Ciena Corporation

Waveserver 5 Control Processor Module

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General 4
1.1 Overview 4
1.2 Security Levels 6
1.3 Additional Information 6
2 Cryptographic Module Specification 6
2.1 Description 6
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 9
2.4 Modes of Operation 9
2.5 Algorithms 9
2.6 Security Function Implementations 12
2.7 Algorithm Specific Information 18
2.8 RBG and Entropy 19
2.9 Key Generation 20
2.10 Key Establishment 20
2.11 Industry Protocols 20
3 Cryptographic Module Interfaces 20
3.1 Ports and Interfaces 20
4 Roles, Services, and Authentication 21
4.1 Authentication Methods 21
4.2 Roles 23
4.3 Approved Services 24
4.4 Non-Approved Services 54
4.5 External Software/Firmware Loaded 54
4.6 Cryptographic Output Actions and Status 54
5 Software/Firmware Security 54
5.1 Integrity Techniques 54
5.2 Initiate on Demand 54
6 Operational Environment 54
6.1 Operational Environment Type and Requirements 54
7 Physical Security 55
7.1 Mechanisms and Actions Required 55
8 Non-Invasive Security 57
8.1 Mitigation Techniques 57
9 Sensitive Security Parameters Management 57

9.1 Storage Areas 57
9.2 SSP Input-Output Methods 57
9.3 SSP Zeroization Methods 59
9.4 SSPs 59
10 Self-Tests 71
10.1 Pre-Operational Self-Tests 71
10.2 Conditional Self-Tests 72
10.3 Periodic Self-Test Information 78
10.4 Error States 79
11 Life-Cycle Assurance 81
11.1 Installation, Initialization, and Startup Procedures 81
11.2 Administrator Guidance 81
11.3 Non-Administrator Guidance 82
11.5 Maintenance Requirements 82
11.6 End of Life 82
11.7 Additional Information 82
12 Mitigation of Other Attacks 82
12.1 Attack List 82

List of Tables

Table 1: Security Levels 6
Table 2: Tested Module Identification – Hardware 9
Table 3: Modes List and Description 9
Table 4: Approved Algorithms 11
Table 5: Vendor-Affirmed Algorithms 11
Table 6: Non-Approved, Allowed Algorithms with No Security Claimed 12
Table 7: Security Function Implementations 18
Table 8: Entropy Certificates 19
Table 9: Entropy Sources 19
Table 10: Ports and Interfaces 20
Table 11: Authentication Methods 23
Table 12: Roles 24
Table 13: Approved Services 53
Table 14: Mechanisms and Actions Required 55
Table 15: Storage Areas 57
Table 16: SSP Input-Output Methods 59
Table 17: SSP Zeroization Methods 59
Table 18: SSP Table 1 65
Table 19: SSP Table 2 71
Table 20: Pre-Operational Self-Tests 72
Table 21: Conditional Self-Tests 77
Table 22: Pre-Operational Periodic Information 78
Table 23: Conditional Periodic Information 79
Table 24: Error States 80

List of Figures

Figure 1: Ciena Waveserver 5 Chassis 7
Figure 2: Block Diagram 7
Figure 3: Waveserver 5 Control Processor Module Cryptographic Boundary 8
Figure 4: Waveserver 5 Control Processor Module (Front and Rear) 8
Figure 5: Location of Tamper Seal Placement on the Waveserver 5 Control Processor Module 56

1 General

1.1 Overview

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation

Program (CMVP) run the FIPS 140-3 program. The NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program

About this Document

This non-proprietary Cryptographic Module Security Policy for the Waveserver 5 Control Processor Module provides an overview of the product and a high-level description of how it meets the overall Level 2 security requirements of FIPS 140-3.

The Waveserver 5 Control Processor Module may also be referred to as the “CP” or “module” in this document.

Disclaimer

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

Notices

This document may be freely reproduced and distributed in its entirety without modification.

Scope

This non-proprietary document describes the cryptographic module security policy for the Waveserver 5 Control Processor Module (Hardware version: 186-3011-900 revision 001 and revision 002 and 186- 3011-901 revision 001 and revision 002, Firmware Version 2.4.52). The two part numbers are equivalent and just used to differentiate the manufacturing process and sites. It contains specification of the security rules under which the cryptographic module operates, including those derived from the requirements of the FIPS 140-3 standard.
The Waveserver 5 Control Processor 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 5 chassis. Its primary function is management of the Waveserver 5 chassis, which includes one or more Waveserver 5 Encryption Modules.

The major components of the module include a Marvell CN9130 System on a Chip (SOC) with external DDR memory, an SSD, a CPLD (Complex Programmable Logic Device), and FPGA (Field-Programmable Gate Arrays). The module is installed inside the Waveserver 5 chassis and is attached to other Waveserver subsystems via a host connector, PCIe, Ethernet, serial, and USB-C.

The module is shipped in factory state and the module is explicitly configured to operate in an Approved mode of operation. Section 14 provides additional information for configuring the module in the Approved mode of operation.

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	3
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

1.3 Additional Information

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. The 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 Encryption Module via TLS v1.3. All communication to the module via its management interface is 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 Figure 2 below provides a block diagram of the module, depicting the major components of the module and the cryptographic boundary as shown in red.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Figure 1 below depicts the Waveserver 5 chassis, which consists of a CP card and up to four Encryption Modules. The validated module i.e., the Control Processor (CP card), is a multi-chip embedded embodiment housed in the Waveserver 5 chassis; the module components are completely enclosed within a hard metal clamshell cover with tamper evident labels applied. The Ciena Control Processor (CP) forms the Trusted Operational Environment's Physical Perimeter (TOEPP) for the module.

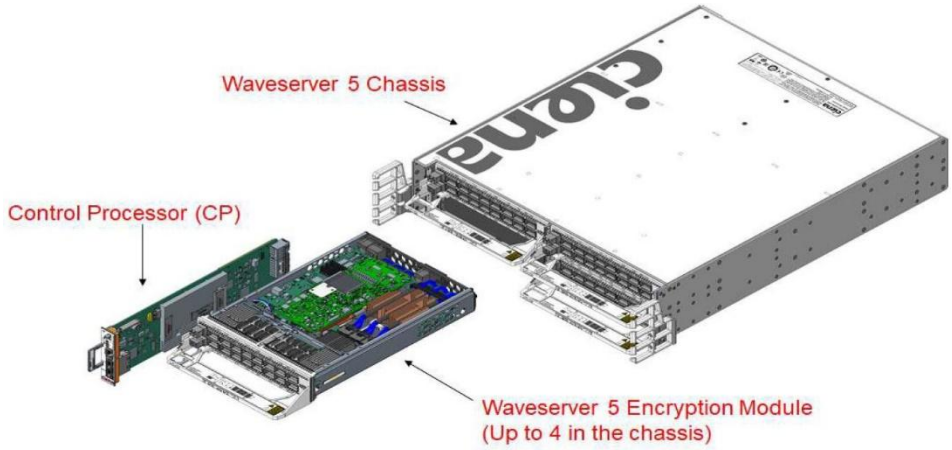


Figure 1: Ciena Waveserver 5 Chassis

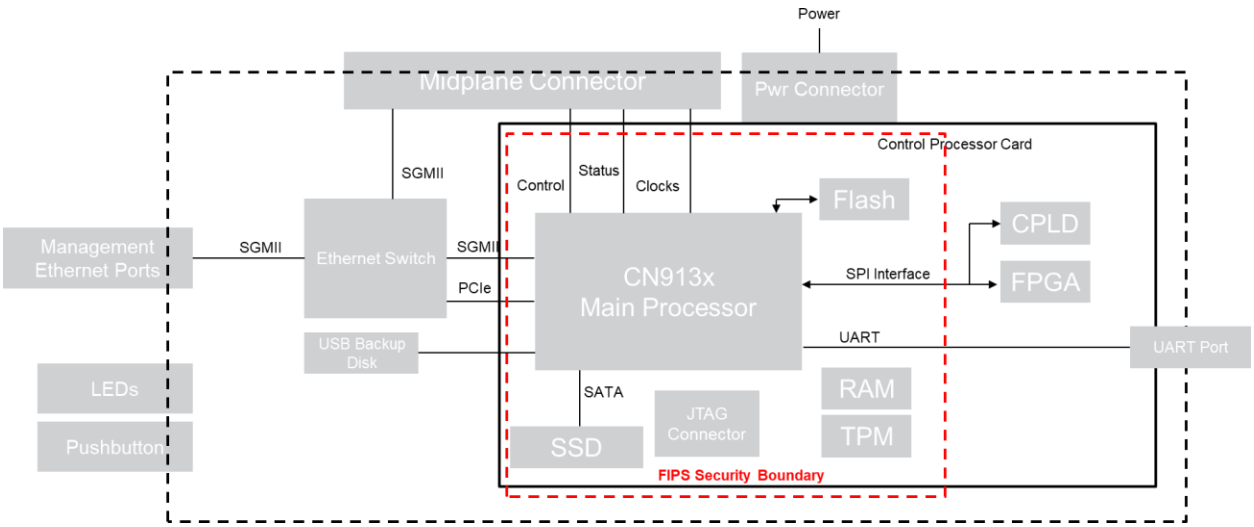


Figure 2: Block Diagram



Figure 3: Waveserver 5 Control Processor Module Cryptographic Boundary



Figure 4: Waveserver 5 Control Processor Module (Front and Rear)

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
186-3011-900	revision 001 and revision 002	2.4.52	Marvell CN9130	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
186-3011-901	revision 001 and revision 002	2.4.52	Marvell CN9130	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 module components have been excluded from the cryptographic boundary.

