Ciena Corporation

Ciena Waveserver Ai WCS-2

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 4
1.1 Overview 4
1.2 Security Levels 5
2 Cryptographic Module Specification 5
2.1 Description 5
2.2 Tested and Vendor Affirmed Module Version and Identification 7
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 8
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 15
2.8 RBG and Entropy 15
2.9 Key Generation 16
2.10 Key Establishment 16
2.11 Industry Protocols 17
3 Cryptographic Module Interfaces 17
3.1 Ports and Interfaces 17
4 Roles, Services, and Authentication 18
4.1 Authentication Methods 18
4.2 Roles 19
4.3 Approved Services 19
4.4 Non-Approved Services 36
4.5 External Software/Firmware Loaded 36
4.7 Cryptographic Output Actions and Status 36
5 Software/Firmware Security 37
5.1 Integrity Techniques 37
5.2 Initiate on Demand 37
6 Operational Environment 37
6.1 Operational Environment Type and Requirements 37
7 Physical Security 37
7.1 Mechanisms and Actions Required 37
8 Non-Invasive Security 39
9 Sensitive Security Parameters Management 39
9.1 Storage Areas 39
9.2 SSP Input-Output Methods 39

9.3 SSP Zeroization Methods 40
9.4 SSPs 41
10 Self-Tests 51
10.1 Pre-Operational Self-Tests 51
10.2 Conditional Self-Tests 51
10.3 Periodic Self-Test Information 51
10.4 Error States 53
11 Life-Cycle Assurance 53
11.1 Installation, Initialization, and Startup Procedures 53
11.2 Administrator Guidance 54
11.3 Non-Administrator Guidance 54
12 Mitigation of Other Attacks 54
12.1 Attack List 54

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 8
Table 4: Approved Algorithms 10
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Non-Approved, Allowed Algorithms with No Security Claimed 11
Table 7: Security Function Implementations 15
Table 8: Entropy Certificates 15
Table 9: Entropy Sources 16
Table 10: Ports and Interfaces 18
Table 11: Authentication Methods 19
Table 12: Roles 19
Table 13: Approved Services 36
Table 14: Mechanisms and Actions Required 37
Table 15: Storage Areas 39
Table 16: SSP Input-Output Methods 40
Table 17: SSP Zeroization Methods 41
Table 18: SSP Table 1 46
Table 19: SSP Table 2 51
Table 20: Pre-Operational Self-Tests 51
Table 21: Pre-Operational Periodic Information 51
Table 22: Conditional Periodic Information 53
Table 23: Error States 53

List of Figures

Figure 1: Waveserver Ai WCS-2 6
Figure 2: Ciena Waveserver Ai Encryption Module Chassis 7
Figure 3: WCS-2 Block Diagram 7
Figure 4: Top View of Ciena Waveserver Ai WCS2 38
Figure 5: Placement for the three temper seals 38

1 General

1.1 Overview

The Ciena Corporation Waveserver Ai WCS-2 Module is a multi-chip embedded hardware cryptographic module. The module is a purpose-built field replaceable unit intended for operation within the Ciena Waveserver Ai chassis. Its primary function is management of the Waveserver Ai Encryption chassis, which includes one or more Waveserver Ai Encryption Modules.

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

The module meets the overall Security Level 2 requirements.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The module serves as the central control and storage facility for any SSPs utilized by the Encryption Module. Management functions of the module include device configuration, alarm monitoring, and log collection. The security functions performed by the module include operations related to the provisioning of the chassis (access controls, user passwords, remote authentication, and firmware upgrades), as well as control of the Waveserver Ai Encryption Module via TLS v1.3. All communication to the module via its management interfaces are encrypted either using TLS v1.2 or SSHv2. The module also supports a local serial console interface and read-only SNMPv3 data.

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

The major components of the module include a Xilinx Zynq MPSOC system on a chip which contains a A53 quad core processor, memory, an SSD, and FPGA (Field-Programmable Gate Arrays). The module is installed inside the Waveserver Ai Encryption chassis and is attached to other Waveserver subsystems via a host connector, PCIe, Ethernet, serial, and USB-C.

Figure 1 below depicts the Waveserver Ai Encryption chassis, which consists of a Waveserver AI WCS-2 and up to four Encryption Modules. The validated module i.e., the Waveserver AI WCS-2, is a multi-chip embedded embodiment housed in the Waveserver Ai Encryption

chassis; the module components are completely enclosed within a hard metal clamshell cover with tamper evident labels applied. Figure 2 provides a block diagram of the module, depicting the major components of the module and the cryptographic boundary as shown in red. No module components have been excluded from the cryptographic boundary.

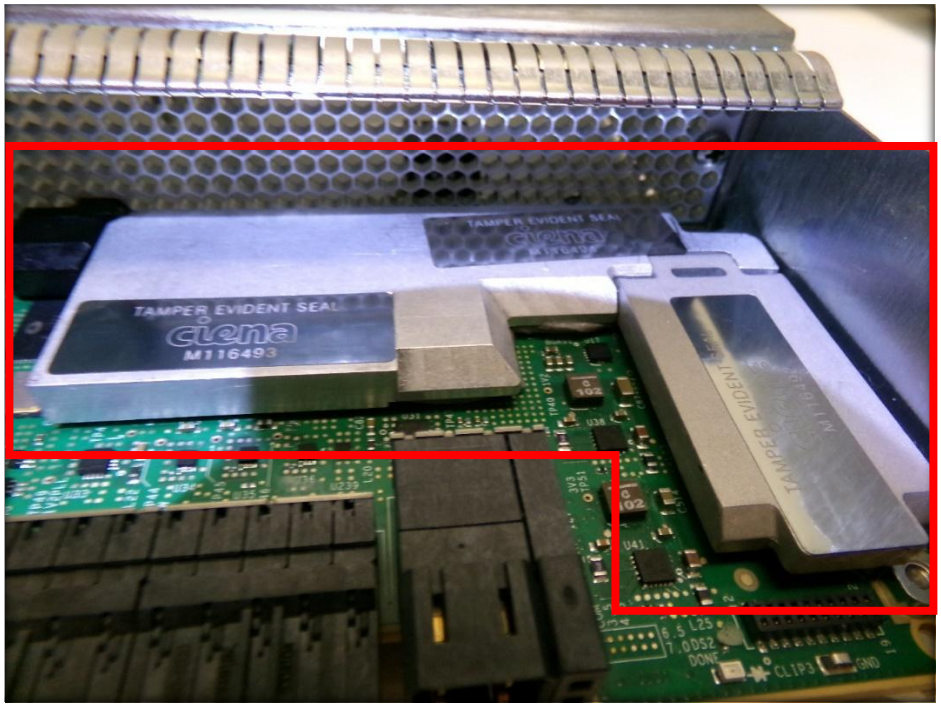
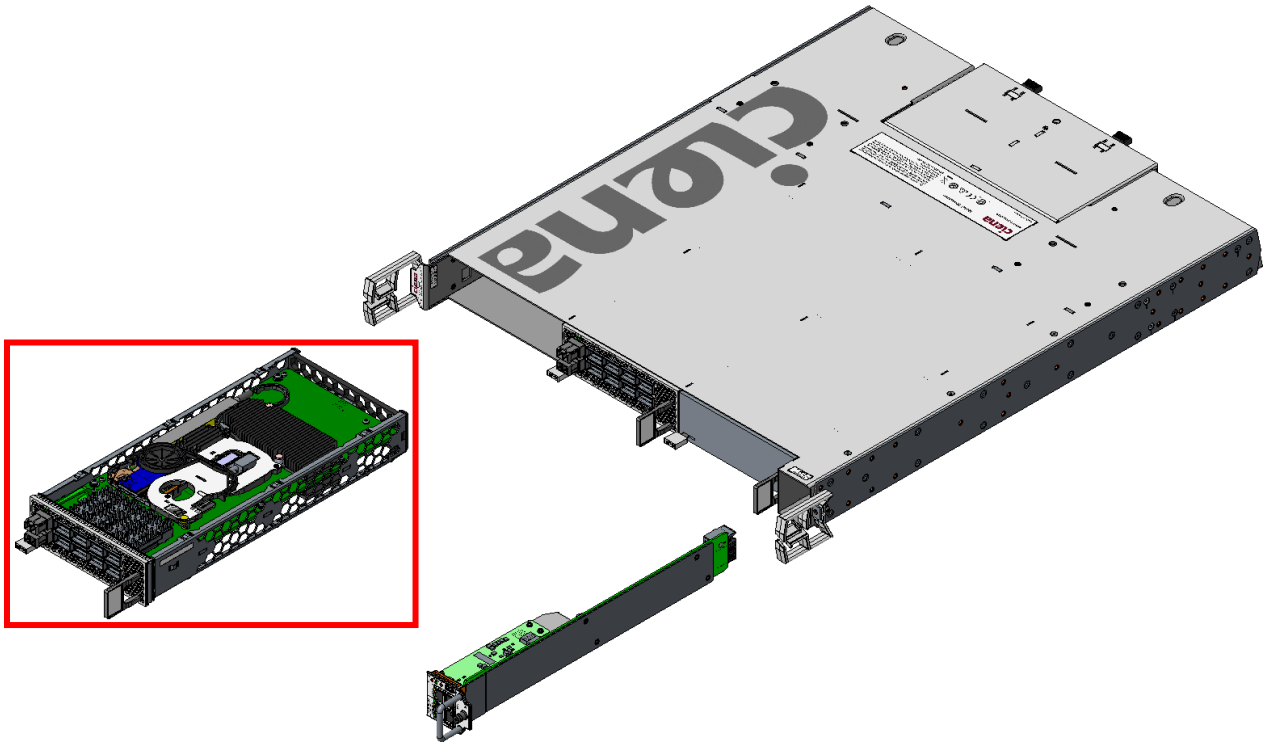


