FIPS 140-3 Non-Proprietary Security Policy

Waveserver 5 Control Processor Module

By

Ciena Corporation

Hardware Version(s): 186-3011-900 revision 001 and revision 002,

186-3011-901 revision 001 and revision 002

Firmware Version: 2.3.12

Date: 11/28/2024

Prepared by:
Acumen Security
2400 Research Blvd, Suite 395
Rockville, MD 20850
www.acumensecurity.net

Table of Contents

List of Tables

List of Figures

1. General

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 2.3.12). 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.

Overview

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 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 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.

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.

The following table lists the level of validation for each area in FIPS 140-3:

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 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

Table 1 – Security Levels

The module meets the overall Security Level 2 requirements.

2. Cryptographic Module Specification

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 Waveserver 5 Control Processor Module (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. 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. The Ciena Waveserver 5 Chassis forms the Trusted Operational Environment's Physical Perimeter (TOEPP) for the module.

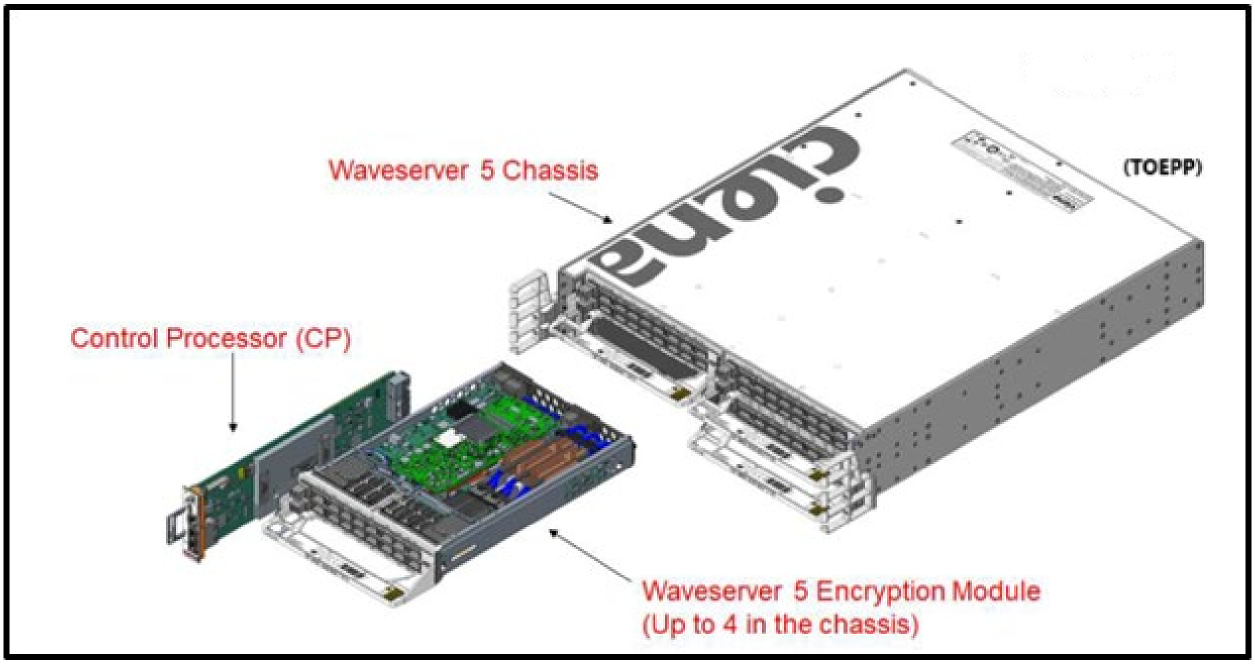


Figure 1 – Ciena Waveserver 5 Chassis

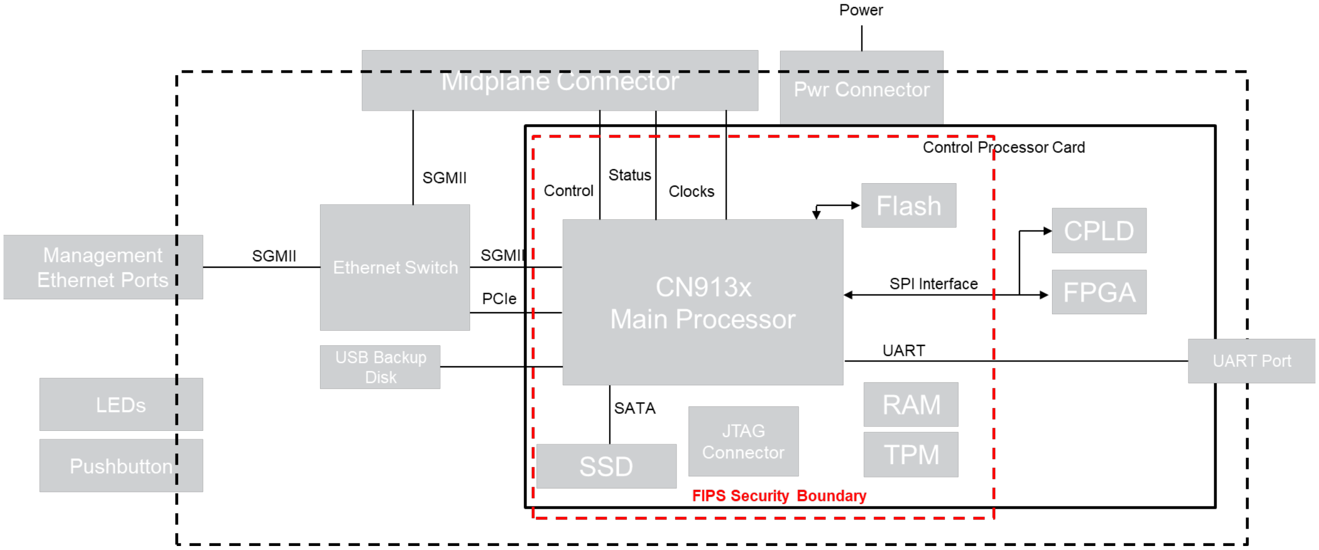


Figure 2 – Waveserver 5 Control Processor Module

Figure 3 below shows the cryptographic boundary of the module (highlighted in red).