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 using the instructions provided in Section 11	Approved	Approved mode indication (command: "system environment show" and "system encryption show")

Table 3: Modes List and Description

The module does not support a non-approved mode.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-CTR, AES-ECB	A4855	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-CTR, AES-ECB	A3283	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-GCM	A3283	Direction - Decrypt, Encrypt IV Generation - External Key Length - 256	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
AES-GCM	A4855	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256	SP 800-38D
ECDSA KeyGen (FIPS186-4)	A4855	Curve - P-256, P-384, P-521 Secret Generation Mode - Testing Candidates	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A4855	Curve - P-256, P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4), ECDSA SigVer (FIPS186-4)	A4855	Curve - P-256, P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4
Hash DRBG	A4855	Prediction Resistance - No Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA-1	A4855	Key Length - Key Length: 112-2048 Increment 8	FIPS 198-1
HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	A4855	Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4855	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	A4855	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	A4855	KDF Mode - Feedback Supported Lengths - Supported Lengths: 256	SP 800-108 Rev. 1
KDF SSH (CVL)	A4855	Cipher - AES-128, AES-192, AES-256 Hash Algorithm - SHA-1, SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
PBKDF	A4855	Iteration Count - Iteration Count: 4096 Password Length - Password Length: 14-128 Increment 1	SP 800-132
RSA KeyGen (FIPS186-4)	A4855	Key Generation Mode - B.3.3 Modulo - 2048, 3072, 4096 Primality Tests - Table C.2 Private Key Format - Standard	FIPS 186-4
RSA SigGen (FIPS186-4), RSA SigVer (FIPS186-4)	A4855	Signature Type - PKCS 1.5 Modulo - 2048, 3072, 4096	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
Safe Primes Key Generation, Safe Primes Key Verification	A4855	Safe Prime Groups - ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048	SP 800-56A Rev. 3
SHA-1, SHA2-256, SHA2-384, SHA2-512	A4855	Message Length - Message Length: 0-65528 Increment 8	FIPS 180-4
TDES-CBC	A4855	Direction - Decrypt	SP 800-67 Rev. 2
TLS v1.2 KDF RFC7627 (CVL)	A4855	Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A4855	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 6.2.2 Symmetric Keys Derived from a Pre-existing Key; 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 algorithms that are allowed for use within an Approved mode of operation.

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
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

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

Non-Approved, Not Allowed Algorithms:

The module does not support Non-Approved Algorithms Not Allowed in the Approved Mode of Operation.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Firmware Upgrade	DigSig-SigVer SHA	Perform system wide firmware upgrade		ECDSA SigVer (FIPS186-4): (A4855) SHA2-384: (A4855)
TLS	AsymKeyPair-KeyGen AsymKeyPair-KeyVer BC-Auth BC-UnAuth CKG DigSig-SigGen DigSig-SigVer DRBG KAS-135KDF KAS-SSC MAC	Cryptography used in the context of TLS 1.2/TLS 1.3 sessions		ECDSA KeyGen (FIPS186-4): (A4855) ECDSA KeyVer (FIPS186-4): (A4855) ECDSA SigGen (FIPS186-4): (A4855) ECDSA SigVer (FIPS186-4): (A4855) KAS-ECC-SSC Sp800-56Ar3: (A4855) RSA KeyGen (FIPS186-4): (A4855) RSA SigGen (FIPS186-4): (A4855) RSA SigVer (FIPS186-4): (A4855) TLS v1.2 KDF RFC7627:

Name	Type	Description	Properties	Algorithms
				(A4855) TLS v1.3 KDF: (A4855) AES-ECB: (A3283, A4855) AES-GCM: (A3283, A4855) AES-CBC: (A4855) HMAC-SHA2-256: (A4855) HMAC-SHA2-384: (A4855) Hash DRBG: (A4855) KAS-FFC-SSC Sp800-56Ar3: (A4855) CKG - Section 4: () Key Type: Symmetric and Asymmetric AES-CTR: (A3283)
Manage the Encryption Modem (Perform approved security functions)	BC-UnAuth DigSig-SigVer DRBG	Manage the directly connected Encryption Modem using TLS 1.3 Select PSK for DPE peer authentication and provision the modem or Activate certificate peer authentication and provision the modem Over the TLS 1.3 interface		AES-CBC: (A4855) Hash DRBG: (A4855) ECDSA SigVer (FIPS186-4): (A4855)
Import/Install Certificate	DigSig-SigVer	Install customer certificates using SSH		ECDSA SigVer (FIPS186-4): (A4855) RSA SigVer

Name	Type	Description	Properties	Algorithms
				(FIPS186-4): (A4855)
Activate PSK	BC-Auth BC-UnAuth	Activate a PSK for DPE peer authentication via control / data output interface (SGMII)		AES-ECB: (A3283) AES-GCM: (A3283) AES-CTR: (A3283)
Secure Backup (Perform approved security functions)	BC-UnAuth DigSig-SigVer DRBG MAC PBKDF	Activate and perform periodic backup of the CSPs or restore CSPs from the secure backup		ECDSA SigVer (FIPS186-4): (A4855) PBKDF: (A4855) Hash DRBG: (A4855) HMAC-SHA2-384: (A4855) AES-CBC: (A4855) RSA SigVer (FIPS186-4): (A4855)
Perform on demand self-tests	BC-Auth BC-UnAuth DigSig-SigGen DigSig-SigVer DRBG KAS-SSC MAC PBKDF SHA	Perform Self-tests on demand via module restart		ECDSA SigGen (FIPS186-4): (A4855) ECDSA SigVer (FIPS186-4): (A4855) AES-CBC: (A4855) AES-CTR: (A4855) AES-ECB: (A4855) AES-GCM: (A4855, A3283) Hash DRBG: (A4855) TLS v1.3 KDF: (A4855) RSA SigGen

Name	Type	Description	Properties	Algorithms
				(FIPS186-4): (A4855) RSA SigVer (FIPS186-4): (A4855) HMAC-SHA-1: (A4855) HMAC-SHA2-256: (A4855) HMAC-SHA2-384: (A4855) HMAC-SHA2-512: (A4855) SHA-1: (A4855) PBKDF: (A4855) SHA2-256: (A4855) SHA2-512: (A4855) TLS v1.2 KDF RFC7627: (A4855) KDF SSH: (A4855) KAS-FFC-SSC Sp800-56Ar3: (A4855) TDES-CBC: (A4855) KAS-ECC-SSC Sp800-56Ar3: (A4855) KDF SP800-108: (A4855) CKG - Section 4: () Key Type: Symmetric and Asymmetric

Name	Type	Description	Properties	Algorithms
SSH	AsymKeyPair-KeyGen AsymKeyPair-KeyVer BC-Auth BC-UnAuth CKG DigSig-SigGen DigSig-SigVer DRBG KAS-135KDF KAS-SSC MAC	Cryptography used in the context of SSH sessions		AES-CBC: (A4855) AES-CTR: (A4855) AES-ECB: (A4855) AES-GCM: (A4855) ECDSA KeyGen (FIPS186-4): (A4855) ECDSA KeyVer (FIPS186-4): (A4855) ECDSA SigGen (FIPS186-4): (A4855) ECDSA SigVer (FIPS186-4): (A4855) Hash DRBG: (A4855) HMAC-SHA2-256: (A4855) HMAC-SHA2-384: (A4855) HMAC-SHA2-512: (A4855) KAS-ECC-SSC Sp800-56Ar3: (A4855) KAS-FFC-SSC Sp800-56Ar3: (A4855) KDF SSH: (A4855) RSA KeyGen (FIPS186-4): (A4855)

Name	Type	Description	Properties	Algorithms
				RSA SigGen (FIPS186-4): (A4855) RSA SigVer (FIPS186-4): (A4855) CKG - Section 4: () Key Type: Symmetric and Asymmetric
KAS-1	KAS-Full	NIST SP 800- 56Arev3 Key Agreement in the context of SSH and TLS; KAS-ECC-SSC per IG D.F Scenario 2 path (2): P-256, P-384 and P521curves providing 128 bits, 192 bits and 256 bits of encryption strength	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: (A4855) KDF SSH: (A4855) TLS v1.2 KDF RFC7627: (A4855) TLS v1.3 KDF: (A4855)
KAS-2	KAS-Full	NIST SP 800- 56Arev3 Key Agreement in the context of SSH and TLS; KAS-FFC-SSC per IG D.F Scenario 2 path (2): 2048, 3072, 4096, 6144, 8192-bit keys with 112, 192, 152, 176, 200 bits of encryption strength	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: (A4855) KDF SSH: (A4855) Safe Primes Key Generation: (A4855) Safe Primes Key Verification: (A4855) TLS v1.2 KDF RFC7627: (A4855) TLS v1.3 KDF: (A4855)

Name	Type	Description	Properties	Algorithms
KTS-1	KTS-Wrap	SP 800-38D and SP 800- 38F; Key Transport (Wrapping) in the context of SSH and TLS per IG D.G: 128, 192, and 256- bit keys providing 128, 192, or 256 bits of encryption strength	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: (A4855) AES-CTR: (A4855) HMAC-SHA-1: (A4855) HMAC-SHA2-256: (A4855) HMAC-SHA2-384: (A4855) HMAC-SHA2-512: (A4855) SHA-1: (A4855) SHA2-256: (A4855) SHA2-384: (A4855) SHA2-512: (A4855)
KTS-2	KTS-Wrap	SP 800-38D and SP 800- 38F; Exits the module in optional security backup, encrypted with BAKKEY: 256- bit keys providing 256 bits of encryption strength	Standard :SP 800-38D IG D.G: approved method from IG D.G Key confirmation :no Caveat :Key establishment methodology provides 256 bits of security strength	AES-GCM: (A4855)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

• 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 supports Sections 4, 5.1, 5.2, 6.1, 6.2.1, 6.2.3 per NIST SP 800-133r2.
• The module's AES-GCM implementation conforms to IG C.H Scenario #1 following RFC 5288 for TLS v1.2. The operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. The counter portion of the IV is set by the module within its cryptographic boundary.

