KDF	Key-Derivation Function
KEK	Key Encrypting Key
MKEK	Master Key Encrypting Key
NIST	National Institute of Standards and Technology
NDRNG	Non-Deterministic Random Number Generator
OS	Operating System
PCB	Printed Circuit Board
PCT	Pairwise Consistency Test
PKCS	Public-Key Cryptography Standard
PKG	Public Key Generation
PKV	Public Key Validity
PSK	Pre-Shared Key
RAM	Random Access Memory

Term	Description
RMA	Return Material Authorization
RSA	Rivest Shamir Adleman
RTFD	Return To Factory Default
SGMII	Serial Gigabit Media Independent Interface
SHA	Secure Hash Algorithm
SSD	Solid State Drive

Table 13 - Glossary of Terms