FIPS 140-2 Non-Proprietary Security Policy

Ciena® Corporation

Ciena Waveserver Ai Encryption Module

Hardware version: 186-1606-820-EB, Revision 003 with PCB P/N: 174-0534-220 Revision 002 or PCB P/N: 174-0534-222 Revision 001

Firmware version: 1.3.5, 1.3.6 or 1.3.61

And

Hardware version: 186-1606-820-EB, Revision 003 with PCB P/N: 174-0534-221 Revision 001 or PCB P/N: 174-0534-223 Revision 001

Firmware version: 1.3.6 or 1.3.61

Date: 07/29/2020

Prepared for:

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 Communications Security Establishment Canada (CSE) 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/index.html

About this Document

This non-proprietary Cryptographic Module Security Policy for Ciena Waveserver Ai Encryption 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 Encryption Module 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. 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 Encryption Module, Hardware version: 186-1606-820-EB, Revision 003 with PCB P/N: 174-0534-220 Revision 002 or PCB P/N: 174-0534-222 Revision 001 with firmware version 1.3.5, 1.3.6 or 1.3.61 and Hardware version: 186-1606-820-EB, Revision 003 with PCB P/N: 174-0534-221 Revision 001 or PCB P/N: 174-0534-223 Revision 001 with firmware version 1.3.6 or 1.3.61 (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

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

The Waveserver Ai Encryption Module is implemented as components on a Waveserver Ai Encryption circuit pack. It is the physical security boundary and is composed of FPGA, processor, DDR4 (DRAM), 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). All traffic entering and exiting the module is encrypted/decrypted at wire speed (100Gb/s, 200Gb/s, 300Gb/s and 400Gb/s depending on line modulation scheme selected) using AES-256 GCM mode. The module provides fully secure cryptographic functionality, including peer authentication, key derivation, datapath encryption, physical security, and identification and authentication of the module's Crypto Officer (CO) and User.

This module is configured and provisioned by the directly connected Waveserver Ai WCS-2 module over the mid-plane connector.

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	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	3
Mitigation of Other Attacks	N/A
Overall Level	2

Table 1 - Security Level

3. Cryptographic Module Specification

3.1 Cryptographic Boundary

The Waveserver Ai Encryption Module is a hardware module with a multiple-chip embedded embodiment. The module consists of two primary components: a Xilinx Zynq Ultrascale+ processor and an FPGA enclosed in a tamper-proof enclosure. These two components communicate via wire connections embedded beneath multiple PCB layers. The module also contains integrated circuits, Dynamic Random-Access Memory (DRAM), and flash memories (NOR and eMMC). The module Datapath FPGA supports 400Gbps wire speed AES 256-bit GCM encryption. Once the circuit pack is booted up, traffic on the line side is either encrypted or squelched. This module is plugged into a Waveserver Ai slot 1, 2 or 3. The client interface supported is 100GE.

The overall security level of the module is 2. The cryptographic boundary of the Waveserver Ai Encryption Module surrounds the processor, FPGA and memory components described above. The portion of the PCB under which the connecting wire traces are embedded, and all physical security mechanisms described in Section 6.

The module as it appears on the circuit pack can be seen in Figure 1 and Figure 2, while Figure 3 is the FPGA ball grid. Figure 4 provides the module's block diagram. Both figures 1 and 2 surround the module's cryptographic boundary with a dotted blue line.