Figure 1: Waveserver Ai WCS-2



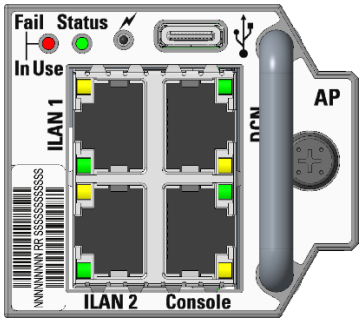


Figure 2: Ciena Waveserver Ai Encryption Module Chassis

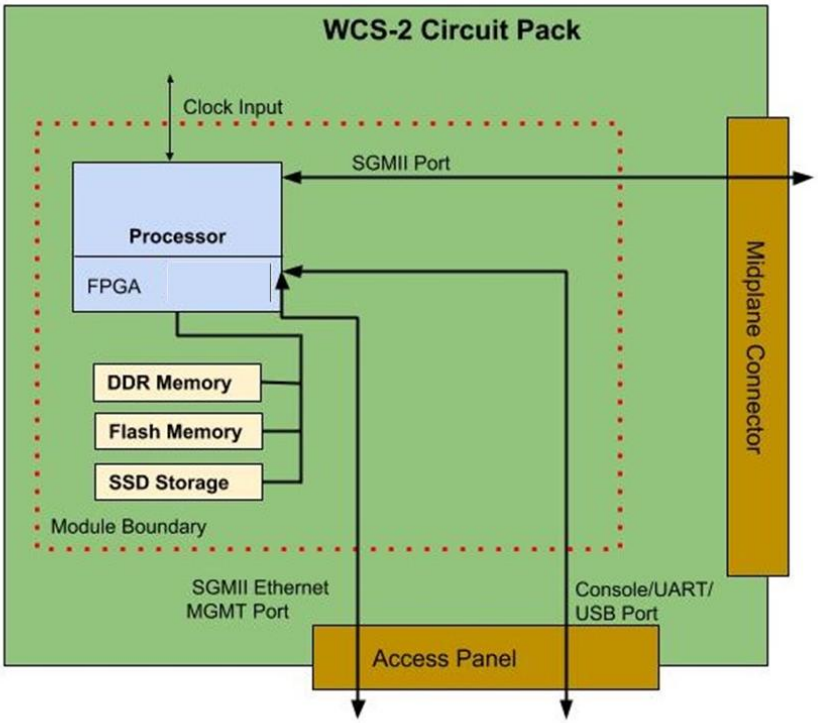


Figure 3: WCS-2 Block Diagram

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
PCB 186- 1034-210 Revision 001	Hardware 186-1034-411-EB [Revision 002, 003, 004, 005, 006, and 007]	2.4.50	ARM Cortex A53	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

The module does not contain any components that are excluded from the FIPS 140-3 requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved Mode	The module is shipped in factory state and the module is explicitly configured to operate in an Approved mode of operation	Approved	Global indication that system is running in an approved mode.

Table 3: Modes List and Description

The module is shipped in factory state and the module is explicitly configured to operate in an Approved mode of operation. Section 11 provides additional information for configuring the module in the Approved mode of operation. The module does not support a non-approved mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5908	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR	A5908	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-GCM	A5908	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128 IV Length - IV Length: 96	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 128, 256 AAD Length - AAD Length: 0, 256	
ECDSA KeyGen (FIPS186-5)	A5908	Curve - P-256, P-384, P-521 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A5908	Curve - P-256, P-384, P-521	FIPS 186-5
ECDSA SigGen (FIPS186-5), ECDSA SigVer (FIPS186-5)	A5908	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-5
Hash DRBG	A5908	Prediction Resistance - No Supports Reseed - Yes Mode - SHA2-256 Entropy Input - Entropy Input: 256 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0 Additional Input - Additional Input: 0 Returned Bits - 1024	SP 800-90A Rev. 1
HMAC-SHA-1	A5908	MAC - MAC: 80-160 Increment 8 Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256	A5908	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-384	A5908	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-512	A5908	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A5908	Domain Parameter Generation Methods - P-256, P-384, P-521 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KAS-FFC-SSC Sp800-56Ar3	A5908	Domain Parameter Generation Methods - FC, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048 Scheme - dhEphem - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SP800-108	A5908	KDF Mode - Feedback MAC Mode - HMAC-SHA2-256 Supported Lengths - Supported Lengths: 256 Fixed Data Order - After Fixed Data Counter Length - 8	SP 800-108 Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		Supports Empty IV - Yes Requires Empty IV - Yes Custom Key In Length - 0	
KDF SSH (CVL)	A5908	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
PBKDF	A5908	Iteration Count - Iteration Count: 4096 HMAC Algorithm - SHA2-256 Password Length - Password Length: 14-128 Increment 1 Salt Length - Salt Length: 128-512 Increment 8 Key Data Length - Key Data Length: 128	SP 800-132
RSA KeyGen (FIPS186-5)	A5908	Key Generation Mode - probable Modulo - 2048, 3072, 4096 Primality Tests - 2powSecStr Info Generated By Server - No Private Key Format - standard Public Exponent Mode - random	FIPS 186-5
RSA SigGen (FIPS186-5)	A5908	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
RSA SigVer (FIPS186-5)	A5908	Hash Pair - Hash Algorithm - SHA2-224 Modulo - 2048, 3072, 4096 Signature Type - pkcs1v1.5 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
Safe Primes Key Generation, Safe Primes Key Verification	A5908	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048	SP 800-56A Rev. 3
SHA-1, SHA2-256, SHA2-384, SHA2-512	A5908	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
TDES-CBC	A5908	Direction - Decrypt Keying Option - 1	SP 800-67 Rev. 2
TLS v1.2 KDF RFC7627 (CVL)	A5908	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512 Key Block Length - Key Block Length: 1024	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A5908	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG - Section 4	Key Type:Symmetric and 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; 6.1: The Direct Generation of Symmetric Keys; Section 6.2.1: Symmetric Keys Generated Using Key Agreement Schemes; Section 6.2.3 Symmetric Keys Derived from Passwords

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not implement any non-Approved, Allowed algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
SNMPv2C (MD5, DES, 3DES, SHA-1 AES-128, AES-192, AES-256)	No Security Claimed	SNMPv2C is used for non-security relevant status output such as alerts, alarms etc. Hence no security claimed as per IG 2.4.A Additional Comment 2 and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.
SNMPv3 (MD5, DES, 3DES, SHA-1 AES-128, AES-192, AES-256)	No Security Claimed	SNMPv3 is used for non-security relevant status output such as alerts, alarms etc. Hence no security claimed as per IG 2.4.A Additional Comment 2 and the following requirements per the Additional Comment 2 are satisfied: 1) the algorithm is not used whatsoever to meet any FIPS 140-3 requirements; 2) the algorithm does not access or share CSPs in a way that counters the requirements of the IG; 3) i) the algorithm is not intended to be used as a security function 4) the algorithm's non-approved use and purpose (from 3)) is unambiguous to the operator and can't be easily confused for a security function given as the purpose is not providing any security functionality recognized in FIPS 140-3.

