Ciena Corporation

Waveserver Ai Encryption Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

The Waveserver Ai Encryption 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). The physical boundary is composed of FPGA, processor, DDR4 (DRAM), Flash and the PCB-embedded wire connections between them, and all associated physical security mechanisms. All traffic entering and exiting the module is encrypted/decrypted at wire speed (100Gb/s, 200Gb/s, 300Gb/s and 400Gb/s depending on the line modulation scheme selected) using AES-256 GCM mode.

The Waveserver Ai Encryption Module may also be referred to as the “module” in this document.

1.2 Security Levels

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

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Waveserver Ai Encryption Module is an optical transponder service module. It consists of a multiple chip-embedded, Metus FPGA along with optical components and supporting circuitry.

All security-relevant communications to the module via its management interface (Ethernet) are encrypted using TLS v1.3. The module also supports a client input and output data interface and optical connector. All traffic entering and exiting the module via the client optical connectors is encrypted/decrypted using AES GCM when passing through the line interface. All data passing through the client interface is always plaintext. This module is configured and monitored by a Ciena Waveserver Ai Control Module.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

As shown in Figure 1 (below), the module consists of an ARM Cortex A53 processor with internal RAM. The firmware running on the processor performs all the monitoring/control activities related to the datapath encryption feature. The Metus FPGA contains the AES/GCM ciphers for the line interface. The Metus FPGA performs the AES-GCM encryption and decryption function on the client payload data. The firmware runs on the CPU implementing the "WaveServer Ai Encryption Module FW Crypto Library 2".