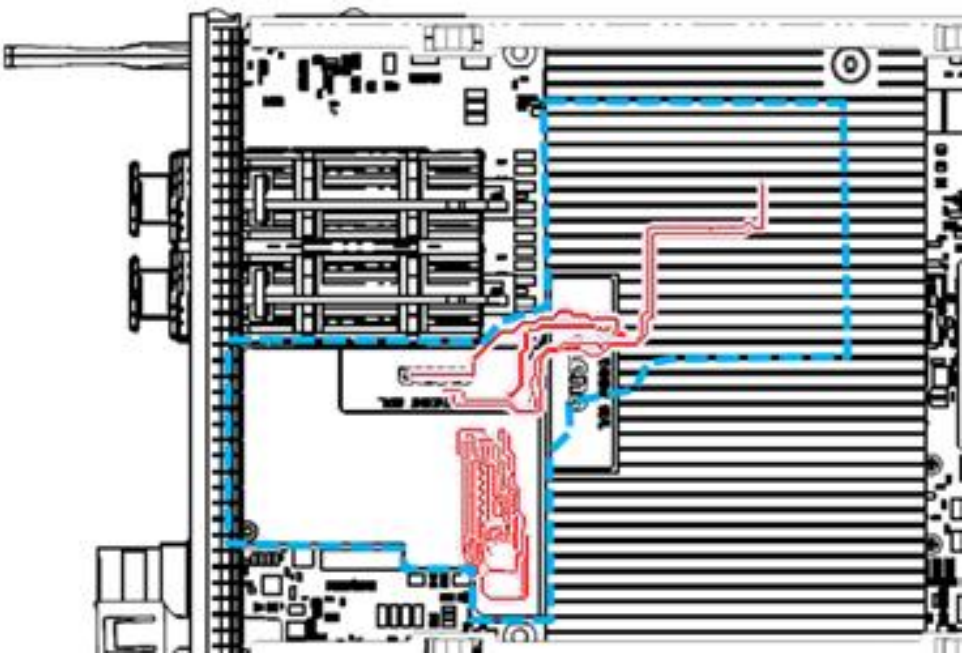

Figure 1- Top of the Module

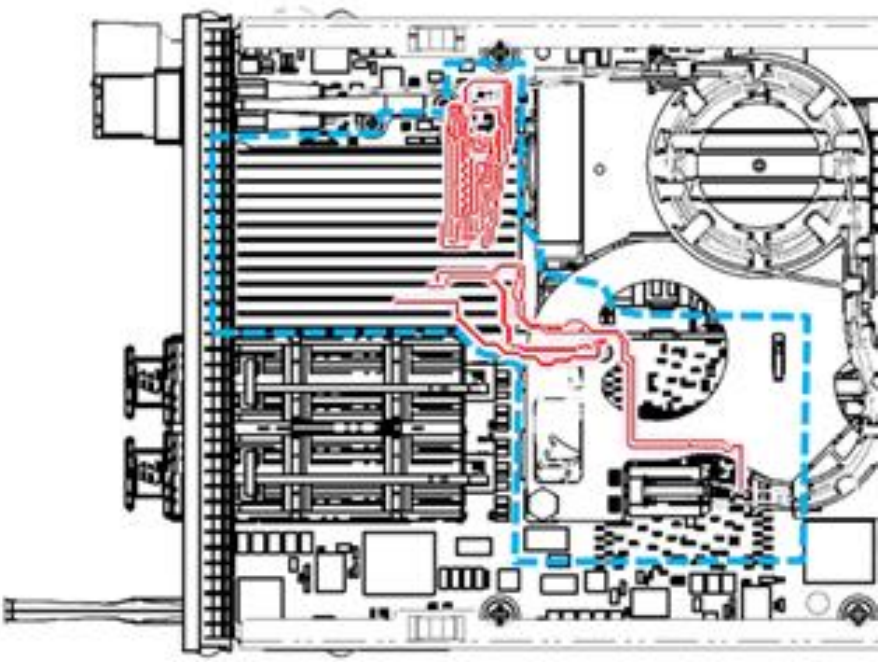

Figure 2 - Bottom of the Module

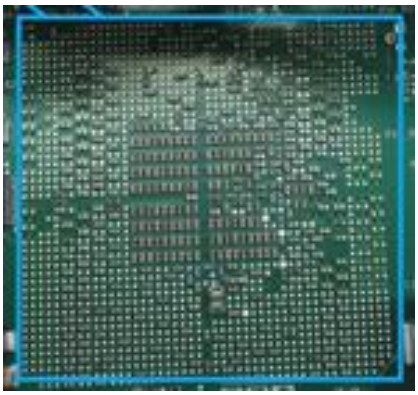

Figure 3 - Bottom of module with FPGA Ball Grid shown

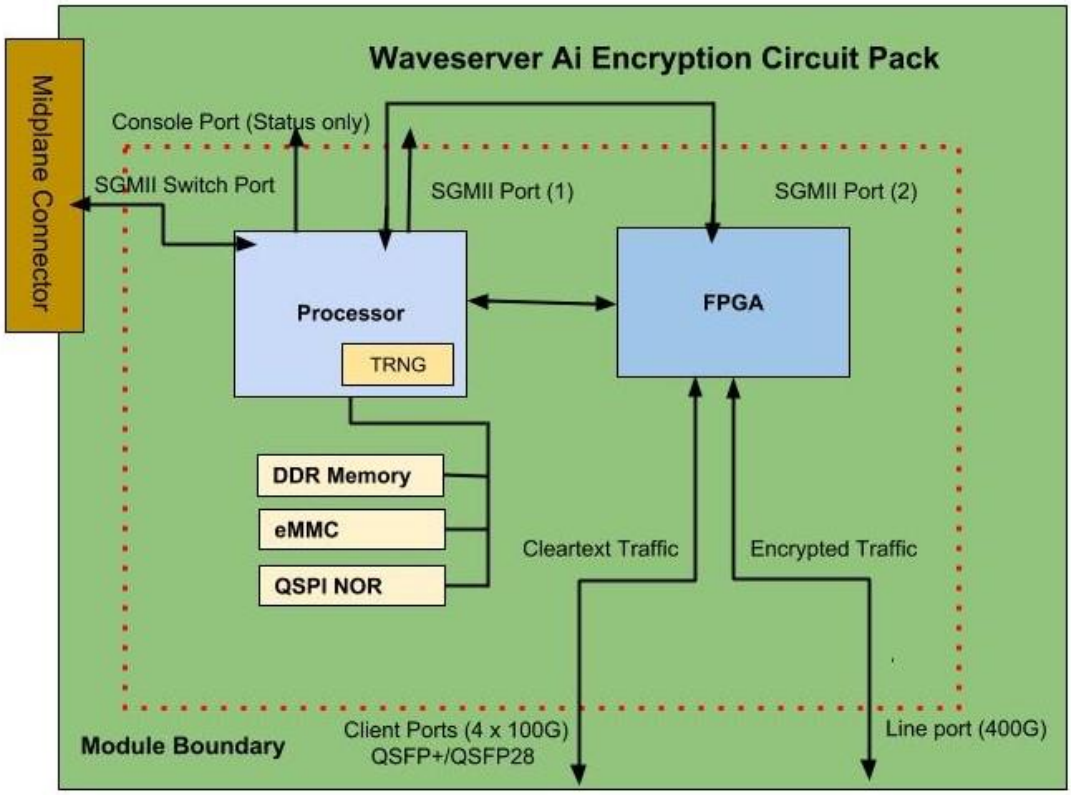

Figure 4 - Waveserver Encryption Module Block Diagram

4. Cryptographic Module Ports and Interfaces

The module provides the following number of physical and logical interfaces to the host circuit pack, 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 host circuit pack.
The physical ports and interfaces of the Waveserver Ai Encryption Module consist of the midplane connector (which directly connects to the WCS-2 Cryptographic Module), an FPGA ball grid and SGMI interface. An optical connector is directly attached to the FPGA pins of the module.

Table 2 lists the physical ports and interfaces available in the Waveserver Ai Encryption Module and provides the mapping from the physical ports and interfaces to logical interfaces as defined by FIPS 140-2. Interfaces are provided by both the Processor and FPGA. Note that the FPGA ball grid pins are categorized into the following groupings (with associated pin counts):

- Client Data In (Clear Text) (32 pins)
- Backplane Data Out (Clear Text) (33 pins)
- Line Data In (Encrypted) (32 pins)
- Line Data Out (Encrypted) (32 pins)
- Control In (40 pins)
- Status Out (8 pins)
- Power In (360 pins)

The FPGA also includes the following pin groupings that, based upon their purpose, are not mapped into the FIPS logical interface categories:

- General Purpose I/O pins (provide interfaces for pre-installation scan testing; unused once installed)
- Internal Control/Status I/O pins (provide internal interfaces between module components)
- Unused pins
- Clock Pins
- Ground pins

The logical interfaces and their mappings are described in the following table:

Physical Port	FIPS 140-2 Logical Interface Mapping
Midplane connector (SGMII Switch Port)	Data Input and Output Interface Status Output Interface Control Input Interface
Line Port (400G)	Data Input and Data Output Interface
SGMII Port (1)	Data Input and Data Output Interface Status Output Interface Control Input Interface
SGMII Port (2)	Data Input and Output Interface
Console Port	Status Output Interface[1]
Power	Power 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 role is 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 the role-based authentication methods in section 5.3.