Table 6: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

The module does not implement any non-Approved, not Allowed algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Integrity Test	SHA	Firmware integrity test		SHA2-384: (A5908)
Module Configuration	BC-Auth DigSig-SigVer KAS-135KDF	Select PSK for DPE peer authentication and provision the encryption MOTR. or Activate certificate peer authentication and provision the encryption MOTR Over the TLS 1.3 interface.		RSA SigVer (FIPS186-5): (A5908) ECDSA SigVer (FIPS186-5): (A5908) ECDSA SigGen (FIPS186-5): (A5908) RSA SigGen (FIPS186-5): (A5908)
Firmware Upgrade	DigSig-SigVer	Initiate a system wide firmware upgrade using RSA 4096-bit Load Test		RSA SigVer (FIPS186-5): (A5908)
Asymmetric Key Generation	AsymKeyPair-KeyGen CKG	RSA, DH and ECDH Key Pair Generation		ECDSA KeyGen (FIPS186-5): (A5908) RSA KeyGen (FIPS186-5): (A5908) Hash DRBG: (A5908) Safe Primes Key Generation: (A5908) ECDSA KeyVer (FIPS186-5): (A5908) Safe Primes Key Verification: (A5908) CKG -

Name	Type	Description	Properties	Algorithms
				Section 4: () Key Type: Symmetric and Asymmetric
Authentication	DigSig-SigVer	Verify Public Key Certificates (RSA/ECDSA) on initial device authentication		ECDSA SigVer (FIPS186-5): (A5908) RSA SigVer (FIPS186-5): (A5908)
KTS-1	KTS-Wrap	Key Transport in the context of industry protocols	Standard: SP 800-38F IG D.G:approved method from IG D.G Key confirmation:no Caveat : Key establishment methodology provides between 128 and 256 bits of security strength	AES-CBC: (A5908) AES-CTR: (A5908) AES-ECB: (A5908) HMAC-SHA-1: (A5908) HMAC-SHA2-256: (A5908) HMAC-SHA2-384: (A5908) HMAC-SHA2-512: (A5908) SHA-1: (A5908) SHA2-256: (A5908) SHA2-384: (A5908) SHA2-512: (A5908)
Key Derivation	CKG KAS-135KDF KBKDF PBKDF	Key Derivation Functions		KDF SSH: (A5908) KDF SP800-108: (A5908) PBKDF: (A5908) CKG - Section 4: () Key Type: Symmetric and Asymmetric

Name	Type	Description	Properties	Algorithms
TDES	BC-UnAuthDecrypt	Triple-DES Decryption (Legacy Use only)		TDES-CBC: (A5908)
KTS-2	KTS-Wrap	Key Transport using AES-GCM	Standard:SP 800-38D IG D.G:approved method from IG D.G Key confirmation :no Caveat :Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A5908)
KAS-1	CKG KAS-Full	Key Agreement in the context of TLS and SSH	IG:IG D.F Scenario 2, path (2), split Key confirmation :no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat :Key establishment methodology provides between 128 and 256 bits of security strength	KAS-ECC-SSC Sp800-56Ar3: (A5908) KDF SSH: (A5908) TLS v1.2 KDF RFC7627: (A5908) TLS v1.3 KDF: (A5908) CKG - Section 4: ()
KAS-2	CKG KAS-Full	Key Agreement in the context of TLS and SSH	IG :IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat :Key establishment methodology provides between 112 and 200 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A5908) KDF SSH: (A5908) Safe Primes Key Generation: (A5908) Safe Primes Key Verification: (A5908) TLS v1.2 KDF RFC7627: (A5908)

Name	Type	Description	Properties	Algorithms
				TLS v1.3 KDF: (A5908) CKG - Section 4: () Key Type: Symmetric and Asymmetric

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

Overall security design and the rules of operation:

- No parts of the TLS, and SSH protocols, 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 conforms to IG C.H Scenario #1 following RFC 5288 for TLS v1.2. Per RFC 5246, if the module is the party that encounters this condition, it will trigger a handshake to establish a new encryption key. The module also complies with Scenario #1 Option 2 for TLS protocol IV generation. The module performs nonce_explicit rollover check and returns an error if that condition occurs. The module supports AES-GCM cipher suites from Section 3.3.1 of SP800-52 rev2. The module's AES-GCM implementation also conforms to IG C.H Scenario #5 following RFC 8446 for TLS v1.3 and provides support for GCM cipher suites from Section 8.4 of RFC 8446. The IV is generated internally using the module's Approved DRBG.
- The module's AES-GCM implementation also conforms to IG C.H Scenario #2 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.
- The module's RSA CAVP Cert. #A5908 meets the requirements of IG C.F as approved moduli 2048, 3072 and 4096 have been tested (approved Key Generation, Signature Generation and Signature Verification). No untested moduli apply.
- IG C.M applies to the module for its usage of Three-key TDEA Decryption.

The initialization requirements for the module can be found in Section 11.1 Life-cycle Assurance in this document.

2.8 RBG and Entropy

Cert Number	Vendor Name
E199	Ciena Corporation

Table 8: 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 9: 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. The 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
• There are two implemented key agreement schemes compliant with NIST SP 800-135rev1, NIST SP 800-56Ar3 and IG D.F Scenario 2 (path (2)):

o KAS-ECC (Key Agreement Scheme Elliptic Curve Cryptography): Key Agreement Scheme – Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135r1 (CVL Cert. #A5908); provides 128, 192, 256 bits of security strength (corresponding to the P-256, P-384, P-521 curves), used in the context of the IETF TLS and SSH protocols:
KAS1: KAS (KAS-ECC-SSC Cert. #A5908 and CVL Cert. #A5908; SSP establishment methodology provides between 128 and 256 bits of encryption strength)

o KAS-FFC (Key Agreement Scheme Finite Field Cryptographic): Key Agreement Scheme Shared Secret Computation (KAS-SSC) per SP 800-56Arev3, Key Derivation per SP 800-135r1 (CVL Cert. #A5908); provides 112 and 200 bits of security strength (corresponding to the safe prime groups), used in the context of the IETF SSH and TLS protocols:
KAS2: KAS (KAS-FFC-SSC Cert.#A5908 and CVL Cert. #A5908; SSP establishment methodology provides 112 and 200 bits of encryption strength)

Key Transport
• There are two implemented key transport schemes compliant with NIST SP 800-38F and NIST SP 800-38D: 1) AES-CBC, CTR, ECB with HMAC used in the context of the IETF SSH and TLS protocols, and 2) AES-GCM
• Per IG D.G approved and allowed methods respectively are as follows:
o KTS1: KTS (AES Cert. #A5908 and HMAC Cert. #A5908; SSP establishment methodology provides between 128 and 256 bits of encryption strength)
o KTS2: KTS (AES Cert. #A5908; SSP establishment methodology provides between 128 and 256 bits of encryption strength)