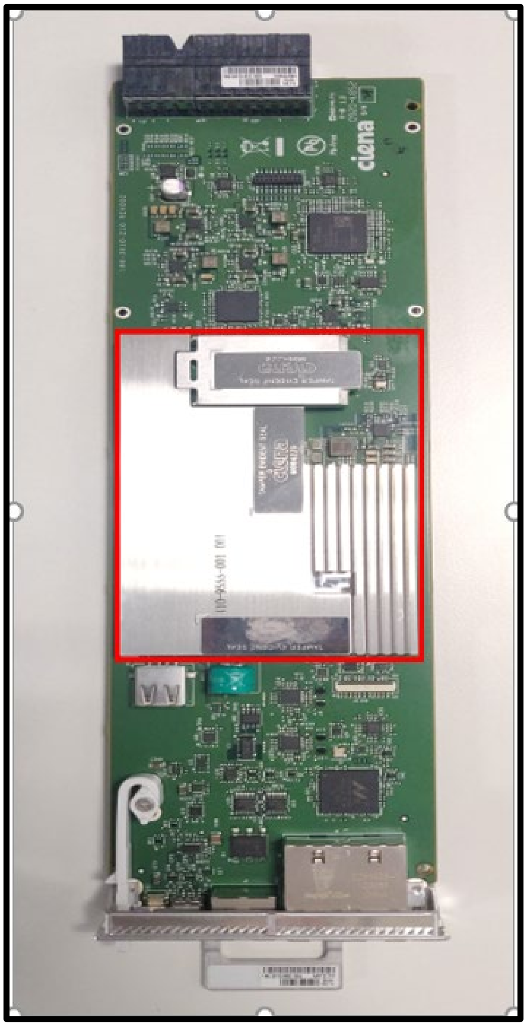


Figure 3 – Waveserver 5 Control Processor Module Cryptographic Boundary

The cryptographic module tested configuration can be found in the table below:

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
CP Type 2	186-3011-900 revision 001 and revision 002, 186-3011-901 revision 001 and revision 002	2.3.12	1) Marvell CN9130 SoC 2) Infineon SLB 9672 SRNG TPM module 3) DDR/RAM memory 4) Flash 5) SSD 6) CPLD 7) FPGA 8) UART/Console port 9) Ethernet ports 10) USB-C port 11) Status LEDs

Table 2 – Cryptographic Module Tested Configuration

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.

The module implements the following Approved algorithms in Table 3:

CAVP Cert[1]	Algorithm and Standard		Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
A3284	AES	FIPS PUB 197 NIST SP800-38A	CBC ECB CTR	128, 192, 256 bits 128, 192, 256 bits	Encryption/ Decryption
		FIPS PUB 197 NIST SP800-38D	GCM	128, 192, 256 bits	Authenticated Encryption/ Decryption
	ECDSA	FIPS 186-4	Key Generation Key Verification Signature Generation Signature Verification	Key Generation (P-256/384/521) Key Verification (P-256/384/521)	Key Gen/ Key Ver Sign/Verify

[1] There are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an approved service of the module.

CAVP Cert[1]	Algorithm and Standard		Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
				Signature Generation (P-256/384/521) Signature Verification (P-256/384/521)	
	DRBG	NIST SP 800-90Arev1	Hash	256 bits	Random Bit Generation
	HMAC	FIPS PUB 198-1	SHA-1 SHA2-256 SHA2-384 SHA2-512	160, 256, 384, 512 bits	Keyed-Hash Message Authentication
	KAS-ECC-SSC	NIST SP 800-56Arev3	Domain Parameter Generation Methods: P-256, P-384, P-521 Scheme: ephemeralUnified	P-256, P-384, P-521	Key Agreement
	KAS-FFC-SSC	NIST SP 800-56Arev3	Domain Parameter Generation Methods: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048 Scheme: dhEphem	2048, 3072, 4096, 6144, 8192 bits	Key Agreement
	KDF SP 800-108	NIST SP 800-108	Feedback, HMAC-SHA2-256	256 bits	Key Derivation
	KDF SSH (CVL)	NIST SP 800-135rev1	Cipher: AES-128, AES-192, AES-256	128, 192, 256 bits	Key Derivation

Public Material – May be reproduced only in its original entirety (without revision).

CAVP Cert[1]	Algorithm and Standard		Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
			Hash Algorithm: SHA-1, SHA2-256, SHA2-384, SHA2-512		
	PBKDF	NIST SP 800-132	Option 1 a HMAC-SHA2-256	Password Length: 14-128 Salt Length: 128-512 Key Data Length: 128	Key Derivation
	RSA	FIPS PUB 186-4	Key Generation (Mode: B.3.3), Signature Generation (Signature Type: PKCS 1.5), Signature Verification (Signature Type: PKCS 1.5)	186-4: 2048/3072 bits, 186-4: PKCS1 v1.5 – 2048/3072 bits, PKCS1 v1.5 – 2048/3072 bits	Key Gen/ Sign/Verify
	SafePrimes Key Gen and Key Ver	NIST SP800-56Arev3	ffdhe2048 ffdhe3072 ffdhe4096 ffdhe6144 ffdhe8192 MODP-2048	2048, 3072, 4096, 6144, 8192 bits	Key Agreement
	SHS	FIPS PUB 180-4 (SHA-1 and SHA2functions)	SHA-1 SHA2-224 SHA2-256 SHA2-384 SHA2-512	160, 224, 256, 384, 512 bits	Hashing
	TDES (Legacy)	NIST SP800-67	CBC	192 bits	Decryption
	TLS 1.2 KDF (CVL)	RFC7627	SHA2-256, SHA2-384, SHA2-512	256, 384, 512 bits	Key Derivation