The module supports AES-GCM cipher suites from Section 3.3.1 of SP800-52 rev2. The implementation of the nonce_explicit management logic inside the module ensures that when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key (e.g., a 64-bit counter starting from 0 and increasing, when it reaches the maximum value of 2^64 -1), either party (the client or the server) that encounters this condition triggers a handshake to establish a new encryption key (per Sections 7.4.1.1 and 7.4.1.2 in RFC 5246).
• 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 and will only be used in the context of the AES-GCM encryption in the context of the TLS v1.3 protocol.
• 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 only supports testable RSA moduli/key sizes (2048 and 4096 bits) and thus the requirements per FIPS 140-3 IG C.F do not apply.
• The module implements a CAVP compliance tested key derivation function compliant to NIST SP800- 132 KDF (PBKDF). The password consists of at least 14-128 bits. The probability that a random attempt will end up with the same output is: 1/(2^14) = 0.00006 (using a minimum size for the password). PBKDFv2 is implemented to support option 1 a per SP800-132. The iteration count is 4086 bits. This is in accordance with NIST SP 800-132 which recommends that iteration count should be selected as large as possible, as long as the time required to generate the key using the entered password is acceptable for the users. The derived keys may only be used in storage applications.
• In accordance with IG 2.4.B, the CVLs i.e. SSH KDF, TLS 1.2 KDF and TLS 1.3 KDF shall only be used in the context of the respective protocols.
• In accordance with IG C.M, the usage of Triple-DES decryption is permitted for legacy purposes.
• The module conforms to Scenario 1 (a) described in FIPS 140-3 IG 9.3A. The entropy source produces sufficient entropy to generate keys of the largest size supported by the module i.e. 256 bits.
• IG C.M applies to the module for its usage of Three-key TDEA Decryption.

2.8 RBG and Entropy

Cert Number	Vendor Name
E23	Ciena Corporation

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Trusted Platform Module 2.0 SLB 9672	Physical	Infineon SLB 9672 security controller IC	8 bits	7.5173 bits	

Table 9: Entropy Sources

The module is a hardware module with an entropy generating SRNG inside the module's cryptographic boundary consistent with Scenario 1 (a) described in FIPS 140-3 IG 9.3A. The

entropy source produces sufficient entropy to generate keys of the largest size supported by the module i.e. 256 bits.

2.9 Key Generation

The module generates keys as described in SP800-133 rev2 Section 4, Option #1. It uses an Approved Hash DRBG (as specified in SP800-90Arev1) to generate symmetric keys and seed for asymmetric keys. The DRBG is seeded from seeding material provided by a hardware based SRNG (Infineon SLB9672 SRNG), which provides an entropy source and unbiased random sequence of bits to the DRBG.

2.10 Key Establishment

The module supports the key establishment mechanisms as defined in the Security Functions Implementation Table in this document, namely: KAS-1, KAS-2, KTS-1 and KTS-2.

2.11 Industry Protocols

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

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Console Interface (Console and USB-C connectors on front panel)	Control Input Status Output	Console Management
Ethernet (SGMII, DCN-1, DCN-2, Backplane Connector & PCIe)	Data Input Data Output Control Input Control Output Status Output	SSHv2, TLS 1.2 and TLS 1.3 communications
Internal USB on the backplane connector	Data Input Data Output	Secure Backup Operation
Reset Button	Control Input	Reset Signal
Status LEDs	Status Output	LED Active/On
Power Supply	Power	Power supply/input from within the Waveserver 5 chassis where the module resides

Table 10: Ports and Interfaces

The module supports the following physical ports and interfaces:

- UART interface (providing connectivity to external Console port)
- USB-C console interface
- 10/100/1000 Base-T Ethernet interface (providing connectivity to internal chassis components and the external DCN-1/DCN-2 physical ports)
- Reset button
- Status LEDs

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Public Key Certificates (TLS/HTTPS) Public key-based authentication (SSH) - ECDSA	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.	ECDSA SigVer (FIPS186-4) (A4855)	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; 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 less than 1:1,000,000. The fastest network connection supported by the modules over Management interfaces is 10 Gb/s	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.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Public Key Certificates (TLS/HTTPS) Public key-based authentication (SSH) - RSA	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.	RSA SigVer (FIPS186-4) (A4855)	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; 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 less than 1:1,000,000. The fastest network connection supported by the modules over Management interfaces is 10 Gb/s	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.
Password-based	For HTTPS, 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 and HTTPS; Therefore, there can be at most 10:96^8 attempts in a one-minute period, which is less than 1:100,000
Initial Device ID (iDevID)	This is for the communication	ECDSA SigVer	This is for the communication	At most 10 ×10^9 × 60 = 6 × 10^11 =

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
and Local Device ID (LDevID) Public Key	between module and encryption modem using TLS 1.3.	(FIPS186-4) (A4855)	between module and encryption modem using TLS 1.3; Using conservative estimates and equating the use of ECDSA with P-521 elliptic curve to a 256-bit symmetric key, the probability for a random attempt to succeed is: 1:2^256 or 1: 1.16 x 10^77 which is less than 1:1,000,000; The fastest network connection supported by the modules over Management interfaces is 10 Gb/s.	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: (2^256 possible keys / ((6 × 10^11 bits per minute) / 256 bits per key)) 1: (2^256 possible keys / 2,343,750,000 keys per minute) 1: 4.9 x 10^67 which is less than 1:100,000 within one minute

Table 11: Authentication Methods

The module supports both role-based and identity-based authentication. Module operators must authenticate before being allowed access to services that require the assumption of an authorized role. The module authenticates an operator using password or operator public key. Authentication is achieved by initiating a console, SSH, or TLS/HTTPS session. Digital certificates and public keys are used for SSH and TLS authentication. The strength calculations below provide the minimum strength based on the public key or password.

The module employs the authentication methods described in Table 7 above to authenticate Crypto Officers.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO (Role-based)	Role	Crypto Officer	Public Key Certificates (TLS/HTTPS) Public key-based authentication (SSH) - ECDSA Public Key Certificates (TLS/HTTPS) Public key-based authentication (SSH) - RSA Initial Device ID (iDevID) and Local Device ID (LDevID) Public Key

Name	Type	Operator Type	Authentication Methods
CO (Identity-based)	Identity	Crypto Officer	Password-based

Table 12: Roles

The module supports one authorized role: Crypto Officer role. The CO role is responsible for module initialization and module configuration, including security parameters, key management, status activities, and audit review. The CO role is able to configure and monitor the module via a console, HTTPS or SSH connection.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure PSK and certificate	Set to PSK mode and provision the PSK or set to certificate mode and provision the certificate 32-256 bytes	Global Approved mode indicator (show status indicator)	N/A	Global Approved mode indicator (show status indicator)	None	
Firmware Upgrade (Perform approved security functions)	Perform system wide firmware upgrade	Command response Log generation	Command	Command response	Firmware Upgrade	CO (Role-based) - Ciena Signature Public key: E CO (Identity-based) - Ciena Signature Public key: E
View/Display the firmware version of the module (Show module's versioning information - Show Version)	Report the running firmware version of the module	Command response	Command	Command response	None	CO (Role-based) CO (Identity-based)
Initialize and configure	Perform initialization of the module	Module status show	SSPs, Commands	Command	TLS SSH KAS-1	CO (Role-based) - Base Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
the module (Perform approved security functions)	Configure the module settings, Import certificates over SSH or the Console, Setup data path encryption modem, HTTPS keys etc. Via control / data input interface (SGMII,console) Perform require operations to enter Approved mode Configure encryption PSK or certificate	command. Event Log generation Command response Approved mode indication (command: "system environment show" and "system encryption show")		response, SSPs	KAS-2 KTS-1 KTS-2	Encryption Key (BKEK) CSP: E - Master Key Encryption Key (MKEK) CSP: E - Ciena Device ID private key (iDevID- priv) CSP: E - COID_P RIV CSP: G,E - COID_PUB PSP: G,E - Data Encryption Key (DPE-KEK) CSP: G,E - DRBG Seed CSP: G,E,Z - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP: G,R,E,Z - TLS Private key CSP: G,E,Z - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authenticatio n Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Password CSP: W,E - DPE Customer Enrollment Certificate (DPE- CERT) PSP: G,W,E - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: R,W,E - Ciena Signature Public key: E - X.509 Key Encryption Key (PKIX-KEK) CSP: G - LDEVID_ PUB PSP: R,W,E - Customer Enrollment Certificate (CUST-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						CERT) PSP: G,W,E - Entropy Input CSP: G,E,Z - DRBG C CSP: G,E,Z - DRBG V CSP: G,E,Z CO (Identity-based) - Base Key Encryption Key (BKEK) CSP: E - Master Key Encryption Key (MKEK) CSP: E - Ciena Device ID private key (iDevID- priv) CSP: E - COID_P RIV CSP: G,E - COID_PUB PSP: G,E - Data Encryption Key (DPE-KEK) CSP: G,E - DRBG Seed CSP: G,E,Z - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key PSP: G,R,E,Z - TLS Private key CSP: G,E,Z - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Password CSP: W,E - DPE Customer Enrollment Certificate (DPE- CERT) PSP: G,W,E - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: R,W,E - Ciena Signature