2.11 Industry Protocols

The Module conforms to Resolution 2 per [FIPS140-3_IG] D.C References to the Support of Industry Protocols: while it provides [SP800-56Ar3] conformant schemes and API entry points-oriented TLS usage, the module contains full implementation of TLS. The following caveat is applicable:

- No parts of the TLS and SSH protocols, 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
Console Interface (RJ-45, UART Interface and USB-C connectors on front panel)	Control Input Status Output	Console Management
Ethernet (SGMII, Midplane connector, PCIe, & faceplate connector)	Data Input Data Output Control Input Status Output	SSHv2, TLS 1.2 and TLS 1.3 communications
Reset Button (Module faceplate)	Control Input	Reset Signal
Control pins (Midplane connector)	Control Output	Power control for the encryption MOTR
LED (Module faceplate)	Status Output	LED Active/On

Physical Port	Logical Interface(s)	Data That Passes
Power Supply (Midplane connector)	Power	Power supply/input from within the Waveserver Ai Encryption Module chassis where the module resides

Table 10: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
ECDSA Public Key Certificate	The module supports ECDSA P-256, P-384 and P-521 bit digital certificate authentication for TLS 1.2 and public key-based authentication for SSH.	SSH Authentication	The module supports ECDSA P-256, P-384 and P- 521 bit digital certificate authentication for TLS 1.2 and public key-based authentication for SSH	At most (1 ×10^10 × 60 = 6 × 10^11) 600,000,000,000 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 × 10^11 bits per minute) / 112 bits per key)) = 1: (2^112 possible keys / 535,714,2857 keys per minute) = 1: 9.69 × 10^23 which is less than 1:100,000 within one minute.
RSA Public Key Certificate	The module supports ECDSA P-256, P-384 and P-521 bit and RSA 2048, 3072- and 4096-bit digital certificate authentication for TLS 1.2 and public key-based authentication for SSH.	SSH Authentication	Using conservative estimates and equating the use of RSA with 2048 bits with 112 bits of security strength (the lowest strength offered by the module), the probability for a random attempt to succeed is: 1:2^112 or 1: 5.19 x 10^33 which is	At most (1 ×10^10 × 60 = 6 × 10^11) 600,000,000,000 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 × 10^11 bits per minute) / 112 bits per

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			less than 1:1,000,000. The fastest network connection supported by the modules over Management interfaces is 1 Gb/s	key)) = 1: (2^112 possible keys / 535,714,2857 keys per minute) = 1: 9.69 × 10^23 which is less than 1:100,000 within one minute.
Password-based	For SSH and Console the module enforces 8- character passwords (at minimum) chosen from the 96 human readable ASCII characters.	8- character passwords (at minimum) chosen from the 96 human readable ASCII character	The password can be a maximum of 128 characters. Based on the minimum password length, the probability for a random attempt to succeed is: 1:96^8 or 1: 7.21 X 10^15 Which is less than 1:1,000,000	A limit of 10 failed attempts is enforced by the module for SSH; Therefore, there can be at most 10:96^8 attempts in a one-minute period, which is less than 1:100,000

Table 11: Authentication Methods

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	ECDSA Public Key Certificate RSA Public Key Certificate Password-based

Table 12: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize and configure the module	Perform boot-up and initialization of the module, configure the module settings, Import certificates	Completion of all these activities results in a global flag indicating system is running	N/A	N/A	Integrity Test KTS-1 Key Derivation TDES KTS-2 KAS-1 KAS-2	CO - Ciena signature public key (CPK): E - Base Key Encryption Key (BKEK): E - Master Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	over SSH or the Console, Via control / data input interface (SGMII,console) Disable root account / diag shell.	in an approved mode.				Encryption Key (MKEK): E - Ciena Device ID certificate (iDevID): E - DRBG Seed (DRBG): W,E - Entropy Input (EI): W,E - TLS Public Key (TLS-PUB): G,R,W,E - TLS Private Key (TLS-Priv): G,R,W,E - TLS Master Secret (TLSMS): G,R,W,E - TLS Pre-Master Secret (TLSPMS): G,R,W,E - TLS Session Key (TLSK): G,R,W,E - TLS Authentication Key (TLSAK): G,R,W,E - ECDH Public Key (Pub-ECKP): G,R,W,E - ECDH Private Key (Priv-ECKP): G,R,W,E - DH Public Key (Pub-DHKP):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R,W,E - DH Private Key (Priv-DHKP): G,R,W,E - SSH Session MAC Key (SSHAK): G,R,W,E - SSH Encryption Key (SSHK): G,R,W,E - SSH Server Host Key (SSHHK): G,R,W,E - Customer Enrollment Certificate CUST-CERT: W,E - Password: W,E - X509 Passphrase (X509- PW): W,E - X.509 Key Encryption Key (PKIX-KEK): G - TLS Extended Master Secret (TLSEMS): G,R,W,E - Ciena Device ID private key (iDevID-priv): R - DRBG Secret C: G,E - DRBG Secret V: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure datapath encryption	Install encryption PSK or certificate for datapath encryption	Global Approved mode indicator (show status indicator)	Pre-Shared Keys (PSK)	Command Response	Module Configuration Asymmetric Key Generation KTS-1 KTS-2 KAS-1 KAS-2	CO - DPE Pre-Shared Keys (PSK): W - DPE Customer Enrollment Certificate (DPE-CERT): W - DPE Customer Enrollment Certificate Private Key (Priv-DPE-CERT): W - DPE Customer Enrollment CA Certificate (DPE-CA): W - Customer Enrollment Certificate CUST-CERT: W - Data Encryption Key (DPE-KEK): G - X.509 Key Encryption Key (PKIX-KEK): G - SSH Session MAC Key (SSHAK): G,R,W,E - SSH Encryption Key (SSHK): G,R,W,E - SSH Server Host Key (SSHHK): G,R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH User Authentication Public Key (SSHPK): G,R,W,E - DH Public Key (Pub-DHKP): G,R,W,E - DH Private Key (Priv-DHKP): G,R,W,E - ECDH Public Key (Pub-ECKP): G,R,W,E - ECDH Private Key (Priv-ECKP): G,R,W,E
Perform a Firmware Upgrade	Initiate a system wide firmware upgrade using RSA 4096 load test.	Global Approved mode indicator (show status indicator)	Load Firmware from SSD	Command response; Log generation	Firmware Upgrade KTS-1 KTS-2 KAS-1 KAS-2	CO - Ciena signature public key (CPK): E - SSH Session MAC Key (SSHAK): G,R,W,E - SSH Encryption Key (SSHK): G,R,W,E - SSH Server Host Key (SSHHK): G,R,W,E - SSH User Authentication Public Key (SSHPK): G,R,W,E - ECDH Public Key (Pub-ECKP): G,R,W,E - ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key (Priv-ECKP): G,R,W,E - DH Public Key (Pub-DHKP): G,R,W,E - DH Private Key (Priv-DHKP): G,R,W,E
Manage the encryption MOTR module	1) Select PSK for DPE peer authentication and provision the encryption MOTR. 2) Activate certificate peer authentication and provision the encryption MOTR Over the TLS 1.3 interface.	Global Approved mode indicator (show status indicator)	N/A	DPE Pre-shared Keys (PSK) or Certificate	KTS-1 KTS-2 KAS-1 KAS-2	CO - DPE Pre-Shared Keys (PSK): R - Data Encryption Key (DPE-KEK): E - X.509 Key Encryption Key (PKIX-KEK): E - DPE Customer Enrollment Certificate Private Key (Priv-DPE-CERT): R,E - DPE Customer Enrollment Certificate (DPE-CERT): R,E - DPE Customer Enrollment CA Certificate (DPE-CA): R,E - TLS Public Key (TLS-PUB): R,W,E - TLS Master Secret (TLSMS):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						R,W,E - TLS Pre-Master Secret (TLSPMS): R,W,E - TLS Private Key (TLS-Priv): R,W,E - TLS Session Key (TLSK): R,W,E - TLS Authentication Key (TLSAK): R,W,E - TLS Extended Master Secret (TLSEMS): R,W,E - DH Public Key (Pub-DHKP): R,W,E - DH Private Key (Priv-DHKP): R,W,E - ECDH Public Key (Pub-ECKP): R,W,E - ECDH Private Key (Priv-ECKP): R,W,E
Zeroise -- Secure Erase via RTFD command	Clear all SSP's and disable cryptographic output via control pins (power down of modules) (Zeroise)	Successful power cycle and the module initializes after power cycle	RTFD Command	N/A	None	CO - DRBG Seed (DRBG): Z - Entropy Input (EI): Z - ECDH Public Key (Pub-ECKP): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- ECDH Private Key (Priv-ECKP): Z - Data Encryption Key (DPE-KEK): Z - X509 Passphrase (X509- PW): Z - X.509 Key Encryption Key (PKIX-KEK): Z - TLS Authentication Key (TLSAK): Z - TLS Public Key (TLS-PUB): Z - TLS Private Key (TLS-Priv): Z - SSH Session MAC Key (SSHAK): Z - SSH Encryption Key (SSHK): Z - SSH Server Host Key (SSHHK): Z - SSH User Authentication Public Key (SSHPK): Z - DH Public Key (Pub-DHKP): Z - DH Private Key (Priv-DHKP): Z - Customer Enrollment