CAVP Cert[1]	Algorithm and Standard		Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
	TLS 1.3 KDF (CVL)	RFC8446	HMAC-SHA2-256 and HMAC-SHA2-384 Running Mode: DHE and PSK-DHE	256, 384 bits	Key Derivation
KAS-1 KAS-ECC-SSC Sp800-56Ar3/A3284 KDF SSH/A3284 TLS v1.2 KDF RFC7627/A3284 TLS v1.3 KDF/A3284	KAS	NIST SP 800-56Arev3	KAS-ECC-SSC per IG D.F Scenario 2 path (2)	P-256, P-384 and P-521curves providing 128 bits, 192 bits and 256 bits of encryption strength	Key Agreement (SSH and TLS)
KAS-2 KAS-FFC-SSC Sp800-56Ar3/A3284 KDF SSH/A3284 TLS v1.2 KDF RFC7627/A3284 TLS v1.3 KDF/A3284	KAS	NIST SP 800-56Arev3	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	Key Agreement (SSH and TLS)
KTS AES-CBC/A3284 AES-CTR/A3284 HMAC-SHA-1/A3284 HMAC-SHA2-256/A3284 HMAC-SHA2-384/A3284 HMAC-SHA2-512/A3284	KTS	SP 800-38D and SP 800-38F	key wrapping per IG D.G	128, 192, and 256- bit keys providing 128, 192, or 256 bits of encryption strength	Key Transport (SSH and TLS)

CAVP Cert[1]	Algorithm and Standard		Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
A3283	AES	FIPS PUB 197 NIST SP800-38A	CTR ECB	256 bits	Decryption
		FIPS PUB 197 NIST SP800-38D	GCM	256 bits	Decryption
Vendor Affirmed	CKG	SP800-133rev2	Section 4 Using the Output of a Random Bit Generator Option 1 (Symmetric keys and seed values for Asymmetric keys) Section 5.1 Key Pairs for Digital Signature Schemes Section 5.2 Key Pairs for Key Establishment Section 6.1 Direct Generation of Symmetric Keys 6.2.1 Symmetric Keys Generated Using Key-Agreement Schemes Section 6.2.3 Symmetric Keys Derived from Passwords	Section 4 Using the Output of a Random Bit Generator Option 1 (Symmetric keys and seed values for Asymmetric keys) Section 5.1 Key Pairs for Digital Signature Schemes Section 5.2 Key Pairs for Key Establishment Section 6.1 Direct Generation of Symmetric Keys 6.2.1 Symmetric Keys Generated Using Key-	Cryptographic Key Generation

CAVP Cert[1]	Algorithm and Standard		Mode/Method	Description / Key Size(s) / Key Strength(s)	Use/Function
				Agreement Schemes Section 6.2.3 Symmetric Keys Derived from Passwords	

Table 3 – Approved Algorithms

The module does not implement any non-Approved algorithms that are allowed for use within an Approved mode of operation.

The following table lists the Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed.

Algorithm	Caveat	Use/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 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Overall security design and the rules of operation

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

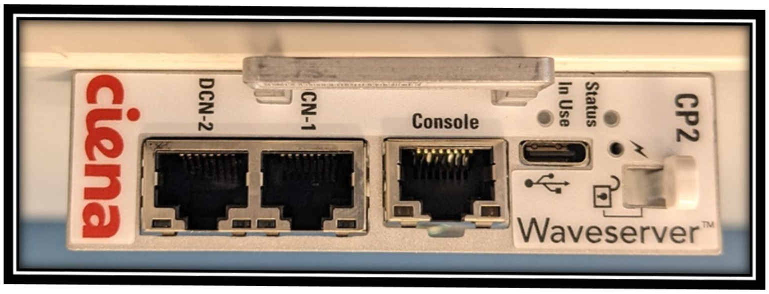
- The module's AES-GCM implementation also conforms to IG C.H Scenario #5 following RFC 8446 for TLS v1.3 and provides support for GCM cipher suites from Section 8.4 of RFC 8446. The IV is generated internally using the module's Approved DRBG and will only be used in the context of the AES-GCM encryption 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 3072 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.

The initialization requirements for the module can be found in Section 11 Life-cycle Assurance in this document.

3. Cryptographic Module 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



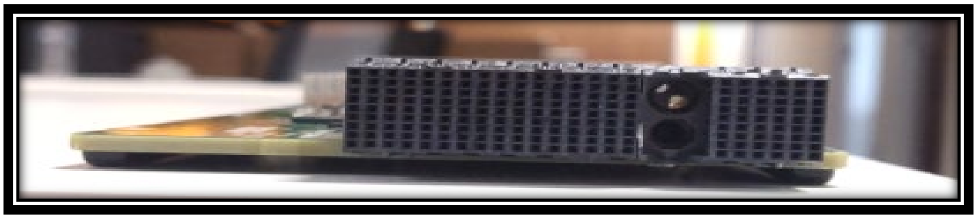


Figure 4 – Waveserver 5 Control Processor Module (Front and Rear)

Table 5 below provides a mapping of the physical interfaces of the module to the logical interfaces:

Physical port	Logical interface	Data that passes over port/interface
Console Interface (Console and USB-C connectors on front panel)	Control Input Interface, Status Output Interface	Console management
Ethernet (SGMII, DCN-1, DCN-2, Backplane Connector & PCIe)	Data Input Interface, Data Output Interface, Control Input Interface, Control Output Interface and Status Output Interface	SSHv2, TLS 1.2 and TLS 1.3 communications
Internal USB on the backplane connector	Data Output Interface, Data Input Interface	Secure Backup Operation
Reset button	Control Input Interface	Reset signal
Status LEDs	Status Output Interface	LED active/on

Power Supply/Input	Power Interface	Power supply/input from within the Waveserver 5 chassis where the module resides

Table 5 – Ports and Interfaces

4. Roles, Services, and Authentication

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 module supports both role-based and identity-based operator authentication methods as specified in Section 5.1. The CO role is able to configure and monitor the module via a console, HTTPS or SSH connection.