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public key: E - X.509 Key Encryption Key (PKIX-KEK) CSP: G - LDEVID_ PUB PSP: R,W,E - Customer Enrollment Certificate (CUST-CERT) PSP: G,W,E - Entropy Input CSP: G,E,Z - DRBG C CSP: G,E,Z - DRBG V CSP: G,E,Z
Alarms, status & Statistics (Show Status)	View and monitor active alarms and module status for diagnostic purposes	Command Response Approved mode indication (command: "system environment show")	Commands	Command response	None	CO (Role-based) CO (Identity-based)
View System Logs (Show Status)	View system status messages, events and provisioning logs locally or via Syslog over TLS	Status Output via SSH, Console or syslog over TLS	Command, SSPs	Command response	TLS SSH KAS-1 KAS-2 KTS-1	CO (Role-based) - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP: G,R,E,Z - TLS Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						key CSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - Password CSP: W,E CO (Identity-based) - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,R,E,Z - TLS Private key CSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - Password CSP: W,E
Manage the Encryption Modem (Perform approved security functions)	Manage the directly connected Encryption Modem using TLS 1.3 Select PSK for DPE peer authentication and provision the modem or Activate certificate peer authentication	Log generation Module Show command Approved mode indication (command: "system environment show")	SSPs, Command	SSPs, Command response	TLS Manage the Encryption Modem (Perform approved security functions) SSH KAS-1 KAS-2 KTS-1 KTS-2	CO (Role-based) - DPE Pre-Shared Keys (PSK) CSP: R - DPE Customer Enrollment Certificate (DPE- CERT) PSP: E - DPE Customer Enrollment CA Certificate

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	and provision the modem Over the TLS 1.3 interface					(DPE- CA) PSP: E - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP: G,R,E,Z - TLS Private key CSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - LDEVID_ PUB PSP: R,W,E - Ciena Device ID private key (iDevID- priv) CSP: E - Ciena Device ID certificate (iDevID) PSP: E - X.509 Key Encryption Key (PKIX-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						KEK) CSP: E - DRBG Seed CSP: G,E,Z - Entropy Input CSP: G,E,Z - DRBG C CSP: G,E,Z - DRBG V CSP: G,E,Z - Customer Enrollment Certificate (CUST-CERT) PSP: G,E CO (Identity-based) - DPE Pre-Shared Keys (PSK) CSP: R - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: E - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP: G,R,E,Z - TLS Private key CSP: G,E,Z - DH Public Key PSP: G,R,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - LDEVID_ PUB PSP: R,W,E - Ciena Device ID private key (iDevID- priv) CSP: E - Ciena Device ID certificate (iDevID) PSP: E - X.509 Key Encryption Key (PKIX-KEK) CSP: E - DRBG Seed CSP: G,E,Z - Entropy Input CSP: G,E,Z - DRBG C CSP: G,E,Z - DRBG V CSP: G,E,Z - DPE Customer Enrollment Certificate (DPE- CERT) PSP: G,E
Perform Secure Transfer (Perform approved security functions)	Transfer configuration file or firmware image to the module	Command Response Approved mode indication (command: "system	SSPs, Command	Command response	SSH KAS-1 KAS-2 KTS-1	CO (Role-based) - SSH Session Authentication Key CSP: G,E,Z - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		environment show")				Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Password CSP: W,E CO (Identity-based) - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Password CSP: W,E
Import/Install Certificate (Perform approved security functions)	Install customer certificates using SSH	Successful completion of service Approved mode indication (command: "system environment show")	SSPs, Command	Command response	Import/Install Certificate SSH KAS-1 KAS-2 KTS-1	CO (Role-based) - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Customer Enrollment Certificate (CUST-CERT) PSP: G,W,E CO (Identity-based) - SSH Session Authentication Key CSP:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Customer Enrollment Certificate (CUST-CERT) PSP: G,W,E
Import PSK (Perform approved security functions)	Import PSK using SSH	Successful Completion of the service Approved mode indication (command: "system environment show")	SSPs, Command	Command response	SSH KAS-1 KAS-2 KTS-1 KTS-2	CO (Role-based) - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - DPE Pre-Shared Keys (PSK) CSP: W CO (Identity-based) - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - DPE Pre-Shared Keys (PSK) CSP: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Activate PSK	Activate a PSK for DPE peer authentication via control / data output interface (SGMII)	Command response Log generation Approved mode indication (command: "system environment show")	SSPs, Command	Command response	Activate PSK KTS-2	CO (Role-based) - Data Encryption Key (DPE-KEK) CSP: E - DPE Pre-Shared Keys (PSK) CSP: R,E CO (Identity-based) - Data Encryption Key (DPE-KEK) CSP: E - DPE Pre-Shared Keys (PSK) CSP: R,E
Zeroize-Secure Erase via RTFD command or pushbutton (Perform zeroization)	Clear all SSP's for which the zeroisation is applicable and disable cryptographic output (Zeroise)	Log generation. Approved mode indication (command: "system environment show")	Command	Command response	None	CO (Role-based) - Ciena Device ID private key (iDevID- priv) CSP: Z - Ciena Device ID certificate (iDevID) PSP: Z - Backup Passphrase (BAK- PW): Z - Security Backup encryption key (BAK-KEY) CSP: Z - Data Encryption Key (DPE-KEK) CSP: Z - COID_P RIV CSP: Z - COID_PUB PSP: Z - LDEVID_

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PUB PSP: Z - DPE Pre-Shared Keys (PSK) CSP: Z - DPE Customer Enrollment Certificate (DPE- CERT) PSP: Z - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: Z - TLS Pre-Master Secret CSP: Z - TLS Master Secret CSP: Z - TLS Authentication Key CSP: Z - TLS Session Key CSP: Z - TLS Public key PSP: Z - TLS Private key CSP: Z - SSH Session Authentication Key CSP: Z - SSH Encryption Key CSP: Z - SSH Server Host Key CSP: Z - SSH User Authentication Public Key PSP: Z - DH Public Key PSP: Z - DH Private Key CSP: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- ECDH Public Key PSP: Z - ECDH Private Key CSP: Z - DRBG Seed CSP: Z - Entropy Input CSP: Z - DRBG C CSP: Z - DRBG V CSP: Z - Customer Enrollment Certificate (CUST-CERT) PSP: Z - Password CSP: Z - X509 Passphrase (X509-PW) CSP: Z CO (Identity-based) - Ciena Device ID private key (iDevID- priv) CSP: Z - Ciena Device ID certificate (iDevID) PSP: Z - Backup Passphrase (BAK- PW): Z - Security Backup encryption key (BAK-KEY) CSP: Z - Data Encryption Key (DPE-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						KEK) CSP: Z - COID_P RIV CSP: Z - COID_PUB PSP: Z - LDEVID_ PUB PSP: Z - DPE Pre-Shared Keys (PSK) CSP: Z - DPE Customer Enrollment Certificate (DPE- CERT) PSP: Z - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: Z - TLS Pre-Master Secret CSP: Z - TLS Master Secret CSP: Z - TLS Authenticatio n Key CSP: Z - TLS Session Key CSP: Z - TLS Public key PSP: Z - TLS Private key CSP: Z - SSH Session Authenticatio n Key CSP: Z - SSH Encryption Key CSP: Z - SSH Server Host Key CSP: Z - SSH User Authenticatio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Public Key PSP: Z - DH Public Key PSP: Z - DH Private Key CSP: Z - ECDH Public Key PSP: Z - ECDH Private Key CSP: Z - DRBG Seed CSP: Z - Entropy Input CSP: Z - DRBG C CSP: Z - DRBG V CSP: Z - Customer Enrollment Certificate (CUST-CERT) PSP: Z - Password CSP: Z - X509 Passphrase (X509-PW) CSP: Z
Secure Backup (Perform approved security functions)	Activate and perform periodic backup of the CSPs or restore CSPs from the secure backup	Log generation Approved mode indication (command: "system environment show")	SSPs, Command	SSPs, Command response	Secure Backup (Perform approved security functions) SSH KAS-1 KAS-2 KTS-1 KTS-2	CO (Role-based) - Backup Passphrase (BAK- PW): W,E,Z - Security Backup encryption key (BAK-KEY) CSP: G,E,Z - SSH Session Authentication Key CSP: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z - SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Password CSP: W,E CO (Identity-based) - Backup Passphrase (BAK- PW): W,E,Z - Security Backup encryption key (BAK-KEY) CSP: G,E,Z - SSH Session Authentication Key CSP: G,E,Z - SSH Encryption Key CSP: G,E,Z - SSH Server Host Key CSP: G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- SSH User Authentication Public Key PSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z - Password CSP: W,E
Issue remote CP reauthentica tion Command (Perform approved security functions)	Send command to remote node to initiate a reauthenticati on with the CO via control output interface (SGMII)	Successfu l completio n of service Approved mode indication (command : "system environme nt show")	SSPs, Comman d	SSPs, Comma nd respons e	TLS KAS-1 KAS-2 KTS-1	CO (Role-based) - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP: G,R,E,Z - TLS Private key CSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Private Key CSP: G,E,Z CO (Identity-based) - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authentication Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - TLS Public key PSP: G,R,E,Z - TLS Private key CSP: G,E,Z - DH Public Key PSP: G,R,E,Z - DH Private Key CSP: G,E,Z - ECDH Public Key PSP: G,R,E,Z - ECDH Private Key CSP: G,E,Z
Perform on demand self-tests (Perform self-tests)	Perform Self-tests on demand via module restart	Successful completion of service Approved mode indication (command: "system environment show")	Power cycle	Self-test indicator	Perform on demand self-tests	CO (Role-based) Unauthenticated CO (Identity-based)
Factory Reset	Factory reset is available	Successful	Reset Signal	Self-test indicator	None	CO (Role-based)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	via a signal which zeroizes all SSPs and returns the module to its initial state	completion of service Approved mode indication (command: "system environment show")				- Backup Passphrase (BAK- PW): Z - Security Backup encryption key (BAK-KEY) CSP: Z - Data Encryption Key (DPE-KEK) CSP: Z - COID_P RIV CSP: Z - COID_PUB PSP: Z - LDEVID_PUB PSP: Z - DPE Pre-Shared Keys (PSK) CSP: Z - DPE Customer Enrollment Certificate (DPE- CERT) PSP: Z - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: Z - TLS Pre-Master Secret CSP: Z - TLS Master Secret CSP: Z - TLS Authentication Key CSP: Z - TLS Session Key CSP: Z - TLS Public key PSP: Z - TLS Private key CSP: Z - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Authentication Key CSP: Z - SSH Encryption Key CSP: Z - SSH Server Host Key CSP: Z - SSH User Authentication Public Key PSP: Z - DH Public Key PSP: Z - DH Private Key CSP: Z - ECDH Public Key PSP: Z - ECDH Private Key CSP: Z - DRBG Seed CSP: Z - Entropy Input CSP: Z - DRBG C CSP: Z - DRBG V CSP: Z - Customer Enrollment Certificate (CUST-CERT) PSP: Z - Password CSP: Z - X509 Passphrase (X509-PW) CSP: Z Unauthenticated - Backup Passphrase (BAK- PW): Z - Security