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Certificate CUST-CERT: Z - Password: Z - DPE Pre-Shared Keys (PSK): Z - DPE Customer Enrollment Certificate Private Key (Priv-DPE-CERT): Z - DPE Customer Enrollment Certificate (DPE-CERT): Z - TLS Session Key (TLSK): Z - TLS Pre-Master Secret (TLSPMS): Z - TLS Master Secret (TLSMS): Z - TLS Extended Master Secret (TLSEMS): Z - DRBG Secret C: Z - DRBG Secret V: Z Unauthenticated - DRBG Seed (DRBG): Z - Entropy Input (EI): Z - ECDH Public Key (Pub-ECKP):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - ECDH Private Key (Priv-ECKP): Z - Data Encryption Key (DPE-KEK): Z - X509 Passphrase (X509- PW): Z - X.509 Key Encryption Key (PKIX-KEK): Z - TLS Authentication Key (TLSAK): Z - TLS Public Key (TLS-PUB): Z - TLS Private Key (TLS-Priv): Z - SSH Session MAC Key (SSHAK): Z - SSH Encryption Key (SSHK): Z - SSH Server Host Key (SSHHK): Z - SSH User Authentication Public Key (SSHPK): Z - DH Public Key (Pub-DHKP): Z - DH Private Key (Priv-DHKP): Z - Customer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Enrollment Certificate CUST-CERT: Z - Password: Z - DPE Pre-Shared Keys (PSK): Z - DPE Customer Enrollment Certificate Private Key (Priv-DPE-CERT): Z - DPE Customer Enrollment Certificate (DPE-CERT): Z - DPE Customer Enrollment CA Certificate (DPE-CA): Z - TLS Session Key (TLSK): Z - TLS Pre-Master Secret (TLSPMS): Z - TLS Master Secret (TLSMS): Z - TLS Extended Master Secret (TLSEMS): Z - DRBG Secret C: Z - DRBG Secret V: Z
Perform operator	Authenticate operators	Global Approve	SSH Key (RSA) Or	N/A	Authentication	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
authentication	using module local database	d mode indicator (show status indicator)	SSH Key (ECDSA) Or SSH Password		KTS-1 KTS-2 KAS-1 KAS-2	- Password: W,E - TLS Public Key (TLS-PUB): R,W,E - TLS Private Key (TLS-Priv): R,W,E - TLS Master Secret (TLSMS): R,W,E - TLS Pre-Master Secret (TLSPMS): R,W,E - TLS Session Key (TLSK): R,W,E - TLS Authentication Key (TLSAK): R,W,E - ECDH Public Key (Pub-ECKP): R,W,E - ECDH Private Key (Priv-ECKP): R,W,E - DH Public Key (Pub-DHKP): R,W,E - DH Private Key (Priv-DHKP): R,W,E - SSH Session MAC Key (SSHAK): R,W,E - SSH Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key (SSHK): R,W,E - SSH Server Host Key (SSHHK): R,W,E - SSH User Authentication Public Key (SSHPK): R,W,E - TLS Extended Master Secret (TLSEMS): R,W,E
Perform on demand self-tests	Perform power-up selftests via a module reset.	Log status output	N/A	Log status output		
View module status, alarms, and statistics (Show Status)	View and monitor active alarms and module status for diagnostic purposes	Global Approved mode indicator (show status indicator)	Command	Status Output	KTS-1 KTS-2 KAS-1 KAS-2	Unauthenticated - TLS Public Key (TLS-PUB): R,W,E - TLS Private Key (TLS-Priv): R,W,E - TLS Master Secret (TLSMS): R,W,E - TLS Pre-Master Secret (TLSPMS): R,W,E - TLS Session Key (TLSK): R,W,E - TLS Authentication Key (TLSAK): R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DH Public Key (Pub-DHKP): G,R,W,E - DH Private Key (Priv-DHKP): G,R,W,E - ECDH Public Key (Pub-ECKP): G,R,W,E - ECDH Private Key (Priv-ECKP): G,R,W,E - SSH Session MAC Key (SSHAK): G,R,W,E - SSH Encryption Key (SSHK): G,R,W,E - SSH Server Host Key (SSHHK): G,R,W,E - TLS Extended Master Secret (TLSEMS): R,W,E
Display the running Firmware (Show Version)	Report the running Firmware version of the WCS-2 and the encryption MOTR.	Global Approved mode indicator (show status indicator)	Command	Command response output	KTS-1 KTS-2 KAS-1 KAS-2	Unauthenticated - SSH Session MAC Key (SSHAK): G,R,W,E - SSH Encryption Key (SSHK): G,R,W,E - SSH Server Host Key (SSHHK):

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R,W,E - SSH User Authenticatio n Public Key (SSHPK): G,R,W,E - ECDH Public Key (Pub-ECKP): G,R,W,E - ECDH Private Key (Priv-ECKP): G,R,W,E - DH Public Key (Pub-DHKP): G,R,W,E - DH Private Key (Priv-DHKP): G,R,W,E - TLS Public Key (TLS-PUB): R,W,E - TLS Private Key (TLS-Priv): R,W,E - TLS Master Secret (TLSMS): R,W,E - TLS Pre-Master Secret (TLSPMS): R,W,E - TLS Session Key (TLSK): R,W,E - TLS Extended Master Secret (TLSEMS): R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform secure file transfer	Transfer configuration file, certificate, PSK or firmware image to the module. Keys are then installed in the module.	Global Approved mode indicator (show status indicator)	DPE Pre-shared Key, Certificate or Firmware Key	N/A	KTS-1 KTS-2 KAS-1 KAS-2	CO - SSH Session MAC Key (SSHAK): R,W,E - SSH Encryption Key (SSHK): R,W,E - SSH Server Host Key (SSHHK): R,W,E - SSH User Authentication Public Key (SSHPK): R,W,E - ECDH Public Key (Pub-ECKP): R,W,E - ECDH Private Key (Priv-ECKP): R,W,E - DH Public Key (Pub-DHKP): R,W,E - DH Private Key (Priv-DHKP): R,W,E - Password: W,E
View system logs	View system status messages, events and provisioning logs locally or via syslog over TLS	Global Approved mode indicator (show status indicator)	Command	Status Output	KTS-1 KTS-2 KAS-1 KAS-2	Unauthenticated - TLS Public Key (TLS-PUB): G,R,W,E - TLS Private Key (TLS-Priv): G,R,W,E - TLS Pre-Master

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Secret (TLSPMS): G,R,W,E - TLS Session Key (TLSK): G,R,W,E - TLS Authentication Key (TLSAK): G,R,W,E - ECDH Public Key (Pub-ECKP): G,R,W,E - ECDH Private Key (Priv-ECKP): G,R,W,E - DH Public Key (Pub-DHKP): G,R,W,E - DH Private Key (Priv-DHKP): G,R,W,E - SSH Session MAC Key (SSHAK): G,R,W,E - SSH Encryption Key (SSHK): G,R,W,E - SSH Server Host Key (SSHHK): G,R,W,E - TLS Master Secret (TLSMS): G,R,W,E - SSH User Authentication Public Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(SSHPK): G,R,W,E
Perform on-demand self- tests	Perform pre-operational and conditional cryptographic algorithm self-tests on demand via module restart	Global Approved mode indicator (show status indicator)	Power-cycle/reboot	Successful module reboot	None	Unauthenticated

Table 13: Approved Services

4.4 Non-Approved Services

The module does not support non-approved services.