Role	Service	Input	Output
CO	Firmware Upgrade (Perform approved security functions)	Command	Command response
CO	View/Display the firmware version of the module (Show module's versioning information)	Command	Command response
CO	Initialize and configure the module (Perform approved security functions)	SSPs, Commands	Command response, SSPs
CO	Alarms, status & Statistics (Show Status)	Command	Command response
CO	View System Logs (Show Status)	Command, SSPs	Command response
CO	Manage the Encryption Modem (Perform approved security functions)	SSPs, Command	SSPs, Command response
CO	Perform Secure Transfer (Perform approved security functions)	SSPs, Command	Command response
CO	Import/Install Certificate (Perform approved security functions)	SSPs, Command	Command response
CO	Import PSK (Perform approved security functions)	SSPs, Command	Command response
CO	Activate PSK	SSPs, Command	Command response
CO	Zeroise - Secure Erase via the Return to Factory Defaults (RTFD) command or pushbutton (Perform zeroisation)	Command	Command response
CO	Secure Backup/ Restore (Perform approved security functions)	SSPs, Command	SSPs, Command response
CO	Issue remote CP reauthentication Command (Perform approved security functions)	SSPs, Command	Command response
CO	Perform on demand self-tests (Perform self-tests)	Power Cycle	Self-test indicator
CO	Factory reset is available via a signal which zeroises all SSPs and returns the module to its initial state	Reset Signal	Self-test indicator

Table 6 – Roles, Service Commands, Input and Output

The module does not support a bypass capability.

Role	Authentication Method	Authentication Strength
CO	Public Key Certificates (TLS/HTTPS) Public key-based authentication (SSH)	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; 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.; Hence, 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.
CO	Initial Device ID (iDevID) and Local Device ID (LDevID) Public Key	This is for the communication 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.

Role	Authentication Method	Authentication Strength
		Hence, at most 10 ×10^9 × 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: (2^256 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
CO	Password-based	For HTTPS, SSH and Console the module enforces 8-character passwords (at minimum) chosen from the 96 human readable ASCII characters; The password can be a maximum of 128 characters. Based on the minimum password length, the probability for a random attempt to succeed is: 1:96^8 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

Table 7– Roles and Authentication

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 = Zeroise: The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Firmware Upgrade (Perform approved security functions)	Perform system wide firmware upgrade	ECDSA #A3284	Ciena signature public key (CPK)	CO	CPK (R, X)	Command response Log generation
View/Display the firmware version of the module (Show module's versioning information)	Report the running firmware version of the module	None	None	CO	None	Command response
Initialize and configure the module (Perform approved security functions)	Perform initialization of the module 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 required operations to enter Approved mode Configure encryption PSK or certificate	ECDSA, AES, DRBG, HMAC, KAS SSC (ECDH Key Pair), CVL, RSA #A3283 and #A3284	CPK, BKEK, MKEK, IDEVID COID, DPE-KEK, PKIX-KEK, DRBG, ESV Cert. #E23 [TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentication Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key]	CO	CPK, BKEK, MKEK, IDEVID (X) COID, DPE-KEK, PKIX-KEK, (G) DRBG, ESV Cert. #E23 (W, X) [TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentication Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key], (R, X, G) [SSH SSPs: SSH Session	Module status show command. Event Log generation Command response Approved mode indication (command: "system environment show" and "system encryption show")

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] Password, DPE-CERT, DPE-CA, CUST-CERT]		Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (R, X, G) Password, DPE-CERT, DPE-CA, CUST-CERT (W)	
Alarms, status & Statistics (Show Status)	View and monitor active alarms and module status for diagnostic purposes	None	None	CO	None	Command Response Approved mode indication (command: "system environment show")
View System Logs (Show Status)	View system status messages, events and provisioning logs locally or via Syslog over TLS	AES, HMAC, ECDSA, KAS SSC (ECDH Key Pair), CVL, RSA.	[TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentica	CO	[TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authenticatio	Status Output via SSH, Console or syslog over TLS

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
		#A3283 and #A3284	tion Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] or [SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] Or Password		n Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (G, R. X) or [SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (G, R, X) Or Password (W, X)	Approved mode indication (command: "system environment show")
Manage the Encryption Modem (Perform approved security functions)	Manage the directly connected Encryption Modem using TLS 1.3	ECDSA, AES, HMAC, KAS SSC (ECDH Key Pair), CVL	PSK DPE-CERT, DPE-CA Or PKIX-KEK	CO	PSK (R) DPE-CERT, DPE-CA (R) Or PKIX-KEK (X)	Log generation Module Show command

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
	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	#A3283 and #A3284	DPE-CERT, DPE-CA [CP TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentication Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] LDEVID		DPE-CERT, DPE-CA (X,R) [CP TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentication Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (X, R) LDEVID (W, X)	Approved mode indication (command: "system environment show")
Perform Secure Transfer (Perform approved security functions)	Transfer configuration file or firmware image to the module	ECDSA, RSA, AES, HMAC, KAS SSC (ECDH Key Pair), CVL #A3283 and #A3284	[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key,	CO	[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (G, R., X)	Command Response Approved mode indication (command: "system environment show")