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Backup encryption key (BAK-KEY) CSP: Z - Data Encryption Key (DPE-KEK) CSP: Z - X.509 Key Encryption Key (PKIX-KEK) CSP: Z - COID_P RIV CSP: Z - COID_PUB PSP: Z - LDEVID_ PUB PSP: Z - DPE Pre-Shared Keys (PSK) CSP: Z - DPE Customer Enrollment Certificate (DPE- CERT) PSP: Z - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: Z - TLS Pre-Master Secret CSP: Z - TLS Master Secret CSP: Z - TLS Authentication Key CSP: Z - TLS Session Key CSP: Z - TLS Public key PSP: Z - TLS Private key CSP: Z - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Session Authentication Key CSP: Z - SSH Encryption Key CSP: Z - SSH Server Host Key CSP: Z - SSH User Authentication Public Key PSP: Z - DH Public Key PSP: Z - DH Private Key CSP: Z - ECDH Public Key PSP: Z - ECDH Private Key CSP: Z - DRBG Seed CSP: Z - Entropy Input CSP: Z - DRBG C CSP: Z - DRBG V CSP: Z - Customer Enrollment Certificate (CUST-CERT) PSP: Z - Password CSP: Z - X509 Passphrase (X509-PW) CSP: Z CO (Identity-based) - Backup Passphrase (BAK- PW): Z - Security

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Backup encryption key (BAK-KEY) CSP: Z - Data Encryption Key (DPE-KEK) CSP: Z - COID_P RIV CSP: Z - COID_PUB PSP: Z - LDEVID_ PUB PSP: Z - DPE Pre-Shared Keys (PSK) CSP: Z - DPE Customer Enrollment Certificate (DPE- CERT) PSP: Z - DPE Customer Enrollment CA Certificate (DPE- CA) PSP: Z - TLS Pre-Master Secret CSP: Z - TLS Master Secret CSP: Z - TLS Authentication Key CSP: Z - TLS Session Key CSP: Z - TLS Public key PSP: Z - TLS Private key CSP: Z - SSH Session Authentication Key CSP: Z - SSH

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Key CSP: Z - SSH Server Host Key CSP: Z - SSH User Authentication Public Key PSP: Z - DH Public Key PSP: Z - DH Private Key CSP: Z - ECDH Public Key PSP: Z - ECDH Private Key CSP: Z - DRBG Seed CSP: Z - Entropy Input CSP: Z - DRBG C CSP: Z - DRBG V CSP: Z - Customer Enrollment Certificate (CUST-CERT) PSP: Z - Password CSP: Z - X509 Passphrase (X509-PW) CSP: Z
External Key Service	Import keys generated external to the module	String "Key Retrieval with Key ID complete"	IP of the external server	Key retrieved from the server	TLS	CO (Identity-based) - TLS Pre-Master Secret CSP: G,E,Z - TLS Master Secret CSP: G,E,Z - TLS Authenticatio

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						n Key CSP: G,E,Z - TLS Session Key CSP: G,E,Z - Ciena Device ID private key (iDevID- priv) CSP: E - Ciena Device ID certificate (iDevID) PSP: E - DRBG Seed CSP: G,E,Z - Entropy Input CSP: G,E,Z - DRBG C CSP: G,E,Z - DRBG V CSP: G,E,Z - Customer Enrollment Certificate (CUST-CERT) PSP: W,E - COID_PUB PSP: W,E - DPE Pre-Shared Keys (PSK) CSP: W,E

Table 13: Approved Services

The services that require operators to assume an authorized role are listed in Table 8 below:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

In Approved mode, the module provides a limited number of services for which the operator is not required to assume an authorized role (see Table 8). None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

4.4 Non-Approved Services

The module does not support any Non-Approved services.

4.5 External Software/Firmware Loaded

For the firmware load test, the module performs an ECDSA P-521 with SHA2-384 signature verification. Please note that the module does not support complete image replacement, and the upgrade is considered a partial replacement since it is not replacing the entire firmware. 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.

4.6 Cryptographic Output Actions and Status

The module supports self-initiated cryptographic output in the context of two services, namely, the Manage the Encryption Modem and Secure Backup services. The module is designed to require the following two internal actions in support of the self-initiated cryptographic output:

For the Manage the Encryption Modem service:
1) Entered the "system encryption enable" command.
2) Activation of the PSK.

For the Secure Backup service:
1) Invocation of the service.
2) Saved the configuration using “Config save” command.

5 Software/Firmware Security

5.1 Integrity Techniques

The module uses ECDSA P-521 using SHA2-384 for integrity testing/verification. The module also runs self-tests for ECDSA Signature verification and SHA2-384 prior to running the integrity check. The Ciena signature public key (256 bits; ECDSA P-521, #A3284) is used for ECDSA validation of all firmware.

5.2 Initiate on Demand

The firmware integrity test is run at startup and on demand by reloading the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module is a hardware module with the embodiment type as a multi-chip embedded module. Hence, the module's operational environment (OE) is a limited OE since the module is designed to accept only controlled firmware changes that successfully pass the firmware load test.

This section is classified as not applicable as the module is a hardware module and the physical security section is claimed for level 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

The chassis of the multi-chip embedded cryptographic module are sealed with 3 tamper-evident seals, applied during manufacturing. The physical security of the module is intact if there is no evidence of tampering with the tamper-evident seal(s).

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 follow internal security policies which include contacting Ciena. The Figure 5 below shows the placement of the tamper seals:

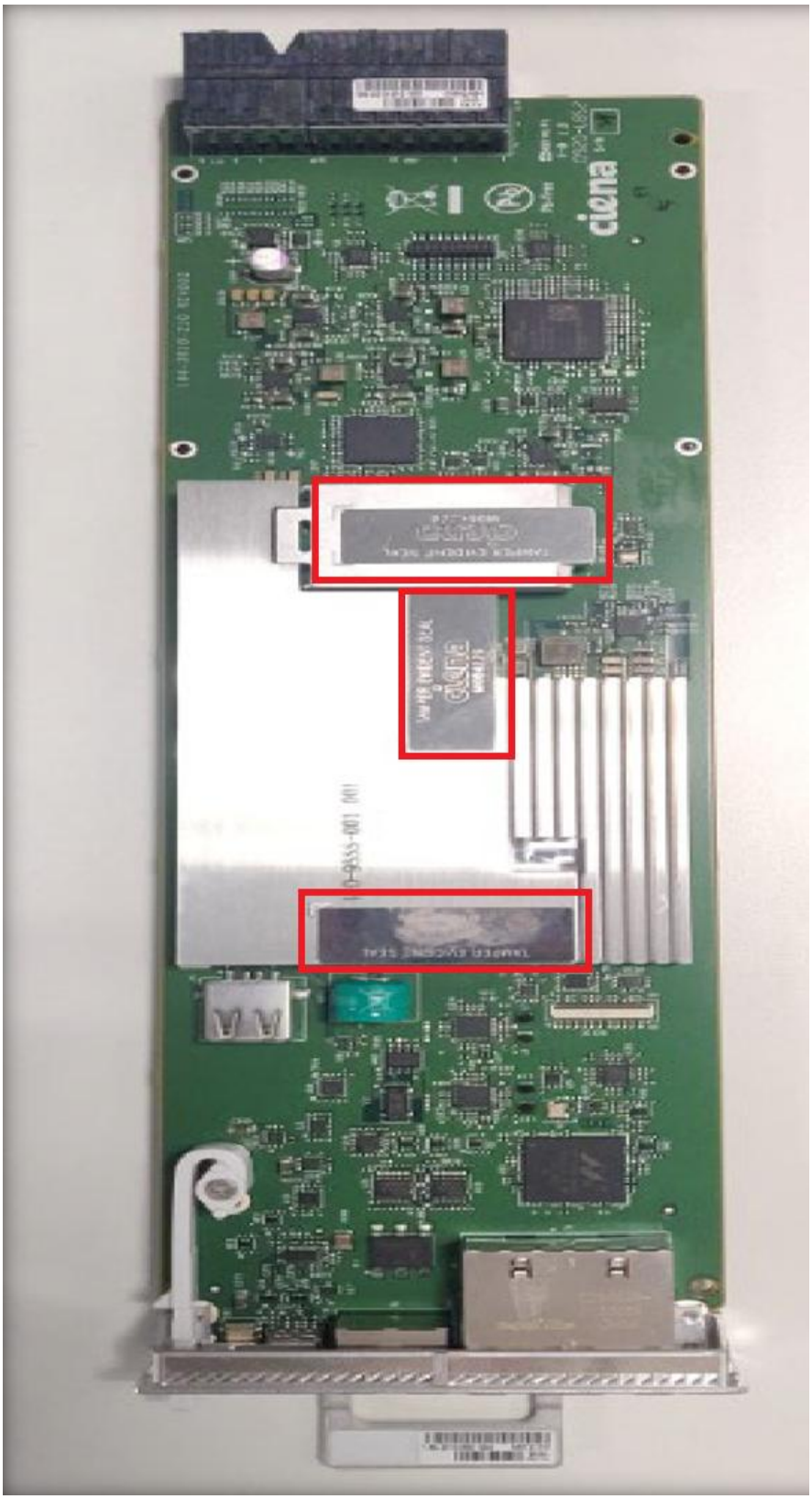


Figure 5: Location of Tamper Seal Placement on the Waveserver 5 Control Processor Module