4.5 External Software/Firmware Loaded

The firmware load test is carried out using RSA 4096-bit signature verification. Firmware Upgrades on the WCS-2 are considered a partial replacement. This interpretation is that the upgrade is performed in multiple stages where the bootloader and kernel are first replaced, followed by the RPM installation is the second stage. Since the SSPs are stored in a different partition, they are not affected during the upgrade, and the upgrade is done within the approved mode of operation. The module version can be verified using “software show” command. Any firmware 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:

On the WCS-2, Manage the encryption module service is considered self-initiated and requires two independent actions to prevent inadvertent output. A description of the first action is “configure the module” and the second action is to perform the “system encryption enable” command.

These two actions satisfy the requirement for two independent actions which prevent inadvertent output. Only a crypto officer may enable it with the intention of initializing and configuring encryption MOTR(s).

5 Software/Firmware Security

5.1 Integrity Techniques

The WCS-2 claims EDC (SHA2-384) for the firmware integrity test. The cryptographic library used for secure boot is Waveserver Ai WCS-2 FW Crypto Library 2 tested under CAVP cert. #A5908.

5.2 Initiate on Demand

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

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	Three 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 14: Mechanisms and Actions Required

Figure 4: Top View of Ciena Waveserver Ai WCS2

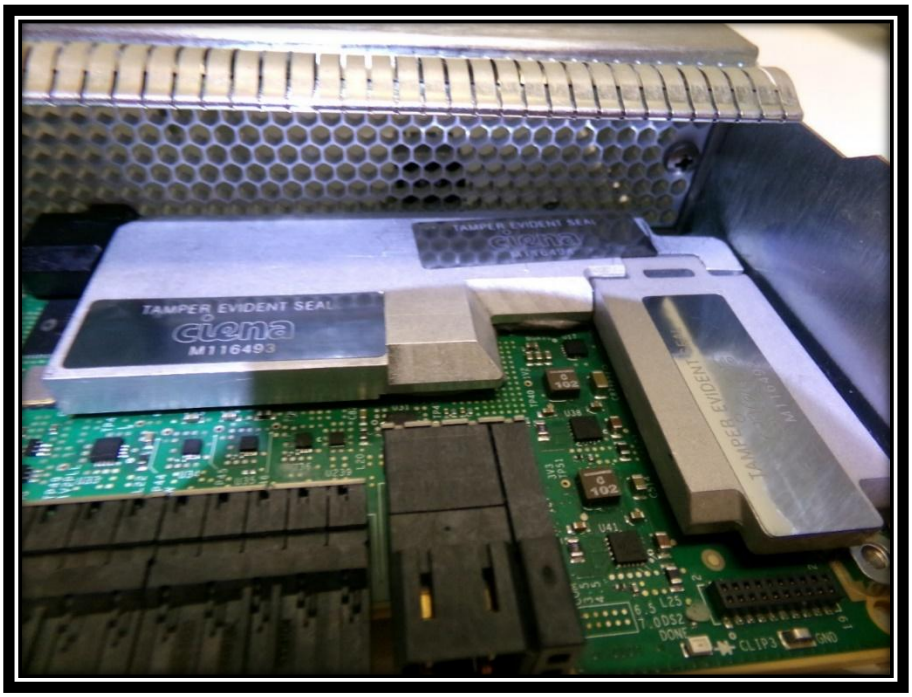


Figure 5: Placement for the three temper seals

The module is shipped from the factory with the required physical security mechanisms (tamper-evident seals, 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 follow internal security policies which include contacting Ciena.

8 Non-Invasive Security

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
Non-Volatile Memory (NVM)	Non-Volatile Memory (NVM)	Static

Table 15: 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	KTS-1
Output_1	RAM	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	KTS-1
Output_2	RAM	External (Outside of the Module's Boundary)	Plaintext	Automated	Electronic	
Input_2	External (Outside of the Module's Boundary)	RAM	Plaintext	Automated	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input_3	External (Outside of the Module's Boundary)	RAM	Encrypted	Automated	Electronic	KTS-2
Stored at manufacture - 2	Manufacturer	Non-Volatile Memory (NVM)	Plaintext	N/A	N/A	
Output_3	RAM	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	KTS-2
Output_4	Non-Volatile Memory (NVM)	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	KTS-1
Output_5	Non-Volatile Memory (NVM)	External (Outside of the Module's Boundary)	Encrypted	Automated	Electronic	KTS-2
Input_4	External (Outside of the Module's Boundary)	Non-Volatile Memory (NVM)	Encrypted	Automated	Electronic	KTS-1
Input_5	External (Outside of the Module's Boundary)	Non-Volatile Memory (NVM)	Plaintext	Automated	Electronic	
Input_6	External (Outside of the Module's Boundary)	Non-Volatile Memory (NVM)	Encrypted	Automated	Electronic	KTS-2

Table 16: 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 executed using the Push Button	SSPs in memory are cleared during 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

Zeroization Method	Description	Rationale	Operator Initiation
Secure Erase	Erase via RTFD Command	Zeroise on demand via RTFD Command	On Demand

Table 17: 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 MKEK and Ciena Device ID	AES GCM 256-bits - 256 bits	Symmetric Key - CSP			
DRBG Seed (DRBG)	Used for random number generation - SHA256 DRBG	256 bits - 256 bits	CSP - CSP	Hash DRBG (A5908)		
Entropy Input (EI)	Used for random number generation	384 bits - 384 bits	CSP - CSP	Hash DRBG (A5908)		
ECDH Public Key (Pub-ECKP)	Public key used for establishing SSH sessions	ECDSA P-256, P-384 and P-521 - 128, 192 and 256 bits	ECDH Public Key - PSP	Asymmetric Key Generation		
ECDH Private Key (Priv-ECKP)	Private key used for establishing SSH sessions	ECDSA P-256, P-384 and P-521 - 128, 192 and 256 bits	ECDH Private Key - CSP	Asymmetric Key Generation		
Master Key Encryption Key (MKEK)	Used for encrypting or decrypting DPE-KEK and PKIX-KEK	AES GCM 256-bits - 256 bits	Symmetric Key - CSP			
Ciena signature public key (CPK)	Used to authenticate the new firmware being loaded during upgrade	RSA 4096 bits - 152 bits	Signature Key - PSP			RSA SigVer (FIPS186-5) (A5908)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Ciena Device ID private key (iDevID-priv)	Used for end point authentication of TLS 1.3 to encryption MOTR	ECDSA P-521 - 256 bits	Private Key - CSP			ECDSA SigVer (FIPS186-5) (A5908)
Ciena Device ID certificate (iDevID)	Used for end point authentication of TLS 1.3 to encryption MOTR	ECDSA P-521 - 256 bits	Public Certificate - PSP			ECDSA SigVer (FIPS186-5) (A5908)
Data Encryption Key (DPE-KEK)	Used for encrypting DPE-PSK, DPE-ENTITY-PRIV	AES GCM 256-bits - 256 bits	Symmetric Key - CSP	Hash DRBG (A5908)		Module Configuration
X509 Passphrase (X509-PW)	Used to protect the private key of the x509 certificate.	AES-CBC, HMAC-SHA-256 - 256 bits	Passphrase - CSP	Hash DRBG (A5908)		
X.509 Key Encryption Key (PKIX-KEK)	Used to encrypt the X509-PW (Security Manager)	AES CBC 256-bits - 256 bits	Symmetric Key - CSP	Hash DRBG (A5908)		
TLS Authentication Key (TLSAK)	Used for authenticating TLS messages when using AES-CBC	256, 384 bits - 256, 384 bits	Authentication Key - CSP		KAS-1 KAS-2	
TLS Public Key (TLS-PUB)	TLS Public Key used during the TLS handshake process	ECDSA P-256, P-384, P-512; RSA 2048, 3072, 4096 bits - ECDSA 128, 192 and 256 bits; RSA	TLS Public Key - PSP			KAS-1 KAS-2