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			ECDH Private Key] Password		Password (W, X)	
Import/Install Certificate (Perform approved security functions)	Install customer certificates using SSH	ECDSA, RSA, AES, HMAC, KAS SSC (ECDH Key Pair), CVL #A3283 and #A3284	[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] CUSTCERT	CO	[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (G, R, X) CUSTCERT (W)	Successful completion of service Approved mode indication (command: “system environment show”)
Import PSK (Perform approved security functions)	Import PSK using SSH	ECDSA, RSA, AES, HMAC, KAS SSC (ECDH Key Pair), CVL #A3283 and #A3284	[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH	CO	[SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key	Successful Completion of the service Approved mode indication (command: “system environment show”)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			Public Key, ECDH Private Key] PSK		] (R. G, X) PSK (W)	
Activate PSK	Activate a PSK for DPE peer authentication via control / data output interface (SGMII)	AES #A3283 and #A3284	DPE-KEK PSK	CO	DPE-KEK (X) PSK (X, R)	Command response Log generation Approved mode indication (command: “system environment show”)
Zeroise – Secure Erase via RTFD command or pushbutton (Perform zeroisation)	Clear all SSP’s for which the zeroisation is applicable and disable cryptographic output	None	ALL SSPs for which the zeroisation is applicable as defined in Section 10 of the SP	CO	ALL SSPs (Z) for which the zeroisation is applicable as defined in Section 10 of the SP	Log generation. Approved mode indication (command: “system environment show”)
Secure Backup (Perform approved security functions)	Activate and perform periodic backup of the CSPs or restore CSPs from the secure backup	ECDSA, RSA, AES, HMAC, KAS SSC (ECDH Key Pair), CVL. #A3283 and #A3284	BAK-PW, BAK-KEY, [SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH	CO	BAK-PW, BAK-KEY (G, W, X), [SSH SSPs: SSH Session Authentication Key, SSH Encryption Key, SSH Server Host Key, SSH User Authentication Public Key, DH Public Key, DH	Log generation Approved mode indication (command: “system environment show”)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
			Public Key, DH Private Key, ECDH Public Key, ECDH Private Key], Password Material part of backup: DPE-KEK, X509-PW, PKIX-KEK, COID_PRIV , LDEVID_PUB, PSK, DPE-CERT, DPE-CA, CUST-CERT		Private Key, ECDH Public Key, ECDH Private Key] (R. G, X), Password (W, X) Material part of backup: DPE-KEK, X509-PW, PKIX-KEK, COID_PRIV, LDEVID_PUB, PSK, DPE-CERT, DPE-CA, CUST-CERT (R or W)	
Issue remote CP reauthentication Command (Perform approved security functions)	Send command to remote node to initiate a reauthentication with the CO via control output interface (SGMII)	ECDSA, AES, HMAC, KAS SSC (ECDH Key Pair), CVL #A3283 and #A3284	[CP TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentication Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key]	CO	[CP TLS SSPs: TLS Pre-Master Secret, TLS Master Secret, TLS Authentication Key, TLS Session Key, TLS Public key, TLS Private key, DH Public Key, DH Private Key, ECDH Public Key, ECDH Private Key] (X)	Successful completion of service Approved mode indication (command: “system environment show”)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Perform on demand self-tests (Perform self-tests)	Perform Self-Tests on demand via module restart	ECDSA P-521 SHA2-512	CPK	CO, Unauthorised	N/A	Successful completion of service Approved mode indication (command: “system environment show”)
Factory Reset	Factory reset is available via a signal which zeroises all SSPs and returns the module to its initial state	N/A	N/A	CO, Unauthorised	All SSPs (Z)	Successful completion of service Approved mode indication (command: “system environment show”)

Table 8 – Approved Services

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. The module does not support any non-approved services.

Self-initiated Cryptographic Output

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.

The tester observed that no other firmware components are executed in the process of activation apart from the firmware/code related to the commands specified above and that related to the services themselves.

Authentication

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.

Public Material – May be reproduced only in its original entirety (without revision).

5. Software/Firmware Security

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

For firmware load test, the module runs ECDSA P-521 with SHA2-384 check. 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.

6. Operational Environment

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

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).

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-evident seals	Periodic inspection of tamper-evident seals when moving/replacing the module	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 9 – Physical Security Inspection Guidelines

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 below figure shows the placement of the tamper seals.

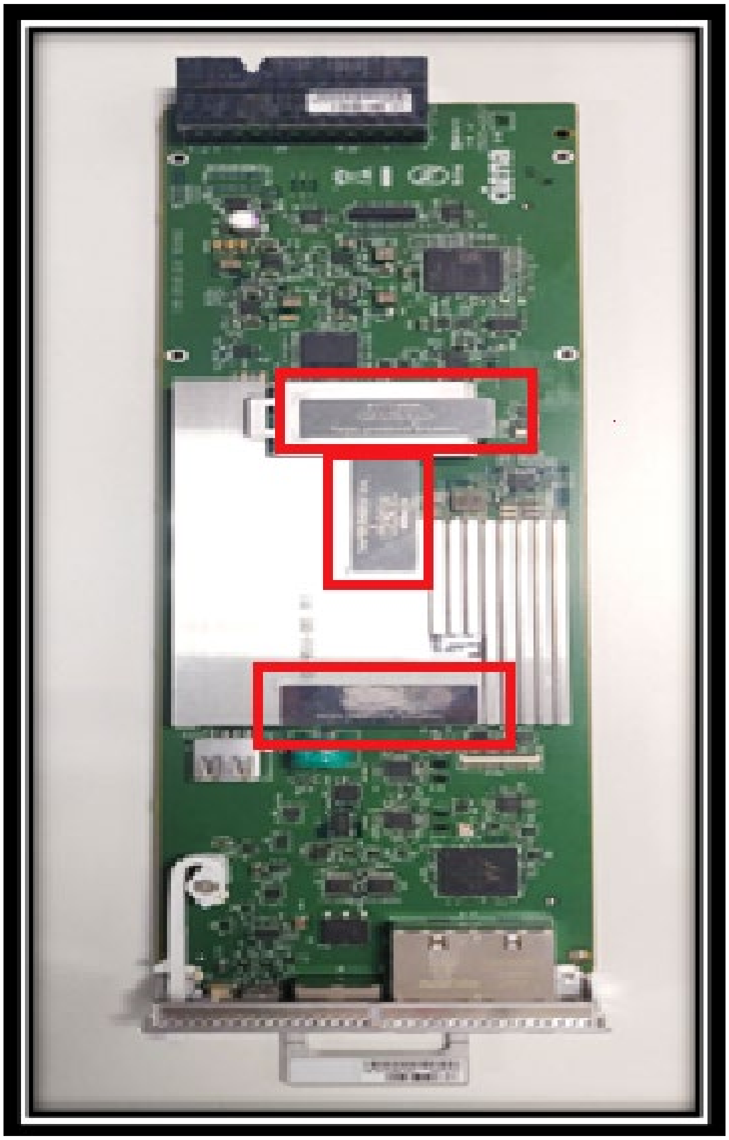


Figure 5 – Location of Tamper Seal Placement on the Waveserver 5 Control Processor Module

8. Non-invasive Security

This section is not applicable. The module does not implement any Non-invasive attack mitigation techniques.