8 Non-Invasive Security

8.1 Mitigation Techniques

This section is 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	Stored in plaintext in the CPU's nonreadable, write once eFuse	Static
Non-Volatile Memory (NVM) - BKEK	Encrypted using BKEK in Non-Volatile Memory (NVM)	Static
Non-Volatile Memory (NVM) - MKEK	Encrypted using MKEK in Non-Volatile Memory (NVM)	Static
Non-Volatile Memory (NVM) - PKIX-KEK	Encrypted using PKIX-KEK in Non-Volatile Memory (NVM)	Static
Non-Volatile Memory (NVM) - DPE-KEK	Encrypted using DPE-KEK in Non-Volatile Memory (NVM)	Static
Non-Volatile Memory - SHA2-512 Hash	Password stored in a salted hashed (SHA2- 512) form in non-volatile memory (file system)	Static
Non-Volatile Memory (NVM)	Stored in plaintext in the 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
Loaded at the factory (NVM)	Generated externally by the manufacturer	Non-Volatile Memory (NVM)	Plaintext	N/A	N/A	
Loaded at the factory (eFUSE)	Generated externally by the manufacturer	eFUSE	Plaintext	N/A	N/A	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Exits the module in plaintext (NVM)	Non-Volatile Memory (NVM)	External Endpoint	Plaintext	Automated	Electronic	
Input electronically over console	External Endpoint	RAM	Plaintext	Automated	Electronic	
Exits the module in optional security backup, encrypted with BAKKEY	Non-Volatile Memory (NVM)	External Endpoint	Encrypted	Automated	Electronic	KTS-2
Imported in plaintext (NVM)	External Endpoint	Non-Volatile Memory (NVM)	Plaintext	Automated	Electronic	
Exits the module in plaintext (RAM)	RAM	External Endpoint	Plaintext	Automated	Electronic	
Exits the module via TLS 1.3 electronically	RAM	External endpoint	Encrypted	Automated	Electronic	KTS-1
Input encrypted via SFTP/SCP (SSH) electronically	External Endpoint	RAM	Encrypted	Automated	Electronic	KTS-1
Exits the module in optional security backup, encrypted with BAKEY - MKEK	Non-Volatile Memory (NVM) - MKEK	External endpoint	Encrypted	Automated	Electronic	KTS-2
Exits the module in optional security backup, encrypted with BAKKEY - PKIX-KEK	Non-Volatile Memory (NVM) - PKIX-KEK	External endpoint	Encrypted	Automated	Electronic	KTS-2

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Exits the module in optional security backup, encrypted with BAKKEY - DPE-KEK	Non-Volatile Memory (NVM) - DPE-KEK	External endpoint	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	Reboot or Power Cycle	SSPs stored emphemerally in RAM zeroised on reboot/power cycle	Operator Initiated, On Demand
Zeroise after use	Zeroise after use	Zeroise after use	Module Initiated, automatically per the module design
Push Button	Power Cycle of Module	SSPs stored emphemerally in RAM zeroised on power cycle as a result of using this button	Operator Initiated, On Demand
Secure Erase	Erase via RTFD Command	The execution of the command results in SSP zeroisation	Operator Initiated, 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) CSP	Used for decrypting the MKEK and Ciena Device ID	256 bits - 256 bits	Symmetric Key - CSP			AES-GCM (A3283)
Master Key Encryption Key (MKEK) CSP	Used for encrypting or decrypting DEK-KEK and PXIX-KEK	256 bits - 256 bits	Symmetric Key - CSP			AES-GCM (A4855)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Ciena Device ID private key (iDevID-priv) CSP	Used for end point authentication of TLS 1.3 to modem	P-521 - 256 bits	Private Key - CSP			ECDSA SigGen (FIPS186-4) (A4855)
Ciena Device ID certificate (iDevID) PSP	Used for end point authentication of TLS 1.3 to modem	P-521 bits - 256 bits	Public Key Certificate - PSP			ECDSA SigVer (FIPS186-4) (A4855)
Backup Passphrase (BAK- PW)	Used to derive the BAK-KEY	128, 256 bits - 128, 256 bits	String - CSP			SSH
Security Backup encryption key (BAK-KEY) CSP	Used for encrypting optional security backup	256 bits - 256 bits	Symmetric Key - CSP	PBKDF (A4855)		AES-GCM (A4855)
Data Encryption Key (DPE-KEK) CSP	Used for encrypting DPE-PSK, COID_PRIV, BAK-KEY	256 bits - 256 bits	Symmetric Key - CSP	Hash DRBG (A4855)		AES-GCM (A3283)
X.509 Key Encryption Key (PKIX-KEK) CSP	Used to encrypt the X509- PW (Security Manager)	256 bits - 256 bits	Symmetric Key - CSP	Hash DRBG (A4855)		AES-CBC (A4855)
COID_P RIV CSP	Used for end point authentication of TLS 1.3 to modem	P-256 - 256 bits	Private Key - CSP	Hash DRBG (A4855)		ECDSA SigGen (FIPS186-4) (A4855)
COID_PUB PSP	Used for end point authentication of TLS 1.3 to modem	P-256 - 256 bits	Public Key - PSP	Hash DRBG (A4855)		ECDSA SigVer (FIPS186-4) (A4855)
LDEVID_ PUB PSP	Used for end point authentication of TLS 1.3 to modem	P-256 - 256 bits	Public Key - PSP			ECDSA SigVer (FIPS186-4) (A4855)
DPE Pre-Shared Keys (PSK) CSP	Used by the modem, only stored on the CP	256- bit to 2048- bit secret - 256- bit to	String - CSP			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		2048- bit secret				
DPE Customer Enrollment Certificate (DPE-CERT) PSP	Used for remote device peer authentication	P-384, P-521 - 192, 256 bits	Certificate - PSP			ECDSA SigVer (FIPS186-4) (A4855)
DPE Customer Enrollment CA Certificate (DPE- CA) PSP	Used for modem remote device peer authentication	P-384, P-256 - 192, 256 bits	Certificate - PSP			ECDSA SigVer (FIPS186-4) (A4855)
TLS Pre-Master Secret CSP	Establish the TLS Master Secret	384 bit - 384 bit	TLS Pre-Master Secret - CSP		KAS-1 KAS-2	TLS v1.2 KDF RFC7627 (A4855) TLS v1.3 KDF (A4855)
TLS Master Secret CSP	Establish the TLS Session and authentication Key	384-bits - 384-bits	TLS Master Secret - CSP	KAS-1 KAS-2		TLS v1.2 KDF RFC7627 (A4855) TLS v1.3 KDF (A4855)
TLS Authentication Key CSP	Used for authenticating TLS communication	256 or 384 bits - 256 or 384 bits	Keyed Hash Key - CSP	KAS-1 KAS-2		HMAC-SHA2-256 (A4855) HMAC-SHA2-384 (A4855)
TLS Session Key CSP	Used for encrypting TLS communication	128-256 bits - 128-256 bits	Symmetric Key - CSP	KAS-1 KAS-2		AES-GCM (A4855)
TLS Public key PSP	Used during the TLS handshake process	ECDSA P-256, P-384, P-512, RSA	Public Key - PSP	ECDSA KeyGen (FIPS186-4)		ECDSA SigVer (FIPS186-4)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
		2048, 3072, 4096 bits for TLS 1.2 and ECDSA P-521 for TLS 1.3 - ECDSA 128, 192, 256 bits, RSA 112, 128, 152 bits for TLS 1.2 and ECDSA 256 bits for TLS 1.3		(A4855) Hash DRBG (A4855) RSA KeyGen (FIPS186-4) (A4855)		(A4855) RSA SigVer (FIPS186-4) (A4855)
TLS Private key CSP	Used during the TLS handshake process	ECDSA P-256, P-384, P-512, RSA 2048, 3072, 4096 bits for TLS 1.2 and ECDSA P-521 for TLS 1.3 - ECDSA 128, 192, 256 bits, RSA 112, 128, 152 bits for TLS 1.2 and ECDSA 256 bits for TLS 1.3	Private Key - CSP	ECDSA KeyGen (FIPS186-4) (A4855) Hash DRBG (A4855) RSA KeyGen (FIPS186-4) (A4855)		ECDSA SigGen (FIPS186-4) (A4855) RSA SigGen (FIPS186-4) (A4855)
SSH Session Authentication Key CSP	It is used to authenticate all SSH data traffic between the	256 bits - 256 bits	Keyed Hash Key - CSP	KAS-1 KAS-2		HMAC-SHA2-256 (A4855) HMAC-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	SSH Client and SSH Server					SHA2-512 (A4855)
SSH Encryption Key CSP	It is used to encrypt all SSH data traffic between the SSH Client and SSH Server.	128 and 256 bits - 128 and 256 bits	Symmetric Key - CSP	KAS-1 KAS-2		AES-CTR (A4855) AES-GCM (A4855)
SSH Server Host Key CSP	Used to identify the host	RSA 2048, 3072, 4096 bits, ECDSA P256, P384, P-521 - 112 bits, 128 bits, 152 bits for RSA 128, 256 bits for ECDSA	Private Key - CSP	ECDSA KeyGen (FIPS186-4) (A4855) Hash DRBG (A4855) RSA KeyGen (FIPS186-4) (A4855)		ECDSA SigGen (FIPS186-4) (A4855) RSA SigGen (FIPS186-4) (A4855)
SSH User Authentication Public Key PSP	Used for Key-based SSH Authentication	RSA 2048, 3072, 4096; ECDSA P256, P384, P521 P-521 - RSA: 112, 128, 152 bits; ECDSA: 128, 192, 256 bits	Public Key - PSP			ECDSA SigVer (FIPS186-4) (A4855) RSA SigVer (FIPS186-4) (A4855)
DH Public Key PSP	Public key used for establishing TLS /SSH sessions	2048 bits - 112 bits	Public Key - PSP	Hash DRBG (A4855)		KAS-FFC-SSC Sp800-56Ar3 (A4855)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DH Private Key CSP	Private key used for establishing TLS /SSH sessions	2048 bits - 112 bits	Private Key - CSP	Hash DRBG (A4855)		KAS-FFC-SSC Sp800-56Ar3 (A4855)
ECDH Public Key PSP	Public key used for establishin g TLS /SSH sessions	P-256, P-384, P-521 - 128-256 bits	Public Key - PSP	Hash DRBG (A4855)		KAS-ECC-SSC Sp800-56Ar3 (A4855)
ECDH Private Key CSP	Private key used for establishing TLS /SSH sessions	P-256, P-384, P-521 - 128-256 bits	Private Key - CSP	Hash DRBG (A4855)		KAS-ECC-SSC Sp800-56Ar3 (A4855)
DRBG Seed CSP	Used for random number generation; Considered a CSP in accordance with IG D.L Resolution	440 bits - 440 bits	DRBG seed - CSP	Hash DRBG (A4855)		Hash DRBG (A4855)
Entropy Input CSP	Used for seeding the DRBG; Considered a CSP in accordance with IG D.L Resolution	256 bits - 256 bits	Entropy Input - CSP	Hash DRBG (A4855)		Hash DRBG (A4855)
DRBG C CSP	Used for random number generation; Considered a CSP in accordance with IG D.L Resolution 1.	440 bits - 440 bits	DRBG State Value - CSP	Hash DRBG (A4855)		Hash DRBG (A4855)
DRBG V CSP	Used for random number generation;	440 bits - 440 bits	DRBG State Value - CSP	Hash DRBG (A4855)		Hash DRBG (A4855)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Considered a CSP in accordance with IG D.L Resolution 1.					
Customer Enrollment Certificate (CUST-CERT) PSP	Used to establish identity prior to a TLS session (Syslog over TLS)	RSA 2048, 3072, 4096; ECDSA P256, P384, P-521 - 112, 128, 152 bits for ECDSA and 12, 128, 152 bits for RSA	Public Key Certificate - PSP	Hash DRBG (A4855)		ECDSA SigVer (FIPS186-4) (A4855) RSA SigVer (FIPS186-4) (A4855)
Password CSP	Used to authenticate the CO	8-128 ASCII characters, 512 bits - 8-128 ASCII characters, 512 bits	Password (String) - CSP			SHA2-512 (A4855)
Ciena Signature Public key	Used for the firmware load and integrity checks	P-521 - 256 bits	Public Key - Neither			Firmware Upgrade
X509 Passphrase (X509-PW) CSP	Passphrase (X509-PW) Used to protect the private key of the X509 certificate	128-256 bits - 128-256 bits	Passphrase - CSP	Hash DRBG (A4855)		