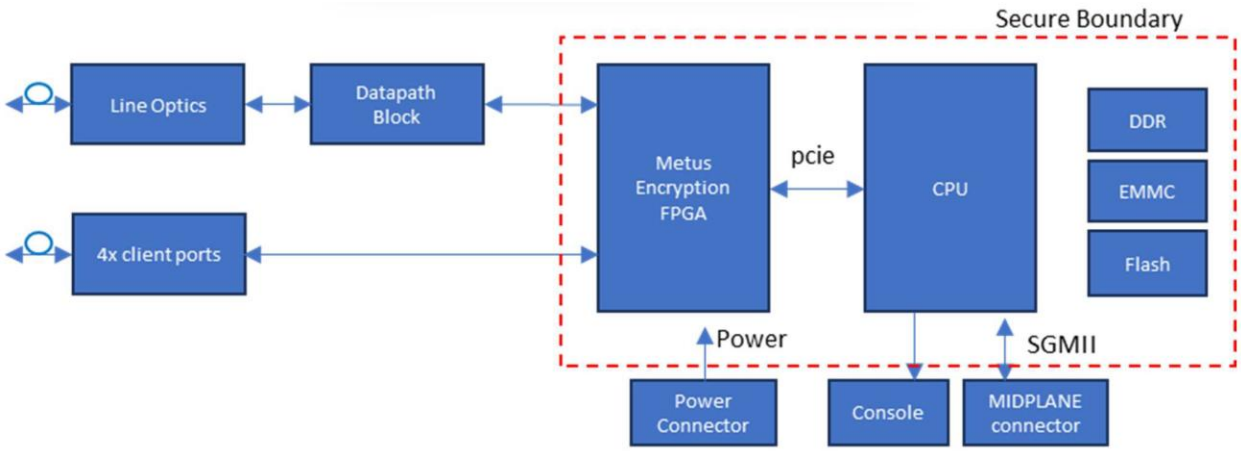

Figure 1: Waveserver Ai Encryption Module Block Diagram

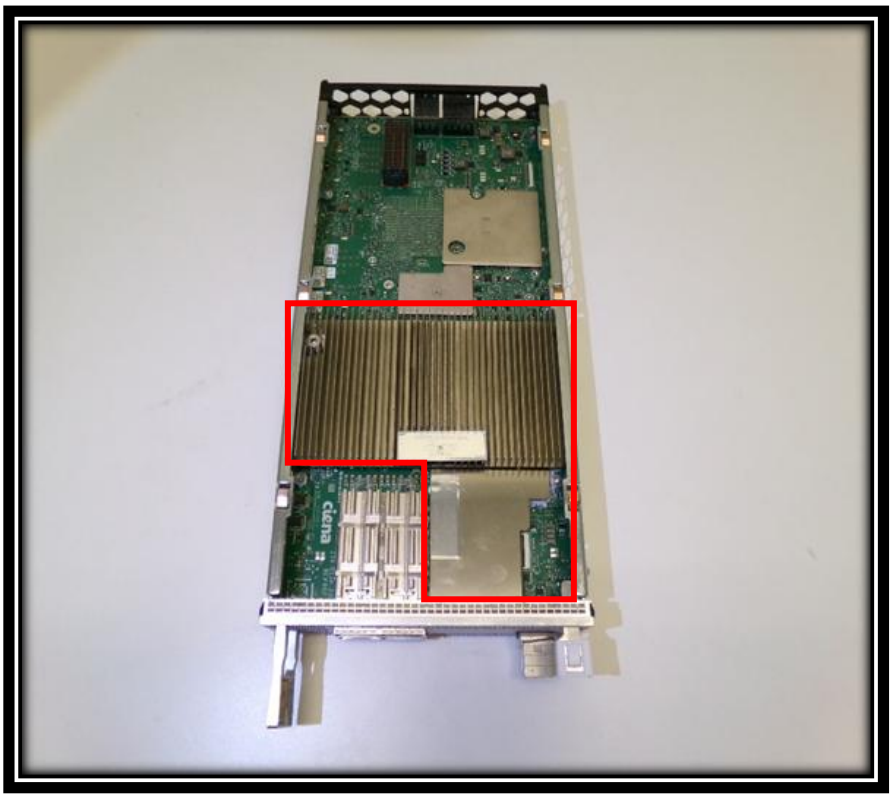

Figure 2 - Physical perimeter of the module (Tamper-evident seal locations)

The module components are embedded behind the parts inside the red rectangle in Figure 2.

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
002/ 174-0534-220	186-1606-820-EB, Revision 003	2.4.50	ARM Cortex A53	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
001/ 174-0534-222	186-1606-820-EB, Revision 003	2.4.50	ARM Cortex A53	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
001/ 174-0534-221	186-1606-820-EB, Revision 003	2.4.50	ARM Cortex A53	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
001/ 174-0534-223	186-1606-820-EB, Revision 003	2.4.50	ARM Cortex A53	The part numbers are equivalent and just used to differentiate the manufacturing process and sites

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

No components have been excluded from the module boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	The module operates in Approved mode by default. No additional configuration is needed for rendering or operating the module in the Approved mode.	Approved	Successful completion of command

Table 3: Modes List and Description

The module does not support a non-Approved mode or a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	C120	Direction - Encrypt Key Length - 256	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A5909	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
AES-GCM	C120	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D
ECDSA KeyGen (FIPS186-5)	A5909	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5909	Curve - P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A5909	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A5909	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
Hash DRBG	A5909	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA2-256	A5909	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5909	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA TwoStep Sp800-56Cr1	A5909	Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256	SP 800-56C Rev. 2
RSA SigVer (FIPS186-5)	A5909	Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
SHA2-256	A5909	Message Length - Message Length: 128-65536 Increment 8	FIPS 180-4
SHA2-384	A5909	Message Length - Message Length: 128-65536 Increment 8	FIPS 180-4
SHA2-512	A5909	Message Length - Message Length: 128-65536 Increment 8	FIPS 180-4

Table 4: Approved Algorithms -

CVL

Algorithm	CAVP Cert	Properties	Reference
TLS v1.3 KDF (CVL)	A5909	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK-DHE	SP 800-135 Rev. 1

Table 5: Approved Algorithms - CVL

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG - Section 4	Key Type: Asymmetric	N/A	NIST SP800-133r2 Section 4: Using the Output of a Random Bit Generator Option 1 (Symmetric keys and seed for asymmetric keys (Option 1)); Section 5.1: Key Pairs for Digital Signature Schemes; Section 5.2: Key Pairs for Key Establishment; Section 6.2.1: Symmetric Keys Generated Using Key Agreement Schemes

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

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

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES-CBC	No Security Claimed	Boot Image Encryption

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

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

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Integrity Test	SHA	Firmware integrity test		SHA2-384: (A5909)
Firmware upgrade	DigSig-SigVer	Initiate the upgrade of the encryption module firmware when directed by the WCS- 2 via control input interface (SGMII)		RSA SigVer (FIPS186-5): (A5909)
FPGA Datapath	BC-Auth	Used to encrypt and decrypt 128		AES-GCM: (C120)

Name	Type	Description	Properties	Algorithms
		bits of data for transfer.		AES-ECB: (C120)
KAS1	KAS-Full	Used for Key Agreement with remote peer	IG:IG D.F Scenario 2, path (2), split Key confirmation: no Key derivation:IG 2.4.B SP 800-135rev1 CVL and KDA (separately tested) Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5909) KDA TwoStep Sp800-56Cr1: (A5909) TLS v1.3 KDF: (A5909) CKG - Section 4: () Key Type: Symmetric and Asymmetric
ECDSA KeyGen	AsymKeyPair-KeyGen	ECDSA KeyGen for Key Agreement Scheme		ECDSA KeyGen (FIPS186-5): (A5909) Hash DRBG: (A5909) CKG - Section 4: () Key Type: Symmetric and Asymmetric ECDSA KeyVer (FIPS186-5): (A5909)
Module Configuration	BC-Auth DigSig-SigVer	Obtains Pre-shared keys or verifies CO certificate		AES-GCM: (A5909) ECDSA SigVer (FIPS186-5): (A5909) TLS v1.3 KDF: (A5909)
Authentication	DigSig-SigVer	Verifies iDevID on initial device authentication with WCS-2		ECDSA SigVer (FIPS186-5): (A5909)
SIgnature Generation	DigSig-SigGen	ECDSA Signature Generation		ECDSA SigGen (FIPS186-5): (A5909) SHA2-256:

Name	Type	Description	Properties	Algorithms
				(A5909) SHA2-384: (A5909) SHA2-512: (A5909)
KTS1	KTS-Wrap	Key Transport for TLS	Standard :SP 800-38D IG D.G:approved method from D.G Key Confirmation:no Caveat:Key establishment methodology provides between 128 and 192 bits of security strength	AES-GCM: (A5909)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

• No parts of the TLS 1.3 protocol, other than the KDF, have been tested by the CAVP and CMVP per FIPS 140-3 IG D.C.