Operators explicitly assume both the CO and User role. The WCS-2 cryptographic module assumes the CO role. As the CO, the WCS-2 authenticates to the module via the midplane interface and can perform security provisioning.

The data plane communications are defined as the User role services. The User role authenticates via peer authentication using a Pre-Shared Key or a X.509 certificate. More information on the authentication mechanisms is provided below in Section 5.3.

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.

[1] Only non-security relevant status information can be obtained from the console port

5.2 Services

The module provides the following Approved services which utilize algorithms listed in Tables 6, 7, 8 and 9:

Please note that the keys and Critical Security Parameters (CSPs) listed in Table 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.

Service	User	Crypto Officer	Description	Input	Output	CSP and Type of Access
Initialize the module		✓	Initialize the module	Command	Status output	BKEK (X); DEK (R/W/X);
Configure/Manage the Module		✓	Configure settings and import certificates or Pre-Shared Keys via SecureMPL	Command and parameters	Command response	Ciena Device ID (R/X); SecureMPL CSPs (R/W/X);
Monitor Alarms (Show status)		✓	Monitor the configuration of the module over the MPL interface	Command	Status output	Ciena Device ID (R/X); SecureMPL CSPs (R/W/X);
Zeroize		✓	Power Cycle or issue ClearCSP	Command	Command Response	Please see the 'Zeroization' column in Table 10 below
Datapath Encryption/ Decryption Service	✓		Encrypt or decrypt customer traffic	Parameters	Status Output	DEK (R/X) IKEv2 CSPs (R/W/X);
Upgrade Application Firmware		✓	Upgrade the application firmware using the RSA signature verification	Command and parameters	Command 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	Command	Status output	Ciena Device ID (R/X) SecureMPL CSPs (R/X);
Perform peer authentication	Authenticate peer devices to the module	Command	Status output	DP Customer Enrolled Certificate (R/X) DP Customer Enrollment PSK (R/X)

Monitor Alarms (Show status)	Obtain non-security relevant status over the console port	N/A	Status Output	N/A
Perform Data Path Encryption Peer Authentication	Authenticate peer device for the purposes of data path encryption	Command	Status output	IKEv2 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

Table 4 – Additional Services

5.3 Authentication

The module supports role-based authentication. Module operators must authenticate to the module before being allowed access to services that require the assumption of an authorized role.

The CO authenticates to the module from the WCS-2 module using the SecureMPL protocol. The SecureMPL uses an ECDSA (P-521) public key.

For User authentication, the module can be configured to use either a Pre-Shared Key or X.509 Certificate. Once authentication type has been configured, all 100G plane connections will only utilize it. The default authentication type for the module is to use a Pre-Shared Key.

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

Authentication Type	Strength
DP Customer Enrolled Certificate	The module supports ECDSA P-256, P-384 and P-521 digital certificate authentication of Users for Datapath Encryption. Using conservative estimates and equating the use of ECDSA P-256 bit certificate to 128 bits of security, the probability for a random attempt to succeed is: $1{:}2^{128}$ or 1: 3.4×10^{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 $1 \times 10^9 \times 60 = 6 \times 10^{10}$ = 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: 5.19×10^{33} which is less than 1:100,000 within one minute as required by FIPS 140-2.
DP Customer Enrollment Pre-Shared Key (PSK)	The module supports the use of a Pre-Shared key for Datapath Encryption peer authentication for Users over IKEv2. The Pre-Shared key can be between 128 bits and 2048 bits. Using conservative estimates, the probability for a random attempt to succeed is: *$1{:}2^{128}$ or 1: 3.4×10^{38}* which is less than 1:1,000,000 (as required by FIPS 140-2). The communication channel used for peer authentication has a hardware limit 13Mbits/sec. The software driver implementation and IKEv2 protocol will further slow down the actual processing rate. Hence, at most $13 \times 10^6 \times 60 = 7.8 \times 10^8$ = 780,000,000 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/ (7.8 x 10^8 bits per minute)/128 bits per key)) 1: (2^{128} possible keys/ 6,093,750 keys per minute) 1: 5.6 x 10^{31} which is less than 1:100,000 within one minute as required by FIPS 140-2. 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 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 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^{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 × 10^{68} which is less than 1:100,000 within one minute as required by FIPS 140-2.