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Base Key Encryption Key (BKEK) CSP	Loaded at the factory (eFUSE)	eFUSE:Plaintext		Secure Erase	Master Key Encryption Key (MKEK) CSP:Decrypts Ciena Device

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					ID private key (iDevID- priv) CSP:Decrypts
Master Key Encryption Key (MKEK) CSP	Loaded at the factory (NVM)	Non-Volatile Memory (NVM) - BKEK:Encrypted		Secure Erase	X.509 Key Encryption Key (PKIX-KEK) CSP:Encrypts Data Encryption Key (DPE-KEK) CSP:Encrypts X.509 Key Encryption Key (PKIX-KEK) CSP:Decrypts Data Encryption Key (DPE-KEK) CSP:Decrypts
Ciena Device ID private key (iDevID- priv) CSP	Loaded at the factory (NVM)	Non-Volatile Memory (NVM) - BKEK:Encrypted		Secure Erase	Ciena Device ID certificate (iDevID) PSP:Paired With
Ciena Device ID certificate (iDevID) PSP	Loaded at the factory (NVM) Exits the module in plaintext (NVM)	Non-Volatile Memory (NVM) - BKEK:Encrypted		Secure Erase	Ciena Device ID private key (iDevID- priv) CSP:Paired With
Backup Passphrase (BAK- PW)	Input electronically over console Input encrypted via SFTP/SCP (SSH) electronically	RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	
Security Backup encryption key (BAK- KEY) CSP		Non-Volatile Memory (NVM) - DPE-KEK:Encrypted		Push Button Secure Erase	Backup Passphrase (BAK-PW):Encrypts

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Data Encryption Key (DPE-KEK) CSP	Exits the module in optional security backup, encrypted with BAKEY - MKEK	Non-Volatile Memory (NVM) - MKEK:Encrypted		Push Button Secure Erase	DPE Pre-Shared Keys (PSK) CSP:Encrypts COID_P RIV CSP:Encrypts Security Backup encryption key (BAK- KEY) CSP:Encrypts
X.509 Key Encryption Key (PKIX-KEK) CSP	Exits the module in optional security backup, encrypted with BAKEY - MKEK	Non-Volatile Memory (NVM) - MKEK:Encrypted		Push Button Secure Erase	X509 Passphrase (X509-PW) CSP:Encrypts
COID_P RIV CSP	Exits the module in optional security backup, encrypted with BAKKEY - DPE-KEK	Non-Volatile Memory (NVM) - DPE-KEK:Encrypted		Push Button Secure Erase	COID_PUB PSP:Paired With
COID_PUB PSP	Exits the module in optional security backup, encrypted with BAKKEY	Non-Volatile Memory (NVM):Plaintext		Push Button Secure Erase	COID_P RIV CSP:Paired With
LDEVID_ PUB PSP	Exits the module in optional security backup, encrypted with BAKKEY	Non-Volatile Memory (NVM):Plaintext		Push Button Secure Erase	
DPE Pre-Shared Keys (PSK) CSP	Exits the module in optional security backup, encrypted	Non-Volatile Memory (NVM) - DPE-KEK:Encrypted		Push Button Secure Erase	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	with BAKKEY - DPE-KEK				
DPE Customer Enrollment Certificate (DPE- CERT) PSP	Exits the module in optional security backup, encrypted with BAKKEY Exits the module via TLS 1.3 electronically	Non-Volatile Memory (NVM):Plaintext		Push Button Secure Erase	
DPE Customer Enrollment CA Certificate (DPE- CA) PSP	Exits the module in optional security backup, encrypted with BAKKEY Exits the module via TLS 1.3 electronically Input encrypted via SFTP/SCP (SSH) electronically	Non-Volatile Memory (NVM):Plaintext		Push Button Secure Erase	
TLS Pre-Master Secret CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	TLS Master Secret CSP:Used to derive
TLS Master Secret CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	TLS Pre-Master Secret CSP:Derived From TLS Authentication Key CSP:Used to derive TLS Session Key

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					CSP:Used to derive
TLS Authentication Key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	TLS Master Secret CSP:Derived From
TLS Session Key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	TLS Master Secret CSP:Derived From
TLS Public key PSP	Exits the module in plaintext (RAM)	RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	TLS Private key CSP:Paired With
TLS Private key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	TLS Public key PSP:Paired With
SSH Session Authentication Key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	
SSH Encryption Key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	
SSH Server Host Key CSP		Non-Volatile Memory (NVM):Plaintext		Push Button Secure Erase	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SSH User Authentication Public Key PSP	Imported in plaintext (NVM)	Non-Volatile Memory (NVM):Plaintext		Push Button Secure Erase	
DH Public Key PSP	Exits the module in plaintext (RAM)	RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	DH Private Key CSP:Paired With
DH Private Key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	DH Public Key PSP:Paired With
ECDH Public Key PSP	Exits the module in plaintext (RAM)	RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	ECDH Private Key CSP:Paired With
ECDH Private Key CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	ECDH Public Key PSP:Paired With
DRBG Seed CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	Entropy Input CSP:Derived From
Entropy Input CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	DRBG Seed CSP:Used to derive

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG C CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	DRBG V CSP:Used With
DRBG V CSP		RAM:Plaintext	Until reboot or power cycle	Reboot or Power Cycle Push Button Secure Erase	DRBG C CSP:Used With
Customer Enrollment Certificate (CUST-CERT) PSP		Non-Volatile Memory (NVM) - PKIX-KEK:Encrypted		Push Button Secure Erase	
Password CSP	Imported in plaintext (NVM)	Non-Volatile Memory - SHA2-512 Hash:Obfuscated		Push Button Secure Erase	
Ciena Signature Public key	Loaded at the factory (NVM)	Non-Volatile Memory (NVM):Plaintext		N/A	
X509 Passphrase (X509-PW) CSP	Exits the module in optional security backup, encrypted with BAKKEY - PKIX-KEK	Non-Volatile Memory (NVM) - PKIX-KEK:Encrypted		Push Button Secure Erase	

Table 19: SSP Table 2

The module supports AD/EE per FIPS 140-3 IG 9.5.A

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A4855)	Verify	KAT	SW/FW Integrity	Global Approved mode indicator (show status indicator)	ECDSA P-521 with SHA2-512 signature verification