• The module's AES-GCM implementation confirms to IG C.H Scenario #5 following RFC 8446 for TLS v1.3 and provides support for GCM cipher suites from Section B.4 of RFC 8446. The IV is generated internally using the module's Approved DRBG. The protocol's implementation is contained within the boundary of the module under test. The generated IV is used in the context of the AES-GCM encryption executing the provisions of the protocol within which the IV was generated.

• The module's AES-GCM implementation also confirms to IG C.H Scenario #3 and the IV is generated by the Approved DRBG that is internal to the module's boundary. The IV length is 96 bits as per SP800-38D.

2.8 RBG and Entropy

Cert Number	Vendor Name
E199	Ciena

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Ciena Kernel CPU Jitter RNG	Non-Physical	Linux kernel 4.14 on AMD Zynq Ultrascale+	256 bits	Full Entropy (256 bits)	A5464 (SHA3-256)

Table 10: Entropy Sources

The entropy source provides 256 bits of entropy which is sufficient for the generation of the SSPs (using the approved DRBGs of the module) with the maximum target security strength (256 bits) needed. Table 2 of Public Use Document for Ciena Kernel CPU Jitter RNG (ESV #E199) summarizes the configuration settings used by the Ciena Kernel CPU Jitter. These settings must be preserved to comply with the CPU Jitter ESV certificate.
The Public Use Document can be found here.
The module implements one NIST SP 800-90Ar1 Hash DRBG and supports the following sections per NIST SP 800-133r2 (CKG): Sections 4, 5.1, 5.2 and 6.2.1.

2.9 Key Generation

- In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133rev2 (vendor affirmed). The resulting symmetric keys and seed value for asymmetric keys are the unmodified output from the Approved DRBG.
- The module generates keys as described in SP 800-133rev2 Section 4, Option #1. It uses an Approved Hash_DRBG (as specified in SP 800-90Arev1) to generate symmetric keys and seed for asymmetric keys. The DRBG is seeded from seeding material provided by JENT Non-Physical Entropy source (Ciena Kernel CPU Jitter RNG), which provides an entropy source and unbiased random sequence of bits to the DRBG.
- The module is a hardware module with an entropy generating Ciena Kernel CPU Jitter RNG inside the module's cryptographic boundary compliant with Scenario 1 (a) described in FIPS 140-3 IG 9.3.A.

2.10 Key Establishment

Key Agreement

Per IG D.F:
The module supports Key Agreement Schemes per NIST SP800-56Ar3 and [FIPS140-3_IG] D.F Scenario 2 (path 2) followed by SP800-56Cr1 or SP800-135r1 compliant Key Derivation. Approved Algorithm list includes the tested components (KAS-ECC-SSC, KDA TwoStep, TLS KDF per NIST SP 800-135r1) as individual entries. The shared secret computation provides between 128 and 256 bits of encryption strength. This is denoted by KAS1 in the Security Function Implementation Table.

The Module obtains the [FIPS140-3_IG] D.F required key agreement assurances: [SP800-56Ar3] in accordance with Section 5.6.2.

Key Transport

The module also supports key transport in the context of the TLS protocol per the KTS1 in the Security Function Implementation Table.

2.11 Industry Protocols

The Module conforms to Resolution 2 per [FIPS140-3_IG] D.C. References to the Support of Industry Protocols: It provides [SP800-56Ar3] conformant schemes and API entry points oriented TLS. The following caveat is applicable:
No parts of the TLS protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.
The Module also conforms to Resolution 7 per [FIPS140-3_IG] 2.4.B Tracking the Component Validation List.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
UART Connector (Console Interface (RS- 232))	Status Output	Status Output
SGMII (Ethernet) / midplane connector	Data Input Data Output Control Input Status Output	TLS 1.3 communication
Midplane connector	Data Input Data Output Control Input Status Output Power	Line recovered clock outputs and inputs can also be considered as status output.
Optical connector	Data Input Data Output Status Output	On Client Interfaces data input and output is in plaintext. On Line Port Interface data input and output is encrypted. Status output is received as part of Line Port Interface.
eMMC	Data Input	Firmware Load
Module faceplate	Status Output	LED status output