9. Sensitive Security Parameter Management

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

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
Base Key Encryption Key (BKEK) CSP	256 bits	AES GCM, ECB 256 bits #A3283	N/A	Loaded at the factory Does not exit the module	N/A	Stored in plaintext in the CPU's non-readable, write once eFuse	N/A	Used for decrypting the MKEK and Ciena Device ID
Master Key Encryption Key (MKEK) CSP	256 bits	AES GCM 256 bits #A3284, #A3283	N/A	Loaded at the factory Does not exit the module	N/A	Stored encrypted with the BKEK in non-volatile memory (NVM)	N/A	Used for encrypting or decrypting DEK-KEK and PXIX-KEK
Ciena Device ID private key (iDevID-priv) CSP	256 bits	ECDSA P-521 Sig Ver #A3284	N/A	Loaded at the factory Does not exit the module	N/A	Stored encrypted with the BKEK in non-volatile memory (NVM)	N/A	Used for end point authentication of TLS 1.3 to modem
Ciena Device ID certificate (iDevID) PSP	256 bits	ECDSA P-521 Sig Ver #A3284	N/A	Loaded at the factory Exits the module in plaintext	N/A	Stored encrypted with the BKEK in non-volatile memory (NVM)	N/A	Used for end point authentication of TLS 1.3 to modem
Backup Passphrase (BAK-PW)	String	AES-GCM 128, 256 bits, AES -	N/A	Input electronically over console or SSH	N/A	RAM only	Power cycle of the module, Secure	Used to derive the BAK-KEY

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
CSP		CTR, 128, 256 bits, #A3284, #A3284 HMAC-SHA-256 #A3284, KDF SSH		Never exits the module			Erase via RTFD command or pushbutton	
Security Backup encryption key (BAK-KEY) CSP	256 bits	AES GCM, ECB 256 bits #A3284 Hash DRBG #A3284, PBKDF #A3284 CKG	Generated by the module using approved DRBG and PBKDF	Neither input nor output	N/A	Encrypted with DPE-KEK and stored in non-volatile memory (NVM)	Secure Erase via RTFD command or pushbutton	Used for encrypting optional security backup
Data Encryption Key (DPE-KEK) CSP	256 bits	AES-GCM 256 bits #A3284 Hash DRBG #A3284 CKG	Generated by the module at runtime from approved DRBG	No Input Exits the module in optional security backup, encrypted with BAK-KEY	N/A	Encrypted with MKEK and stored in non-volatile memory (NVM)	Secure Erase via RTFD command or pushbutton	Used for encrypting DPE-PSK, COID_PRIV, BAK-KEY
X509 Passphrase (X509-PW) CSP	128-256 bits	Hash DRBG #A3284 Or AES-GCM 128, 256 bits, AES - CTR, 128, 256 bits,	Generated by the module at runtime from approved DRBG Or Imported via SSH	Exits the module in optional security backup, encrypted with BAK-KEY	Key transport (SSH)	Encrypted with PKIX-KEK and stored in non-volatile memory (NVM)	Secure Erase via RTFD command or pushbutton	Passphrase (X509-PW) Used to protect the private key of the X509 certificate

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		#A3284, #A3284 HMAC-SHA-256 #A3284, KDF SSH						
X.509 Key Encryption Key (PKIX-KEK) CSP	256 bits	AES CBC 256-bit key #A3284 Hash DRBG #A3284 CKG	Generated by the Module's DRBG at runtime	No Input Exits the module in optional security backup, encrypted with BAK-KEY	N/A	Encrypted with MKEK and stored in non-volatile memory	Secure Erase via RTFD command or pushbutton	Used to encrypt the X509-PW (Security Manager)
COID_PRIV CSP	256 bits	HMAC-SHA2-384 #A3284, AES 256 bits GCM #A3284, ECDSA P-521 #A3284, Hash DRBG #A3284, CKG	Generated by the module at runtime from approved DRBG	No Input Exits the module in optional security backup, encrypted with BAK-KEY and over TLS 1.3	N/A	Encrypted with DPEKEK, stored in non-volatile memory (NVM)	Secure Erase via RTFD command or pushbutton	Used for end point authentication of TLS 1.3 to modem
COID_PUB PSP	256 bits	HMAC-SHA2-384 #A3284, AES 256 bits GCM #A3284, ECDSA P-521 #A3284,	Generated by the module at runtime from approved DRBG	No Input Exits the module in optional security backup, encrypted	N/A	Plaintext in non-volatile memory (NVM) in PEM format	Secure Erase via RTFD command or pushbutton	Used for end point authentication of TLS 1.3 to modem

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		Hash DRBG #A3284, CKG		with BAK-KEY and over TLS 1.3				
LDEVID_ PUB PSP	256 bits	HMAC-SHA2-384 #A3284, AES 256 bits GCM #A3284, ECDSA P-521 #A3284, CKG	N/A	Enters module electronically using TLS 1.3 North-South connection Exits the module in optional security backup, encrypted with BAK-KEY	N/A	Stored in plaintext in non-volatile memory (NVM) in PEM format	Secure Erase via RTFD command or pushbutton	Used for end point authentication of TLS 1.3 to modem
DPE Pre-Shared Keys (PSK) CSP	String - 256-bit to 2048-bit secret	SSH: AES-GCM 128, 256 bits, AES - CTR, 128, 256 bits, #A3284, #A3284 HMAC-SHA-256 #A3284, KDF SSH TLS 1.3:	N/A	Imported via SSH electronically Exits the module via TLS 1.3 electronically or Exits the module in	N/A	Encrypted with DPE-KEK and stored in non-volatile memory (NVM)	Secure Erase via RTFD command or pushbutton	Used by the modem, only stored on the CP