Table 20: Pre-Operational Self-Tests

ISO/IEC 19790 requires the module to perform pre-operational self-tests to ensure the module integrity and the correctness of the cryptographic functionality at start-up. The algorithms supported by the module require cryptographic self-tests and these tests are run when the module is in operational state prior to the first use of algorithm. Some functions also require conditional tests during normal operation of the module.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A4855) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Automatically on boot, manually on demand
AES-CBC (A4855) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Automatically on boot, manually on demand
AES-GCM (A4855) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Automatically on boot, manually on demand
AES-GCM (A4855) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status	256-bit KAT	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				indicator)		
TDES-CBC (A4855)	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	168-bit KAT	Automatically on boot, manually on demand
SHA2-384 (A4855)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	384-bit KAT	Automatically on boot, manually on demand
SHA2-512 (A4855)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	512-bit KAT	Automatically on boot, manually on demand
HMAC-SHA2-256 (A4855)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-256 KAT	Automatically on boot, manually on demand
HMAC-SHA2-384 (A4855)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-384 KAT	Automatically on boot, manually on demand
HMAC-SHA2-512 (A4855)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show	SHA2-512 KAT	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				status indicator)		
KAS-ECC-SSC Sp800-56Ar3 (A4855)	o SP800-56Arev3 KAS-ECC-SSC	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-256	Automatically on boot, manually on demand
ECDSA SigVer (FIPS186-4) (A4855) - P-521 - SHA2-512	ECDSA P-521 Verify KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-521	Automatically on boot, manually on demand
KDF SP800-108 (A4855)	KDF NIST SP 800-108	KAT	CAST	Global Approved mode indicator (show status indicator)	HMAC SHA2-256	Automatically on boot, manually on demand
KAS-FFC-SSC Sp800-56Ar3 (A4855)	Sp800-56Ar3 KAS-FFC-SSC	KAT	CAST	Global Approved mode indicator (show status indicator)	Modulus used: 2048-bit	Automatically on boot, manually on demand
SHA-1 (A4855)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	160-bit KAT	Automatically on boot, manually on demand
SHA2-256 (A4855)	Hash	KAT	CAST	Global Approved mode indicator	256-bit KAT	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				(show status indicator)		
HMAC-SHA-1 (A4855)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA-1 KAT	Automatically on boot, manually on demand
ECDSA SigVer (FIPS186-4) (A4855) - P-256 - SHA2-256	ECDSA P-256 Verify KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	hash: SHA2-256	Automatically on boot, manually on demand
ECDSA SigVer (FIPS186-4) (A4855) - P-256 - SHA2-384	ECDSA P-256 Verify KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	hash: SHA2-384	Automatically on boot, manually on demand
ECDSA SigGen (FIPS186-4) (A4855)	ECDSA P-256 Sign KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	hash: SHA2-256	Automatically on boot, manually on demand
TLS v1.3 KDF (A4855)	KDF TLS 1.3	KAT	CAST	Global Approved mode indicator (show status indicator)	hash: SHA2-256	Automatically on boot, manually on demand
KDF SSH (A4855)	SP800-135rev1	KAT	CAST	Global Approved mode	-	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	KDF SSH KAT			indicator (show status indicator)		
PBKDF (A4855)	SP800-132 PBKDF KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	HMAC SHA2-256	Automatically on boot, manually on demand
TLS v1.2 KDF RFC7627 (A4855)	SP800-135rev1 TLS 1.2 KDF KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	-	Automatically on boot, manually on demand
AES-GCM (A3283)	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Automatically on boot, manually on demand
RSA SigGen (FIPS186-4) (A4855)	RSA 2048 bits Sign KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	2048 bits with SHA2-256 using PKCS1 v1.5	Automatically on boot, manually on demand
RSA SigVer (FIPS186-4) (A4855)	RSA 2048 bits Verify KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	2048 bits with SHA2-256 using PKCS1 v1.5	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Hash DRBG (A4855)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-256 KAT	Automatically on boot, manually on demand
Conditional pairwise-consistency test	P-256, 2048 bits	128 bits, 112 bits	PCT	Global Approved mode indicator (show status indicator)		Automatically on generation of a keypair for use in ECDSA/RSA signature generation/verification or ECC/FFC key agreement
Conditional firmware load test	Firmware loaded using ECDSA P-521 with SHA2-384	256 bits	SW/FW Load	Global Approved mode indicator (show status indicator)	ECDSA P-521 with SHA2-384	Automatically on boot, manually on demand
NIST SP 800-90B Entropy Source Transition Count Health Test (Developer Defined Health Test)	Assesses the health of the noise source using blocks of 128 RAW bits.	-	CAST	Global Approved mode indicator (show status indicator)	Transition Count Health Test on noise source: This test covers both RCT and APT test implementations. The test is implemented per the details of SP800-90B section 4.5 developer defined health tests.	Automatically on boot and continuously, manually on demand

Table 21: Conditional Self-Tests

The CASTs for the cryptographic algorithms used to perform the Approved integrity technique, ECDSA P521 SHA2-384 KATs, occur before the integrity test. The respective Conditional cryptographic algorithm self-tests (CAST) are run prior to the first use of each algorithm for the cryptographic operations. Preoperational self-tests can be performed on demand by reloading

the module. Conditional self-tests can be performed by invoking the corresponding cryptographic functionality of the module.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A4855)	KAT	SW/FW Integrity	On every boot and on demand (Power-cycling)	Programmatically and Manually (on demand)

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A4855) - Encrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-CBC (A4855) - Decrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-GCM (A4855) - Encrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-GCM (A4855) - Decrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
TDES-CBC (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA2-384 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA2-512 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA2-256 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA2-384 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA2-512 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
KAS-ECC-SSC Sp800-56Ar3 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
ECDSA SigVer (FIPS186-4) (A4855) - P-521 - SHA2-512	KAT	CAST	On demand	Manually via reboot/power-cycle
KDF SP800-108 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
KAS-FFC-SSC Sp800-56Ar3 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA-1 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA2-256 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA-1 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A4855) - P-256 - SHA2-256	KAT	CAST	On demand	Manually via reboot/power-cycle
ECDSA SigVer (FIPS186-4) (A4855) - P-256 - SHA2-384	KAT	CAST	On demand	Manually via reboot/power-cycle
ECDSA SigGen (FIPS186-4) (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
TLS v1.3 KDF (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
KDF SSH (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
PBKDF (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
TLS v1.2 KDF RFC7627 (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-GCM (A3283)	KAT	CAST	On demand	Manually via reboot/power-cycle
RSA SigGen (FIPS186-4) (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
RSA SigVer (FIPS186-4) (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
Hash DRBG (A4855)	KAT	CAST	On demand	Manually via reboot/power-cycle
Conditional pairwise-consistency test	128 bits, 112 bits	PCT	On demand	Manually via reboot/power-cycle
Conditional firmware load test	256 bits	SW/FW Load	On demand	Manually via reboot/power-cycle
NIST SP 800-90B Entropy Source Transition Count Health Test (Developer Defined Health Test)	-	CAST	On demand	Manually via reboot/power-cycle

Table 23: 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	Failure of Firmware load test or conditional self-tests	Re-executing the test	Global Approved mode indicator (show status indicator)

Name	Description	Conditions	Recovery Method	Indicator
	is cleared, and the module resumes its services using the previously loaded firmware. If the module encounters an error in any other conditional self-tests (Pairwise Consistency tests, noise source error, etc.) the module will enter a soft error state where the requested command fails. The error condition may be cleared by re-executing the service which prompted the conditional self-test. If the error condition is not cleared, then the module is considered to be malfunctioning and should be returned to Ciena.			
Hard Error	Upon the failure of any pre-operational self-test and the cryptographic algorithm self-tests, the module goes into "Hard Error" state and disables all access to cryptographic functions and SSPs. A permanent error status will be relayed via the status output interface.	Failure of pre-operational self-tests or Cryptographic Algorithm Self-tests	Re-executing the test	The module returns the error indicator/message "Error Validating image" for a failure in the firmware integrity test and "FIPS Self-Test Suite: self-test failure for <algorithm> (forced)" in case of failures triggered in the CASTs.

Table 24: Error States

Upon the failure of any pre-operational self-test and the cryptographic algorithm self-tests, the module goes into “Hard Error” state and disables all access to cryptographic functions and SSPs. A permanent error status will be relayed via the status output interface. The module returns the error indicator/message "Error Validating image" for a failure in the firmware integrity test and "FIPS Self-Test Suite: self-test failure for (forced)" in case of failures triggered in the CASTs.

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.

If the module encounters an error in Pairwise Consistency tests, the module re-generates the key pair and performs the test again until it is passed.

If the error condition is not cleared, then the module is considered to be malfunctioning and should be returned to Ciena.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The following steps must be followed by the CO to place the module in Approved mode of operation. Please note that the module does not support a non-approved mode of operation. The module is shipped to the customers in default state and the following steps must be used by the CO to place the module in Approved mode of operation.

1) As soon as the module is powered up, the module runs the pre-operational self-tests and conditional cryptographic algorithm self-tests. After successful completion of these tests, the module allows the operator to enter the default credentials. The CO can then enter "user set user su password *********" to change the default credentials.
2) Once the default credentials are entered, the operator must configure the IP address and gateway for the module.
3) The operator must enter the following command to disable the shell access to the operator.
   <system environment diag disable diag-shell>

4) The operator must enter the following command to disable the RADIUS and TACACS services to the operator.
   <system encryption remote-authentication radius disable>
   <system encryption remote-authentication tacacs disable>
5) The operator can verify the status by entering the following commands:
system environment show: This command shows if the root/shell access is disabled
system encryption show: This command shows if RADIUS and TACACS is disabled

If both the above commands display that root/shell access, RADIUS and TACACS are disabled, that confirms the operator/tester that the module is in Approved mode of operation.

The CO can monitor and configure the module via the console port or SSH. The CO is responsible for configuring, maintaining, and monitoring the status of the module to ensure that the module is in Approved mode of operation.

11.2 Administrator Guidance

No additional guidance applies.

11.3 Non-Administrator Guidance

No additional guidance applies.

11.5 Maintenance Requirements

No additional maintenance requirements apply for the module. For additional details regarding the management of the module, please refer to Ciena's User's Guide and Technical Practices document.

11.6 End of Life

The end of life for the module meets the ISO/IEC 19790 requirements. The sanitization requirements are met by zeroizing the module using Secure Erase via RTFD command or pushbutton.

11.7 Additional Information

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, C++ and Python.

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.

12 Mitigation of Other Attacks

12.1 Attack List

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