Table 11: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Initial Device ID (iDevID)	The module supports ECDSA digital certificate authentication of CO over TLS 1.3	ECDSA SigVer (FIPS186-5) (A5909)	Using conservative estimates and equating the use of ECDSA with P-521 elliptic curve to a 256- bit strength, the probability for a random attempt to succeed is: 1:2^256 or 1: 1.579 × 10^77 which is less than 1:1,000,000 The fastest network connection supported by the modules over Management interfaces is 1 GB/s	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: 4.94 × 10^68 which is less than 1:100,000 within one minute.
PSK/Certificates	The module supports authentication of the CO using a pre-shared key/certificate over TLS 1.3	ECDSA SigVer (FIPS186-5) (A5909)	Using conservative estimates and equating the use of a 256-bit PSK or an ECDSA with P-521 elliptic curve to a 256-bit strength, the probability for a random attempt to succeed is: 1:2^256 or 1: 1.579 × 10^77 which is less than 1:1,000,000 The fastest network connection supported by the modules over Management	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: 4.94 × 10^68 which is

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			interfaces is 1 GB/s	less than 1:100,000 within one minute.

Table 12: Authentication Methods

The module can be configured to use either a Pre-Shared Key or X.509 Certificate for module peer authentication. The pre-shared key is a 256-bit key. The X.509 certificate is P-384 or P-521. The module also supports authentication of the Ciena WCS-2 using iDevID (an X.509 Certificate).

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	Initial Device ID (iDevID) PSK/Certificates

Table 13: Roles

The module supports one authorized role (i.e., Crypto Officer role). The operator can explicitly assume the CO role by successfully authenticating to the module. The CO role is responsible for module initialization and module configuration, including security parameters, key management, status activities, and audit review.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize the module	Perform initialization of the module. Authenticate and boot the FW load, recover default authentication material. Autonomously performed at power-on.	Global Approved mode indicator (show status indicator)	Command to initialize the module	Same as indicator	Integrity Test KAS1 ECDSA KeyGen SIgnature Generation KTS1	CO - Base Key Encryption Key (BKEK): E - iDevID public key: W,E - DRBG Seed (DRBG): G,E - Entropy Input (EI): G,E - TLS 1.3 Session key (TLS1): G,W,E - TLS 1.3 Pre-Master Secret (TLS3): G,E - TLS 1.3 Master Secret (TLS4): G,E - Nonce: G,E - EC DH Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key: G,E - EC DH Public Key: G,R,E - ECDH peer public key (DPE_PUB): W,E - DPE_Z: G,E - DPE_MACKEY: G,E - DRBG Secret C: G,E - DRBG Secret V: G,E
Configure and manage the module	Set to PSK mode and provision the PSK or set to certificate mode and provision the certificate	Global Approved mode indicator (show status indicator)	Command to configure module	Same as indicator	KAS1 Module Configuration SIgnature Generation KTS1	CO - Datapath Customer Enrolled Pre-shared key (PSK): W,E - Datapath Customer Enrolled Certificate (CERT) and CA: W,E - TLS 1.3 Session key (TLS1): G,W,E - TLS 1.3 Pre-Master Secret (TLS3): G,E - TLS 1.3 Master Secret (TLS4): G,E
Zeroise	Perform Power Down Zeroisation (Zeroise)	Global Approved mode indicator (show status indicator)	Power-cycle/reboot	Same as indicator	None	CO - DRBG Seed (DRBG): Z - Entropy Input (EI): Z - Datapath Customer Enrolled Pre-shared key (PSK): Z - Datapath Customer Enrolled Certificate (CERT) and CA:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - TLS 1.3 Session key (TLS1): Z - TLS 1.3 Pre-Master Secret (TLS3): Z - TLS 1.3 Master Secret (TLS4): Z - Remote certificate public key: Z - Nonce: Z - EC DH Private Key: Z - EC DH Public Key: Z - ECDH peer public key (DPE_PUB): Z - DPE_Z: Z - DPE_MACKEY: Z - DPE_KDK: Z - Datapath Cipher Encrypt/ Decrypt keys (DDEK/DDDK): Z - iDevID public key: Z - DRBG Secret C: Z - DRBG Secret V: Z
Datapath Encryption/ Decryption Service (Perform approved security functions)	Initiate the TLS session to the peer module, perform the key agreement protocol and configure the datapath keys; Automatic	Global Approved mode indicator (show status indicator)	Command to encrypt/ decrypt data along with plaintext and session key	Encrypted/ Decrypted data	FPGA Datapath KAS1 SIgnature Generation KTS1	CO - Datapath Customer Enrolled Pre-shared key (PSK): E - TLS 1.3 Session key (TLS1): G,W,E,Z - TLS 1.3 Pre-Master Secret (TLS3): G,E,Z - TLS 1.3 Master Secret (TLS4): G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	ally performed when PSK or certificate is provisioned					- EC DH Public Key: G,E - EC DH Private Key: G,R,E - ECDH peer public key (DPE_PUB): W,E - DPE_Z: G,E,Z - DPE_MACKEY: G,E,Z - DPE_KDK: G,E,Z - Datapath Cipher Encrypt/ Decrypt keys (DDEK/DDDK): G,E,Z - DPE_IV: G,E,Z - Datapath Customer Enrolled Certificate (CERT) and CA: E
Report the module information and firmware version (Show Version)	View the firmware version and module information	Global Approved mode indicator (show status indicator)	Command to query module information and firmware version	Module information and firmware version	None	Unauthenticated
Firmware upgrade	Initiate the upgrade of the module firmware when directed by the CO via control input interface (SGMII)	Successful firmware upgrade followed by reboot	Command to upgrade firmware	Same as indicator	Firmware upgrade KAS1 SIgnature Generation KTS1	CO - LOAD image public key (LOAD_PUBLIC_KEY): W,E - TLS 1.3 Session key (TLS1): E - TLS 1.3 Pre-Master Secret (TLS3): E - TLS 1.3 Master Secret (TLS4): E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform operator authentication	Authenticate the CO with the module and replace the default authentication material on first connection. This is performed automatically when a WCS-2 module attempts to connect via the SGMII interface.	Event Logs	iDevID Certificate/ PSK	Authentication status	KAS1 Authentication SIgnature Generation KTS1	CO - iDevID public key: W,E - TLS 1.3 Session key (TLS1): G,W,E - TLS 1.3 Pre-Master Secret (TLS3): G,W,E - TLS 1.3 Master Secret (TLS4): G,W,E
Perform on-demand self- tests	Perform pre-operational and conditional self-tests on demand via module restart	Global Approved mode indicator (show status indicator)	Power-cycle/reboot	Successful module reboot	None	Unauthenticated
Monitor alarms, status & statistics (Show Status)	View the encryption related alarms, status and performance monitoring statistics	Global Approved mode indicator (show status indicator)	Command to show alarms	Status of alarms, statistics and active alarms	None	Unauthenticated