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		112, 128, 152,				
TLS Private Key (TLS-Priv)	TLS Private Key used during the TLS handshake process	ECDSA P-256, P-384, P-512; RSA 2048, 3072, 4096 bits - ECDSA 128, 192 and 256 bits; RSA 112, 128, 152 bits	TLS Private Key - CSP			KAS-1 KAS-2
SSH Session MAC Key (SSHAK)	It is used to authenticate all SSH data traffic between the SSH Client and SSH Server	HMAC-SHA2-256, HMAC-SHA2-512 - >= 256 bits	Symmetric Key - CSP		Key Derivation	
SSH Encryption Key (SSHK)	It is used to encrypt all SSH Data Traffic between the SSH Client and SSH Server	AES-GCM 128, 256; AES-CTR 128, 256 - 128 and 256bits	Symmetric Key - CSP		Key Derivation	
SSH Server Host Key (SSHHK)	Used to identify the host	ECDSA P-256, P-384, P-512; RSA 2048, 3072, 4096 bits - ECDSA	Public Key - CSP	Asymmetric Key Generation		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		128, 192 and 256 bits; RSA 112, 128, 152 bits				
SSH User Authentication Public Key (SSHPK)	Used for Key-based SSH Authentication	ECDSA P-256, P-384, P-512; RSA 2048, 3072, 4096 bits - ECDSA 128, 192 and 256 bits; RSA 112, 128, 152 bits	Public Key - CSP			
DH Public Key (Pub-DHKP)	Public key used for establishing SSH sessions	2048 bits - 112 bits	DH Public Key - PSP	Asymmetric Key Generation Safe Primes Key Generation (A5908)		
DH Private Key (Priv-DHKP)	Private key used for establishing SSH sessions	2048 bits - 112 bits	DH Private Key - CSP	Asymmetric Key Generation Safe Primes Key Generation (A5908)		
Customer Enrollment Certificate	Certificates used for authentication (GRPC,	ECDSA P-256, P-384,	Public Certificate - PSP	ECDSA KeyGen (FIPS186		

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CUST-CERT	Webserver, REST, Syslog, RadSec, RADIUS)	P-512; RSA 2048, 3072, 4096 bits - ECDSA 128, 192 and 256 bits; RSA 112, 128, 152 bits		-5) (A5908) RSA KeyGen (FIPS186 -5) (A5908)		
Password	Used to authenticate the CO and User	8-128 ASCII characters - N/A	Passphrase - CSP			
DPE Pre-Shared Keys (PSK)	Used by the encryption MOTR, only stored on the WCS-2	256- bit to 2048-bit - 256- bit to 2048-bit	Symmetric Key - CSP			
DPE Customer Enrollment Certificate Private Key (Priv-DPE-CERT)	Used by the encryption MOTR for remote device peer authentication	ECDSA P-256, P-384, P-512 - ECDSA 128, 192 and 256 bits	Private Key - CSP	ECDSA KeyGen (FIPS186 -5) (A5908)		
DPE Customer Enrollment CA Certificate (DPE-CA)	Used for encryption MOTR remote device peer authentication	ECDSA P-256, P-384, P-512 - ECDSA 128, 192 and 256 bits	Signature - PSP			
TLS Session Key (TLSK)	Used for encrypting/decrypting TLS messages	AES GCM 256-bits - 256 bits	Symmetric Key - CSP			KAS-1 KAS-2

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS Pre-Master Secret (TLSPMS)	Establish the TLS Master Secret	384 bits - 384 bits	Symmetric Key - CSP	TLS v1.2 KDF RFC7627 (A5908) TLS v1.3 KDF (A5908)		
TLS Master Secret (TLSMS)	Establish the TLS Session and authentication Key	384 bits - 384 bits	Symmetric Key - CSP	TLS v1.2 KDF RFC7627 (A5908) TLS v1.3 KDF (A5908)		
DPE Customer Enrollment Certificate (DPE-CERT)	Used by the encryption MOTR for remote device peer authentication	ECDSA P-256, P-384, P-512 - ECDSA 128, 192 and 256 bits	Public Certificate - PSP	ECDSA KeyGen (FIPS186-5) (A5908)		
TLS Extended Master Secret (TLSEMS)	Establish the TLS Extended Master Secret for TLS 1.2	384 bits - 384 bits	Symmetric Key - CSP	TLS v1.2 KDF RFC7627 (A5908) TLS v1.3 KDF (A5908)		
DRBG Secret C	Hash DRBG Internal State Secret C	440bits - 256bits	Entropy - CSP	Hash DRBG (A5908) SHA2-256 (A5908)		Hash DRBG (A5908)
DRBG Secret V	Hash DRBG Internal State Secret V	440bits - 256bits	Entropy - CSP	Hash DRBG (A5908) SHA2-256 (A5908)		Hash DRBG (A5908)

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Base Key Encryption Key (BKEK)	Stored at manufacture	eFUSE:Plaintext		N/A	Master Key Encryption Key (MKEK):Decrypts Ciena Device ID private key (iDevID-priv):Decrypts Ciena Device ID certificate (iDevID):Decrypts
DRBG Seed (DRBG)		RAM:Plaintext	Until Reboot or Power Cycle	Reboot or Power Cycle Secure Erase	Entropy Input (EI):Derived From
Entropy Input (EI)		RAM:Plaintext	Until Reboot or Power Cycle	Reboot or Power Cycle Secure Erase	DRBG Seed (DRBG):Used to derive
ECDH Public Key (Pub-ECKP)	Output_2	RAM:Plaintext	Zeroised after use	Reboot or Power Cycle Zeroise after use Secure Erase	ECDH Private Key (Priv-ECKP):Paired With DRBG Seed (DRBG):Derived From
ECDH Private Key (Priv-ECKP)		RAM:Plaintext	Zeroised after use	Reboot or Power Cycle Zeroise after use Secure Erase	ECDH Public Key (Pub-ECKP):Paired With DRBG Seed (DRBG):Derived From
Master Key Encryption Key (MKEK)	Stored at manufacture	Non-Volatile Memory (NVM):Encrypted		N/A	Data Encryption Key (DPE-KEK):Encrypts Data Encryption Key (DPE-KEK):Decrypts X.509 Key Encryption Key (PKIX-KEK):Encrypts X.509 Key Encryption Key