Table 5 - Authentication Mechanisms

6. Physical Security

All CSPs are stored and protected within the Ciena Waveserver Ai Encryption Module's components using the following physical security mechanisms, which provide opacity and tamper evidence:

- The wire connections are embedded beneath multiple layers of the PCB, preventing visual access. Any attempts to access or tamper with the embedded wires will damage the PCB layers, leaving visual evidence of the attempt.
- Module CPU and memory components are enclosed in a hard aluminum clam shell (part number 410-8040-001 and 410-8041-001) that is completely opaque within the visible spectrum.
- Tamper evident labels are applied at the factory; their locations can be seen in Figure 5. Any attempt to remove the tamper-evident labels will leave visual evidence of the attempt.
- The FPGA is mounted on the motherboard's PCB and covered by a heatsink (part number 410-8031-001) preventing any visibility of the component.
- The heatsink and clam shell are affixed to the PCB using screws which are protected using a tamper-evident labels (part number 415-2424-001) as shown in Figure 5. The tamper-evident label on the heatsink is placed on a label plate (part number 410-8039-001) which is screwed to the heat sink and PCB. Any attempt to defeat these mechanisms will result in physical damage to the module.

After installation, the module should be inspected for evidence of tampering at six month intervals. The metal casings shall be inspected for any signs of tampering. Also, the tamper-evident labels shall be inspected for tears, rips, dissolved adhesive, or other signs of interference. If you evidence of tampering is found, contact Ciena immediately.

7. Operational Environment

The operational environment of the Encryption 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) is performed during each download. If the signature test fails, the new module firmware is ignored, and the current firmware remains loaded. Only the firmware version on this certificate 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 ARM 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 ARM CPU Hardware Algorithm Implementation

FPGA Datapath Cipher (Hardware Algorithm Implementation)					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
C120	AES KTS	256-bits	SP 800-38A FIPS 197 SP 800-38D	ECB, GCM	Encryption, Decryption, Authentication Key Transport per IG D.9

Table 7 – FPGA Datapath Cipher Hardware Implementation Algorithms

FW Crypto Library 1					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
C122	AES KTS	256-bits	SP 800-38A FIPS 197 SP 800-38D	CBC, GCM	Encryption, Decryption, Authentication Key Transport per IG D.9
	CKG (Vendor Affirmed)	N/A	SP 800-133		Key Generation
	DRBG	256-bits	SP 800-90Arev1	AES CTR_DRBG	Random Bit Generation
	ECDSA	P-256, P-384, P-521	FIPS 186-4	PKV, Signature Generation (SHA-256, SHA-384, SHA-512), Signature Verification (SHA-256, SHA-384, SHA-512)	Signature Generation, Signature Verification
	HMAC	384 bits	FIPS 198-1	HMAC-SHA-384	Message Authentication
	KDF		SP 800-135	IKEv2 KDF	Key Derivation
	SHA	256, 384, 512 bits	FIPS 180-4	SHA-256, SHA-384, SHA-256	Hashing, Keyed-Hash, Signature Generation, Signature Verification

Table 8 – FW Crypto Library 1 Firmware Implementation Algorithms

FW Crypto Library 2					
CAVP Cert #	Algorithm	Sizes	Standard	Mode/Method	Use
C186	AES	256 bits	SP 800-38A FIPS 197 SP 800-38D	CBC, CTR	Encryption, Decryption, Authentication
	CKG (Vendor Affirmed)	N/A	SP 800-133		Key Generation
	DRBG	AES-256	SP 800-90Arev1	CTR_DRBG	Random Bit Generation
	ECDSA	P-521	FIPS 186-4	PKV, Signature Generation (SHA-256, SHA-384, SHA-512), Signature Verification (SHA-1, SHA-256, SHA-384, SHA-512)	Signature Generation, Signature Verification
	HMAC	SHA-256	FIPS 198-1	HMAC-SHA-256	Message Authentication
	RSA	2048, 3072 and 4096-bits[2]	FIPS 186-4	Sig Gen PKCS 1.5 (2048, 3072 and 4096 with SHA-256, SHA-384, SHA-512), Sig Ver PKCS 1.5 (2048, 3072 with SHA-256, SHA-384, SHA-512)	Signature Generation, Signature Verification
	SHA	160, 256 and 512 bits	FIPS 180-4	SHA-1, SHA-256 and SHA-512	Hashing, Keyed-Hash, Signature Generation, Signature Verification