Table 14: Approved Services

The module provides a limited number of services for which the operator is not required to assume an authorized role. None of the services listed in Approved Services table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

The module operator must authenticate to the module before being allowed access to services that require the assumption of an authorized role.

4.4 Non-Approved Services

The module does not support non-approved services.

4.5 External Software/Firmware Loaded

The firmware upgrade is initiated by the WCS-2. The Encryption Module performs the load integrity checks followed by the version checks before allowing or denying the upgrade.

The module version can be verified using “software show” command on the WCS-2. Any firmware/software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

4.7 Cryptographic Output Actions and Status

Self-initiated Cryptographic Output
The module supports self-initiated cryptographic output functionality via the Datapath Encryption/ Decryption Service. Before enabling this service, the CO must configure and perform two independent internal actions for the service to get activated.

The independent internal actions are as follows:

1. The CO must authenticate with the module.
2. The CO must perform the “Configure and manage the module” service to activate PSK or install a certificate authentication.

5 Software/Firmware Security

5.1 Integrity Techniques

The module claims EDC (SHA2-384) on the Waveserver Ai Encryption Module FW Crypto Library 2 for the pre-operational firmware integrity test.

5.2 Initiate on Demand

The integrity test can be initiated on demand by rebooting or power cycling the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied :

The operational environment requirements do not apply to this module as the module type is hardware and the overall security level is 2.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-evident seals	Periodic inspection of tamper- evident seals when moving/replacing the module	Two tamper-evident seals are applied to the multi-chip embedded cryptographic module during manufacturing; The physical security of the module is intact if there is no evidence of tampering with the tamper-evident seal(s); If evidence of tamper is found, the Cryptographic Officer is requested to follow their internal IT policies, which may include contacting Ciena for replacing the unit

Table 15: Mechanisms and Actions Required

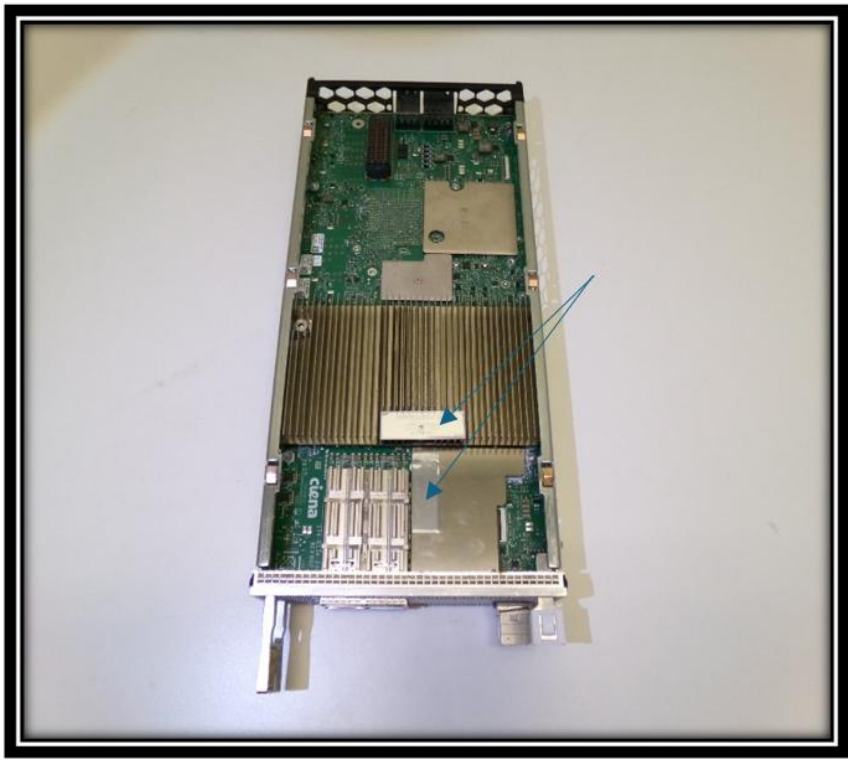

Figure 3 - Top View of Waveserver Ai Encryption Module (Tamper-evident seal locations)