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					(PKIX-KEK):Decrypts
Ciena signature public key (CPK)	Input_1 Input_3 Input_4 Input_6	RAM:Plaintext	Zeroised after use	Reboot or Power Cycle Zeroise after use Secure Erase	
Ciena Device ID private key (iDevID-priv)	Stored at manufacture	Non-Volatile Memory (NVM):Encrypted		N/A	Ciena Device ID certificate (iDevID):Paired With
Ciena Device ID certificate (iDevID)	Stored at manufacture	Non-Volatile Memory (NVM):Encrypted		N/A	Ciena Device ID private key (iDevID-priv):Paired With
Data Encryption Key (DPE-KEK)	Output_1 Output_3 Output_4 Output_5	Non-Volatile Memory (NVM):Encrypted		Secure Erase	DRBG Seed (DRBG):Derived From
X509 Passphrase (X509- PW)	Input_1 Input_2 Input_3 Input_4 Input_5 Input_6	Non-Volatile Memory (NVM):Encrypted		Secure Erase	DRBG Seed (DRBG):Derived From
X.509 Key Encryption Key (PKIX-KEK)		Non-Volatile Memory (NVM):Encrypted		Secure Erase	DRBG Seed (DRBG):Paired With X509 Passphrase (X509-PW):Encrypts
TLS Authentication Key (TLSAK)		RAM:Plaintext	Until Reboot or Power Cycle	Reboot or Power Cycle Secure Erase	
TLS Public Key (TLS-PUB)		RAM:Plaintext	Until Reboot or Power Cycle	Reboot or Power Cycle	TLS Private Key (TLS-Priv):Paired With
TLS Private Key (TLS-Priv)		RAM:Plaintext	Until Reboot or	Reboot or Power Cycle	TLS Public Key (TLS-PUB):Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			Power Cycle		
SSH Session MAC Key (SSHAK)		RAM:Plaintext	Zeroized after use	Reboot or Power Cycle Zeroise after use Secure Erase	
SSH Encryption Key (SSHK)	Output_1 Output_3 Output_4 Output_5	RAM:Plaintext	Zeroized after use	Reboot or Power Cycle Zeroise after use Secure Erase	
SSH Server Host Key (SSHHK)	Input_2 Input_5	Non-Volatile Memory (NVM):Plaintext		Secure Erase	
SSH User Authentication Public Key (SSHPK)	Input_2 Input_5	Non-Volatile Memory (NVM):Plaintext		Secure Erase	
DH Public Key (Pub-DHKP)	Output_2	RAM:Plaintext	Zeroized after use	Reboot or Power Cycle Zeroise after use Secure Erase	DH Private Key (Priv-DHKP):Paired With
DH Private Key (Priv-DHKP)		RAM:Plaintext	Zeroized after use	Reboot or Power Cycle Zeroise after use Secure Erase	DH Public Key (Pub-DHKP):Paired With
Customer Enrollment Certificate CUST-CERT	Input_1 Input_3 Input_4 Input_6	Non-Volatile Memory (NVM):Encrypted		Secure Erase	
Password		Non-Volatile Memory (NVM):Obfuscated		Secure Erase	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DPE Pre-Shared Keys (PSK)		Non-Volatile Memory (NVM):Encrypted		Secure Erase	
DPE Customer Enrollment Certificate Private Key (Priv-DPE-CERT)	Input_1 Input_3 Input_4 Input_6	Non-Volatile Memory (NVM):Encrypted		Secure Erase	
DPE Customer Enrollment CA Certificate (DPE-CA)	Input_1 Input_3 Input_4 Input_6	Non-Volatile Memory (NVM):Plaintext		Secure Erase	
TLS Session Key (TLSK)		RAM:Plaintext	Until Reboot or Power Cycle	Reboot or Power Cycle	TLS Master Secret (TLSMS):Derived From
TLS Pre-Master Secret (TLSPMS)		RAM:Plaintext		Reboot or Power Cycle	DRBG Seed (DRBG):Derived From TLS Master Secret (TLSMS):Used to derive
TLS Master Secret (TLSMS)		RAM:Plaintext	Until Reboot or Power Cycle	Reboot or Power Cycle	TLS Pre- Master Secret (TLSPMS):Derived From
DPE Customer Enrollment Certificate (DPE- CERT)	Input_1 Input_3 Input_4 Input_6	Non-Volatile Memory (NVM):Plaintext		Secure Erase	
TLS Extended Master Secret (TLSEMS)		RAM:Plaintext		Secure Erase	
DRBG Secret C		RAM:Plaintext	Zeroized after use	Reboot or Power Cycle Zeroise	DRBG Seed (DRBG):Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				after use Secure Erase	
DRBG Secret V		RAM:Plaintext	Zeroized after use	Reboot or Power Cycle Zeroise after use Secure Erase	DRBG Seed (DRBG):Derived From

Table 19: 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	Log status output	Verify integrity of the firmware.

Table 20: 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

N/A for this module.

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 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-5) (A5908) - P=521	KAT	CAST	On-Demand	Manually, Power-cycling the module

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-384 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
AES-CBC (A5908) - Encrypt - 256-bits	KAT	CAST	On-Demand	Manually, Power-cycling the module
AES-CBC (A5908) - Decrypt - 256-bits	KAT	CAST	On-Demand	Manually, Power-cycling the module
AES-GCM (A5908) - Encrypt - 256 bits	KAT	CAST	On-Demand	Manually, Power-cycling the module
AES-GCM (A5908) - Decrypt - 256 bits	KAT	CAST	On-Demand	Manually, Power-cycling the module
TDES-CBC (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
SHA-1 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
SHA2-256 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
SHA2-512 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
HMAC-SHA-1 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
HMAC-SHA2-256 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
HMAC-SHA2-384 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
HMAC-SHA2-512 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
KAS-ECC-SSC Sp800-56Ar3 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
KAS-FFC-SSC Sp800-56Ar3 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
ECDSA SigGen (FIPS186-5) (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
ECDSA SigVer (FIPS186-5) (A5908) - P-256 - SHA2-256	KAT	CAST	On-Demand	Manually, Power-cycling the module
ECDSA SigVer (FIPS186-5) (A5908) - P-521 - SHA2-384	KAT	CAST	On-Demand	Manually, Power-cycling the module
RSA SigGen (FIPS186-5) (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
RSA SigVer (FIPS186-5) (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
PBKDF (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
KDF SP800-108 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
TLS v1.2 KDF RFC7627 (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
KDF SSH (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
TLS v1.3 KDF (A5908)	KAT	CAST	On-Demand	Manually, Power-cycling the module
ECDSA KeyGen (FIPS186-5) (A5908)	PCT	CAST	On-Demand	Programmatically, when generating ECDSA key pair
RSA KeyGen (FIPS186-5) (A5908)	PCT	CAST	On-Demand	Programmatically, when generating RSA key pair
ECDSA KeyVer (FIPS186-5) (A5908)	KAT	CAST	On-Demand	Power-cycling the module
Hash DRBG (A5908)	KAT	CAST	On-Demand	Power-cycling the module

Table 22: 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	Reboot or Power Cycle	Status Log
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 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 or conditional self-tests	N/A	A permanent error status will be relayed via the status output interface (Module will be stuck in infinite boot loop)

Table 23: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The CO is responsible for configuring, maintaining, and monitoring the status of the module to ensure that it is running in its 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 of the module, which includes configuring the Datapath parameters and certificates. The CO must:

1. Configure a password for the default account. The CO can optionally create additional accounts.
2. All operator passwords must be a minimum of 8 characters in length.
3. 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.
4. Ensure use of 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
5. Ensure all management traffic is encapsulated within a trusted session
6. For SSH, ensure Group 14 or stronger is selected for Diffie-Hellman
7. Install the PSK or X.509 certificate authentication material
8. Set up Syslog (over TLS) and RADIUS over TLS
9. Disable remote authentication
10. Disable the root account and shell access.
11. The configuration shall be saved once completed

When configured according to this guidance the module only runs in the 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 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.

11.2 Administrator Guidance

For Administrator Guidance (CO user), refer to Ciena's User Guide which can be obtained by contacting Ciena. No additional guidance is required for enabling the Approved mode of operation apart from the guidance in this security policy.

11.3 Non-Administrator Guidance

For Non-Administrator Guidance (unauthenticated user), refer to Ciena's User Guide which can be obtained by contacting Ciena. No additional guidance is required for enabling the Approved mode of operation 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.