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		HMAC-SHA2-384 #A3284, AES 256 bits GCM #A3284, ECDSA P-521 #A3284, CKG		optional security backup, encrypted with BAK-KEY				
DPE Customer Enrollment Certificate (DPE-CERT) PSP	192, 256 bits	ECDSA P-384, P-521 #A3284, SSH: AES-GCM 128, 256 bits, AES - CTR, 128, 256 bits, #A3284, #A3284 HMAC-SHA-256 #A3284, KDF SSH TLS 1.3: HMAC-SHA2-384 #A3284, AES 256 bits GCM #A3284,	Input encrypted via SSH Or Generated by the module's approved DRBG at runtime	Exits the module via TLS 1.3 electronically Or Exits the module in optional security backup, encrypted with BAK-KEY	N/A	Stored in plaintext in non-volatile memory	Secure Erase via RTFD command or pushbutton	Used for remote device peer authentication

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		ECDSA P-521 #A3284, CKG Or Hash DRBG #A3284						
DPE Customer Enrollment CA Certificate (DPE-CA) PSP	192 bits, 256 bits	ECDSA P-384, P-512 public Key #A3284 SSH: AES-GCM 128, 256 bits, AES - CTR, 128, 256 bits, #A3284, #A3284 HMAC-SHA-256 #A3284, KDF SSH TLS 1.3: HMAC-SHA2-384 #A3284, AES 256 bits GCM #A3284, ECDSA P-521 #A3284,	N/A	Input encrypted via SFTP/SCP (SSH) electronically Exits the module via TLS 1.3 electronically, In optional security backup, encrypted with BAK-KEY	N/A	Stored in plaintext in non-volatile memory (NVM)	Secure Erase via RTFD command or pushbutton	Used for modem remote device peer authentication

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		CKG						
TLS Pre-Master Secret CSP	384-bit	KDF TLS 1.2 #A3284, KDF TLS 1.3 #A3284, Hash DRBG #A3284	Generated internally by module's DRBG during session negotiation	Never exits the module	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Establish the TLS Master Secret
TLS Master Secret CSP	384-bit	KDF TLS 1.2 #A3284, KDF TLS 1.3 #A3284	N/A	Never exits the module	Derived using TLS Pre-Master Secret during session negotiation	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Establish the TLS Session and authentication Key
TLS Authentication Key CSP	256 or 384 bits	HMAC-SHA2-256, HMAC-SHA2-384 #A3284, KDF TLS 1.2 #A3284 for TLS 1.2 HMAC-SHA2-384	N/A	Neither Input nor Output	Derived via KDF defined in SP800-135rev1 KDF (TLS 1.2) and TLS 1.3 during session negotiation	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used for authenticating TLS communication

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		#A3284, KDF TLS 1.3 #A3284 for TLS 1.3						
TLS Session Key CSP	128-256 bits	AES GCM 128/256-bit keys for TLS 1.2 #A3284 AES CBC 128/256-bit keys for TLS 1.2 #A3284 AES 256-bit GCM for TLS 1.3 #A3284	N/A	Neither Input nor Output	Derived via KDF defined in SP800-135rev1 KDF (TLS 1.2) and KDF TLS 1.3 during session negotiation	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used for encrypting the TLS communication
TLS Public key PSP	TLS Public key PSP	ECDSA P-256, P-384, P-512 #A3284, RSA 2048, 3072, 4096 bits #A3284 for TLS 1.2 ECDSA P-521 #A3284	Generated as per defined in FIPS 186-4 and seed generated by using module's DRBG	No Input exits in plaintext	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used during the TLS handshake process

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establis h-ment	Storage	Zeroisatio n	Use & related keys
		for TLS 1.3 CKG						
TLS Private key CSP	128-256 bits	ECDSA P-256, P-384, P-512 #A3284, RSA 2048, 3072, 4096 bits #A3284 for TLS 1.2 ECDSA P-521 #A3284 for TLS 1.3 CKG	Generated as per defined in FIPS 186-4 and seed generated by using module's DRBG	No Input Never exits the module	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used during the TLS handshake process
SSH Session Authentication Key CSP	256 bits	HMAC-SHA2-256, #A3284 HMAC-SHA2-512 #A3284	N/A	Neither Input nor Output	Derived via key derivation function defined in SP800-135rev1 KDF (SSH)	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	It is used to authenticate all SSH data traffic between the SSH Client and SSH Server
SSH Encryption Key CSP	128 and 256 bits	AES-GCM 128, 256 bits, AES - CTR, 128, 256 bits, #A3284,	N/A	Neither Input nor Output	Derived via key derivation function defined	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD	It is used to encrypt all SSH data traffic between the SSH

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		#A3284 HMAC-SHA-256 #A3284, KDF SSH			in SP800-135rev1 KDF (SSH)		command or pushbutton	Client and SSH Server
SSH Server Host Key CSP	112 bits, 128 bits, 152 bits for RSA 128, 256 bits for ECDSA	RSA 2048, 3072, 4096 bits #A3284 ECDSA P-256, P-384, P-521 #A3284 CKG Hash DRBG #A3284 Or AES-GCM 128, 256 bits, AES-CTR, 128, 256 bits #A3284	Generated as per defined in FIPS 186-4 and seed generated by using module's DRBG Or Imported via SSH	Never exits the module	N/A	Stored in plaintext in NVM	Secure Erase via RTFD command or pushbutton	Used to identify the host
SSH User Authentication	112-256 bits	RSA 2048, 3072, 4096 #A3284	N/A	Imported in Plaintext	N/A	Stored in plaintext in NVM	Secure Erase via RTFD command	Used for key based

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
Public Key PSP		ECDSA P-256, P-384, P-521 P-521 #A3284		Never exits the module			or pushbutton	SSH authentication
DH Public Key PSP	112 bits	2048-bits KAS-FFC-SSC #A3284 Hash DRBG #A3284 CKG	Generated Per SP800-56arev3 and seed is generated by the module's DRBG	Exits the module in plaintext	Established per SP800-56Arev3	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Public key used for establishing TLS /SSH sessions
DH Private Key CSP	112 bits	2048-bits KAS-FFC-SSC #A3284 Hash DRBG #A3284 CKG	Generated Per SP800-56arev3 and seed is generated by the module's DRBG	Never exits the module	Established per SP800-56Arev3	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Private key used for establishing TLS /SSH sessions
ECDH Public Key PSP	128-256 bits	KAS-ECC-SSC, P-256, P-384, P-521 #A3284 Hash DRBG #A3284 CKG	Generated Per SP800-56Arev3 and seed is generated by the module's DRBG	Private Key: Never exits the module Public Key: Exits the module in plaintext	Established per SP800-56Arev3	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Public key used for establishing TLS /SSH sessions

Public Material – May be reproduced only in its original entirety (without revision).