The module is shipped from the factory with the required physical security mechanisms (tamper-evident seals, metal covers and PCB layers) installed. The tamper-evident seal locations are indicated by arrows in the above diagram. 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 follow internal security policies which include contacting Ciena.

8 Non-Invasive Security

8.1 Mitigation Techniques

Not applicable. The module does not implement any non-invasive attack mitigation techniques.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Stored in plaintext in RAM	Dynamic
eFUSE	Read-only eFUSE in plaintext	Static

Table 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Stored at manufacture	Manufacturer	eFUSE	Plaintext	N/A	N/A	
Input_1	External (Outside of the Module's Boundary)	RAM	Encrypted	Automated	Electronic	KTS1
Output_1	RAM	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	KTS1
Input_2	External (Outside of the Module's Boundary)	RAM	Encrypted	Automated	Electronic	KTS1
Output_2	RAM	External (Outside of the	Encrypted	Automated	Electronic	KTS1

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
		Module's Boundary)				

Table 17: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reboot or Power Cycle	SSPs in memory are lost during reboot or power cycle.	All the SSPs in memory are cleared during reboot or power cycle	On Demand
Zeroise after use	SSPs are zeroized after use automatically	Ephemeral keys are zeroised by the module after use	Automatically Zeroise after use
Power Removal	SSPs in memory are lost when power supply is removed	All the SSPs in memory are lost when power supply is removed	On Demand
Clear Command	Command zeroises all datapath encryption related SSPs	All encryption related SSPs are zeroised by the command	On demand

Table 18: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Base Key Encryption Key (BKEK)	Used for decrypting the Ciena Device ID	AES-GCM 256 bits - 256 bits	AES GCM 256-bit key - Neither			AES-GCM (A5909)
DRBG Seed (DRBG)	Used for random number generation	256 bits - 256 bits	CSP - CSP	Hash DRBG (A5909)		Hash DRBG (A5909)
Entropy Input (EI)	Used for random number generation	384 bits - 384 bits	CSP - CSP	Entropy Source		Hash DRBG (A5909)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
LOAD image public key (LOAD_PUBLIC_KEY)	Used to authenticate the new firmware being loaded during upgrade	RSA 4096 bits - 152 bits	Public Key - Neither			RSA SigVer (FIPS186-5) (A5909)
Datapath Customer Enrolled Pre-shared key (PSK)	Used for TLS 1.3 communication with remote peer device	256 bits - 256 bits	CSP - CSP			KAS1
Datapath Customer Enrolled Certificate (CERT) and CA	Used for TLS 1.3 communication with remote peer device	ECDSA P-521, P-384 keypair - 256, 192 bits	CSP - CSP			KAS1
TLS 1.3 Session key (TLS1)	Used for encrypting/decrypting TLS messages	AES-GCM 256 bits - 256 bits	CSP - CSP		KAS1	AES-GCM (A5909)
iDevID public key	Used for WCS-2 Authentication on initial setup	ECDSA P-521 - 256 bits	PSP - PSP			ECDSA SigVer (FIPS186-5) (A5909)
TLS 1.3 Pre-Master Secret (TLS3)	Establish the TLS Master Secret	521 bits - 521 bits	CSP - CSP		KAS1	
TLS 1.3 Master Secret (TLS4)	Establish the TLS Session Key	521 bits - 521 bits	CSP - CSP	TLS v1.3 KDF (A5909)		
Remote certificate public key	Used for TLS 1.3 communication with remote peer device	ECDSA P-521, P-384, P-256 - 256, 192, 128 bits	PSP - PSP			KAS1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Nonce	Used for the DH key agreement	256 bits - 256 bits	CSP - CSP	Hash DRBG (A5909)		KAS1
EC DH Private Key	Used for exchanging shared secret to derive session keys during key agreement	ECDSA P-521 - 256 bits	CSP - CSP	ECDSA KeyGen		KAS1
EC DH Public Key	Used for exchanging shared secret to derive session keys during key agreement	ECDSA P-521 - 256 bits	PSP - PSP	ECDSA KeyGen		
ECDH peer public key (DPE_PUB)	Used during key agreement (remote ephemeral public key)	ECDSA P-521 - 256 bits	PSP - PSP			KAS1
DPE_Z	Shared secret resulting from the ECDHE exchange between peers	256 bits - 128 bits	CSP - CSP		KAS1	KAS1
DPE_MACKEY	Used to authenticate key agreement messages	256 bits - 128 bits	CSP - CSP		KAS1	
DPE_KDK	Master key derivation key used to derive the data path cipher keys and IVs	256 bits - 128 bits	CSP - CSP		KAS1	KAS1
Datapath Cipher Encrypt/ Decrypt keys (DDEK/DDDK)	Used for encryption and decryption of the data path	AES-GCM 256 bits - 256 bits	Session keys - CSP		KAS1	AES-GCM (A5909)
DPE_IV	Used for encryption and decryption of the data path	96 bits - 96 bits	IV - CSP	KDA TwoStep Sp800-56Cr1 (A5909)		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG Secret C	Hash DRBG Internal State Secret C	440 bits - 256 bits	Entropy - CSP	Hash DRBG (A5909)		Hash DRBG (A5909)
DRBG Secret V	Hash DRBG Internal State Secret V	440 bits - 256 bits	Entropy - CSP	Hash DRBG (A5909)		Hash DRBG (A5909)