Table 9 – FW Crypto Library 2 Firmware Implementation Algorithms

NOTE: The IKEv2 protocol has not been reviewed or tested by the CAVP or CMVP.

NOTE: Additional algorithms, modes and keys sizes 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. #C122, key agreement; key establishment methodology provides between 128 bits and 256 bits of encryption strength)

[2] Only 4096-bit is used by the module however CAVP testing is only available for 2048-bit and 3072-bit RSA sizes

8.2 Cryptographic Key Management

The module supports the following CSPs listed below in Table 10:

Keys and CSPs	Use	CSP Type	Generation/ Input	Output Method	Storage	Zeroization
Base Key Encryption Key (BKEK)	Used for decrypting the Ciena Device ID	AES GCM 256-bit key	Preloaded at the factory	Never exits the module	Stored in plaintext in the CPUs non-readable, write once eFuse	N/A
Data Encryption Key (DEK)	Used for encryption /decryption of payload data between an authorized external entity and the module	AES GCM 256-bit key	Generated internally during IKEv2 negotiation	Never exits the module	Stored plaintext in RAM during key derivation	Zeroized by reboot or power removal once the key is programmed into HW cipher
SecureMPL Encryption Key	Used for encryption of SecureMPL session	AES CBC 256-bit value	Key is derived from the EC DH shared secret during key establishment	Never exits the module	Stored in plaintext in volatile memory	Reboot or power removal
SecureMPL Integrity Key	Used for the authentication of the SecureMPL session	HMAC-SHA-256	Key is derived from the EC DH shared secret during key establishment	Never exits the module	Stored in plaintext in volatile memory	Reboot or power removal
SecureMPL EC DH Key Pair	Components used for EC DH key exchange	P-256 with SHA-256	Generated internally	Public exits in plaintext. Private never exits the module	Stored in plaintext in volatile memory	Reboot or power removal
Ciena Device ID Key Pair	Used for SecureMPL authentication	ECDSA P-521	Loaded at the factory	Public exits in plaintext. Private never exits the module.	Read-Only. Stored encrypted in non-volatile memory.	N/A
DP Customer Enrolled Certificate	Used for remote device peer authentication	ECDSA P-256, P-384 and P-521	Input encrypted via SecureMPL	Never exits the module	Stored in plaintext in RAM	Zeroized by “Clear CSP” command coming from the WCS-2, reboot or power removal
DP Customer Enrollment Pre-	Used for remote device	128 – 2048-bit string	Input encrypted via SecureMPL	Never exits the module	Stored in plaintext in RAM	Zeroized by “Clear CSP”

Keys and CSPs	Use	CSP Type	Generation/ Input	Output Method	Storage	Zeroization
Shared Key (PSK)	peer authentication					command from the WCS-2, reboot or power removal
IKEv2 EC DH Key Pair	Used for exchanging shared secret to derive session keys during IKEv2	384-bit value	Private: Generated internally during IKEv2 negotiation For the public component of the module: generated internally during IKEv2 negotiation For the public component of a peer: generated externally and enters the module in plaintext	Private: Never exits the module For the public component of the module: exits the module in plaintext For the public component of a peer: never exits the module	Stored in plaintext in RAM	By session termination, reboot or power removal
IKEv2 Session Encryption Key	Used with AES-GCM for encrypting/ decrypting IKEv2 messages	AES GCM 256-bit key	Generated internally	Never exits the module	Stored in plaintext in RAM	By session termination, reboot or power removal
IKEv2 Session Authentication Key	Used for authenticating IKEv2 messages	HMAC SHA-384	Generated internally	Never exits the module	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

Table 10 - Approved Keys and CSPs Table

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. 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 allows an operator to clear the DP Customer Enrollment Pre-Shared Key and DP Customer Enrolled Certificate. The BKEK CSP resides in non-volatile memory.