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Base Key Encryption Key (BKEK)	Stored at manufacture	eFUSE:Plaintext			
DRBG Seed (DRBG)		RAM:Plaintext	Until reboot	Reboot or Power Cycle Power Removal Clear Command	Entropy Input (EI):Derived From
Entropy Input (EI)		RAM:Plaintext	Until reboot	Reboot or Power Cycle Power Removal Clear Command	DRBG Seed (DRBG):Used to derive
LOAD image public key (LOAD_PUBLIC_KEY)	Input_1	RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	
Datapath Customer Enrolled Pre-shared key (PSK)	Input_1	RAM:Plaintext	Until reboot	Reboot or Power Cycle Power Removal Clear Command	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Datapath Customer Enrolled Certificate (CERT) and CA	Input_1	RAM:Plaintext	Until reboot	Reboot or Power Cycle Power Removal Clear Command	
TLS 1.3 Session key (TLS1)		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	TLS 1.3 Master Secret (TLS4):Derived From
iDevID public key	Input_1	RAM:Plaintext	Until reboot	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	
TLS 1.3 Pre-Master Secret (TLS3)		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	TLS 1.3 Master Secret (TLS4):Used to derive DPE_Z:Derived From Datapath Customer Enrolled Pre-shared key (PSK):Derived From
TLS 1.3 Master Secret (TLS4)		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	TLS 1.3 Pre-Master Secret (TLS3):Derived From TLS 1.3 Session key (TLS1):Used to derive

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Remote certificate public key	Input_1 Input_2	RAM:Plaintext	Until reboot	Reboot or Power Cycle Power Removal Clear Command	
Nonce		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	
EC DH Private Key		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	EC DH Public Key:Paired With DPE_Z:Used to derive
EC DH Public Key	Output_1 Output_2	RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	EC DH Private Key:Paired With
ECDH peer public key (DPE_PUB)	Input_1 Input_2	RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	DPE_Z:Used to derive
DPE_Z		RAM:Plaintext	zeroised after use	Reboot or Power Cycle	ECDH peer public key (DPE_PUB):Deriv

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Zeroise after use Power Removal Clear Command	ed From EC DH Private Key:Derived From Nonce:Derived From
DPE_MACKEY		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	DPE_Z:Derived From
DPE_KDK		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	DPE_Z:Derived From
Datapath Cipher Encrypt/ Decrypt keys (DDEK/DDDK)		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	DPE_KDK:Derived From
DPE_IV		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	DPE_KDK:Derived From
DRBG Secret C		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise	DRBG Seed (DRBG):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				after use Power Removal Clear Command	
DRBG Secret V		RAM:Plaintext	zeroised after use	Reboot or Power Cycle Zeroise after use Power Removal Clear Command	DRBG Seed (DRBG):Derived From

Table 20: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
EDC	SHA2-384	EDC	SW/FW Integrity	successful completion	Verifies integrity of the firmware.

Table 21: Pre-Operational Self-Tests

The EDC implementation is as indicated in the above table. The module firmware forces running all the self-tests at startup before any other applications are started. Failure of any algorithm self-test results in setting the red STATUS LED and rebooting the system until such time the self-test passes.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5909) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5909) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart
SHA2-256 (A5909)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart
SHA2-384 (A5909)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	384-bit KAT	Power-Cycle or Restart
SHA2-512 (A5909)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	512-bit KAT	Power-Cycle or Restart
HMAC-SHA2-256 (A5909)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-256 KAT	Power-Cycle or Restart
KAS-ECC-SSC Sp800-56Ar3 (A5909)	SP800-56Arev3 KAS-ECC-SSC	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-521	Power-Cycle or Restart
ECDSA SigVer (FIPS186-5) (A5909)	ECDSA P-521 Sign Ver KAT	KAT	CAST	Global Approved mode indicator (show	Curve used: P-521	Power-Cycle or Restart

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				status indicator)		
TLS v1.3 KDF (A5909)	TLS KDF	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-256, SHA2-384	Power-Cycle or Restart
KDA TwoStep Sp800-56Cr1 (A5909)	Two Step KDA	KAT	CAST	Global Approved mode indicator (show status indicator)	Two Step KDA	Power-Cycle or Restart
AES-ECB (C120) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart
AES-GCM (C120) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart
ECDSA SigGen (FIPS186-5) (A5909)	ECDSA P-521 Sign	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-521	Power-Cycle or Restart
ECDSA KeyGen (FIPS186-5) (A5909)	ECDSA P-521 KeyGen	PCT	PCT	Global Approved mode indicator (show status indicator)	Curve used: P-521	SSP Generation
RSA SigVer (FIPS186-5) (A5909)	RSA 4096 bits	KAT	CAST	Global Approved mode indicator	4096-bit KAT	Power-Cycle or Restart

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				(show status indicator)		
AES-ECB (C120) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart
AES-GCM (C120) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Power-Cycle or Restart
Firmware Load Test	RSA 4096 bits	KAT	SW/FW Load	Global Approved mode indicator (show status indicator)	RSA 4096 KAT	Upon loading firmware
Hash DRBG (A5909)	SHA-256	KAT	CAST	Global Approved mode indicator (show status indicator)	NIST SP 800-90Ar1 Section 11.3 KATs for Instantiate, Generate and Reseed	Power-Cycle or Restart

Table 22: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
EDC	EDC	SW/FW Integrity	On Demand	Manually by power-cycling or restarting the module

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A5909) - Encrypt - 256-bit	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
AES-GCM (A5909) - Decrypt - 256-bit	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
SHA2-256 (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
SHA2-384 (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
SHA2-512 (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
HMAC-SHA2-256 (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
KAS-ECC-SSC Sp800-56Ar3 (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
ECDSA SigVer (FIPS186-5) (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
TLS v1.3 KDF (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
KDA TwoStep Sp800-56Cr1 (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
AES-ECB (C120) - Encrypt - 256-bit	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
AES-GCM (C120) - Decrypt - 256-bit	KAT	CAST	On Demand	Manually by power-cycling or

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				restarting the module
ECDSA SigGen (FIPS186-5) (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
ECDSA KeyGen (FIPS186-5) (A5909)	PCT	PCT	On Demand	By invoking services causing SSP generation
RSA SigVer (FIPS186-5) (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
AES-ECB (C120) - Decrypt - 256-bit	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
AES-GCM (C120) - Encrypt - 256-bit	KAT	CAST	On Demand	Manually by power-cycling or restarting the module
Firmware Load Test	KAT	SW/FW Load	On Demand	By loading firmware from an external source
Hash DRBG (A5909)	KAT	CAST	On Demand	Manually by power-cycling or restarting the module

Table 24: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Soft Error	Upon failure of the firmware load test, the module enters “Soft Error” state. The soft error state is a nonpersistent 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	Failure of Firmware load test	Automatic	Status Log

Name	Description	Conditions	Recovery Method	Indicator
Critical Error	If the module encounters an error in any Pre-Operational self-tests or conditional self-tests the module will enter a Critical error state. In this case, the module will be stuck in an infinite boot loop until the self-tests pass. If the error condition is not cleared, then the module is considered to be malfunctioning and should be returned to Ciena	Failure of pre-operational or conditional self-tests	N/A	A permanent error status will be relayed via the status output interface i.e. setting the red STATUS LED (the module will be stuck in an infinite boot loop)

Table 25: Error States

Failure of any algorithm results in setting the red STATUS LED and rebooting the system until such time the self-test passes.

10.5 Operator Initiation of Self-Tests

Operator can initiate the self-tests through power cycling the module. This action runs pre-operational and conditional self-tests before entering the Approved mode.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module only runs in an Approved mode of operation. The CO can monitor and configure the module via the TLS 1.3 management channel from the Ciena Control Module. Detailed instructions for monitoring and troubleshooting the module are provided in the Ciena's User's Guide and Technical Practices document.

Ciena uses Git software for the management of source code artifacts and SharePoint for hardware and documentation version control. The module is developed using high level programming languages C and C++.

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. 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.

There is no special procedure for decommissioning the module. Disconnecting fibers and removing the encryption module from the system (powering down) results in all SSP zeroisation. There are no other sanitization procedures to complete.

The module only supports an approved mode of operation. No additional configuration is required on the Crypto Officer's part except for installing the module since the provisioning of the module will be taken care of by another Ciena module, the Control Processor.

11.2 Administrator Guidance

The module operates in the Approved mode in default setting. There is no additional guidance apart from the guidance in this security policy. The following actions are required to replace the default authentication data in the module:

1) The first action is the authentication and login of the Crypto Officer (WCS-2 card) "Perform operator authentication" service. This first action represents the intention to configure the module.
2) The second action performed by the Crypto Officer is to provision authentication material via the "Configure and manage the module" service.

11.3 Non-Administrator Guidance

There is no additional guidance apart from the guidance in this security policy.

12 Mitigation of Other Attacks

12.1 Attack List

The module does not support mitigation of other attacks.