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.

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

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 in the Cryptographic 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 ARM CPU Known Answer Tests	• AES GCM Encryption KAT • AES GCM Decryption KAT
Known Answer Tests for FPGA Datapath Cipher (hardware)	• AES ECB Encryption KAT • AES ECB Decryption KAT • AES GCM Encryption KAT • AES GCM Decryption KAT
Known Answer Tests for FW Crypto Library 1 (firmware)	• AES GCM Encryption KAT • AES GCM Decryption KAT • SP 800-90A CTR DRBG KAT • SHA-256 KAT • SHA-384 KAT • SHA-512 KAT • HMAC-SHA-384 KAT • ECDSA Sign/Verify KAT • EC Diffie-Hellman Primitive Z Computation KAT
Known Answer Tests for FW Crypto Library 2 (firmware)	• AES CBC Encryption KAT • AES CBC Decryption KAT • SP 800-90A CTR-DRBG KAT • SHA-1 KAT • SHA-256 KAT • SHA-512 KAT • HMAC-SHA-256 KAT • ECDSA Sign/Verify KAT • RSA Sign/Verify KAT • EC Diffie-Hellman Primitive Z Computation KAT

Table 11 - 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 test that run during operation of the module. Each module performs the following conditional self-tests:

Type	Test Description
Continuous RNG Tests on Entropy Input for the SP 800-90A CTR_DRBG	• Performed on entropy input
DRBG Health Tests	• Performed on DRBG, per SP 800-90A Section 11.3
Firmware Load Test	• RSA 4096-bit Signature Verification operation performed prior to a firmware upgrade.

Table 12 - 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 13 – Critical Function Tests

10.4 Self-Test Failure Handling

Upon the failure of any power-up self-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. All data outputs via data output interfaces are inhibited upon any self-test failure. The Encryption module will report this error condition to WCS-2 which then generates an alarm to the end customer to indicate Cryptographic Algorithm Self-Test Failure.

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.

The module requires rebooting or power-cycling to come out of the error state and resume normal operations. In the case of a firmware load corruption that cannot be corrected via the SecureMPL, 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 Encryption Module Meets Level 2 requirements for FIPS 140-2. The following sections describe how to place and keep the module in FIPS-Approved mode of operation.

12.1 Delivery of the Module

The module is always delivered via commercial bounded carrier. The module 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 host circuit pack from the factory. The CO can perform the Secure Operation responsibilities and tasks listed here.

The module is shipped from the factory with the required physical security mechanisms (tamper-evident labels, heatsink, and PCB layers etc) installed. After removing the circuit pack from the shipping package, but prior to use, the CO must perform a physical inspection of the unit for signs of damage. The CO must 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.

The module is contained in a strong, hard metal enclosure, and is protected by two tamper-evident labels. The wire connections between the Xilinx Zynq Ultrascale+ ARM processor and Datapath FPGA are protected from view and from tampering by multiple PCB layers. The bottom of the PCB where the Xilinx Zynq Ultrascale+ ARM processor connects is protected using a clam shell with a screw and tamper-evident label.

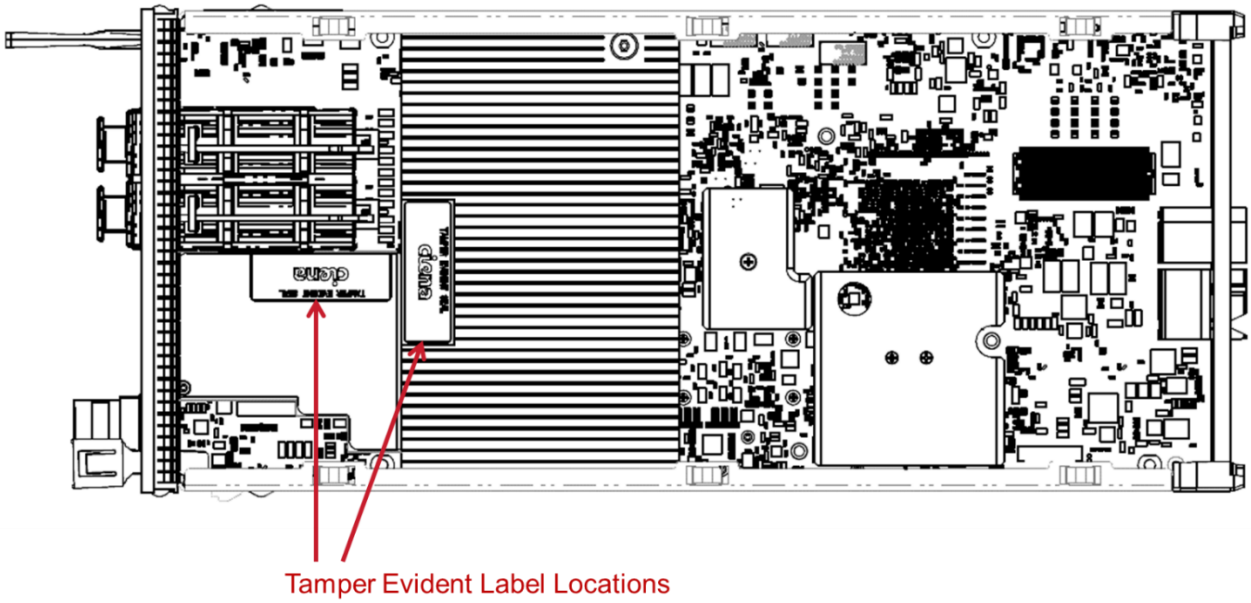

Figure 5 -Tamper Evident Label locations

The CO is responsible for the configuration the module, which includes configuring the data path parameters and certificates. Once properly provisioned, the module will operate in FIPS-Approved mode of operation until it is decommissioned by the CO or the physical security is breached. The module will always operate in FIPS Approved mode as long as the power-up Self-Tests pass.

12.3 Secure Management

The CO 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 *Waveserver Ai User Guide* document.

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

12.3.1 Use of AES GCM in Waveserver Ai Encryption Module

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

The module establishes an IKEv2 session with a remote peer device using AES GCM from Crypto Library 1 for data message encryption. The module uses RFC 7296 compliant IKEv2 to establish the shared secret from which the AES GCM encryption keys are derived. If 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-based AES-GCM implementation in the FPGA Datapath conforms to IG A.5 scenario #2. The Approved DRBG from Crypto Library 1 generates the IV and DEK and sends it to the hardware implementation. All of this takes place internal to the module. The 256-bit encryption DEK and 96-bit IV value is derived periodically (once ~10 seconds) by software between the authenticated peers via an IKEv2 session. A 128-bit counter is constructed according to Section 8.2.2 of NIST SP 800-38D using the 96-bit random field and a 32-bit free field. This is to ensure that a unique 128-bit counter is used each time the Encryption key is used to encrypt 128 bits of data. The 96-bit IV value derived by software and is incremented by 1 for each Optical Transport Network (OTN) frame. The 32- bit free field value is reset to 1 for each OTN frame and is incremented by 1 for each 128-bit block in the OPU4 payload encrypted.

If for any reason, a new encryption session key and IV value is not provided to the FPGA in the defined threshold, the FPGA will squelch traffic automatically in both directions. The GCM "Kill Switch" threshold shall be set by software to allow the last known good key to be used for ~60 minutes.

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 same module) and process between module. The SecureMPL layer was introduced to facilitate privacy and data security communication needs between WCS2 and Encryption Card through the midplane. For example, SecureMPL 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	Crypto Officer
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CTR	Counter
DRAM	Dynamic Random-Access Memory
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
EC DH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
IG	Implementation Guidance
IV	Initialization vector
KAT	Known answer test
KDF	Key-Derivation Function
NIST	National Institute of Standards and Technology
NDRNG	Non-Deterministic Random Number Generator
OTN	Optical Transport Network
PSK	Pre-Shared Key
RAM	Random Access Memory
RSA	Rivest Shamir Adleman
SDRAM	Synchronous Dynamic Random Access Memory
SGMII	Serial Gigabit Media Independent Interface
SHA	Secure Hash Algorithm
SP	Special Publication

Table 14 - Glossary of Terms