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
ECDH Private Key CSP	128-256 bits	KAS-ECC-SSC, P-256, P-384, P-521 #A3284 Hash DRBG #A3284 CKG	Generated Per SP800-56Arev3 and seed is generated by the module's DRBG	Never exits the module	Established per SP800-56Arev3	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Private key used for establishing TLS /SSH sessions
DRBG Seed CSP	440 bits	ESV Cert. #E23	Generated internally using entropy input	Neither input nor output	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used for random number generation
Entropy Input CSP	256 bits	ESV Cert. #E23	Generated internally using ESV Cert. #E23	Neither input nor output	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used for random number generation
DRBG C CSP	440 bits	Hash DRBG #A3284	Generated internally using the approved NIST SP800-90Ar1 DRBG	N/A	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command	Used for random number generation

Key/SSP Name/ Type	Stren-gth	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
							or pushbutton	
DRBG V CSP	440 bits	Hash DRBG #A3284	Generated internally using the approved NIST SP800-90Ar1 DRBG	N/A	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used for random number generation
DRBG Output CSP	256 bits	Hash DRBG #A3284	Generated internally using the approved NIST SP800-90Ar1 DRBG	N/A	N/A	Stored in plaintext in RAM	Power cycle of the module, Secure Erase via RTFD command or pushbutton	Used for random number generation
Customer Enrollment Certificate (CUST-CERT) PSP	112, 128, 152 bits for RSA 128, 192, 152 bits for ECDSA	RSA 2048, 3072, 4096 #A3284 ECDSA P-256, P-384, P-521 #A3284 AES-GCM 128, 256 bits, AES -	Input encrypted via SSH Or Generated internally using the Approved DRBG	Never exits the module	N/A	Stored encrypted with PKI XKEK in non-volatile memory	Secure Erase via RTFD command or pushbutton	Used to establish identity prior to a TLS session (Syslog over TLS)

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establish-ment	Storage	Zeroisation	Use & related keys
		CTR, 128, 256 bits, #A3284, #A3284 HMAC-SHA-256 #A3284, KDF SSH Or Hash DRBG #A3284						
Password CSP	8-128 ASCII characters, 512 bits	SHA2-512 #A3284	N/A	Input by the operator Does not exit the module	N/A	Stored in a salted hashed (SHA2-512) form in non-volatile memory (file system)	Secure Erase via RTFD command or pushbutton	Used to authenticate the CO

Table 10 – SSPs

The Module contains the following non-SSP:

- Ciena signature public key (CPK); 256 bits; ECDSA P-521 public keys #A3284; Used for ECDSA validation of all FW.

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

SSP Generation and Entropy

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.

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.

Entropy sources	Minimum number of bits of entropy	Details
ESV Cert. #E23 Infineon Trusted Platform Module 2.0 SLB 9672 Entropy Source (Ring Oscillator based noise source)	0.73 bits of entropy per bit	The module supports the use of Infineon Trusted Platform Module 2.0 SLB 9672 Entropy Source as an ESV Cert. #E23 approved entropy source; The noise source is the root of security for the entropy source and for the RNG as a whole; This is the component, which contains the nondeterministic, entropy-providing activity that is ultimately responsible for the uncertainty associated with the bit-strings output by the entropy source; If this component fails, no other mechanism in the RNG can compensate for the lack of entropy The entropy source contains a noise source, which includes a bias compensator, an entropy estimator (online health test), and a post-processing algorithm (conditioning algorithm); The noise source makes use of two resetting ring oscillators, a fast oscillator and a slow oscillator; The fast oscillator is sampled using a frequency divided (pre-scaled) version of the slow oscillator. These oscillators are reinitialized each time a new raw bit is requested, and only run until the requested bit is produced

Table 11 – Non-Deterministic Random Number Generation Specification

10. 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.

1. Pre-operational self-tests:
   a. Pre-operational firmware integrity test: ECDSA P-521 with SHA2-384.

2. Conditional self-tests:
   b. Conditional cryptographic algorithm test:

   Ciena Waveserver Crypto Library 1 Implementation:

   - ECDSA P-521 Signature verification KAT
   - SHA2-384 KAT
   - AES-CBC 256-bit KAT (Encrypt)
   - AES-CBC 256-bit KAT (Decrypt)
   - AES-GCM 256-bit KAT (Encrypt)
   - AES-GCM 256-bit KAT (Decrypt)
   - Triple-DES CBC KAT (Decrypt)
   - SHA-1 KAT
   - SHA2-256 KAT
   - SHA2-384 KAT
   - SHA2-512 KAT
   - HMAC-SHA-1 KAT
   - HMAC-SHA2-256 KAT
   - HMAC-SHA2-384 KAT
   - HMAC-SHA2-512 KAT
   - Hash DRBG (SHA2-256) KAT
     - SP800-90Arev1 Section 11 health tests
   - KAS-ECC-SSC primitive “Z” KAT (Curves used for CAST: P-256)
   - KAS-FFC-SSC primitive “Z” KAT (Modulus used for CAST: 2048-bit)
   - ECDSA P-256 with SHA2-256 Sign KAT
   - ECDSA P-256 with SHA2-256 Verify KAT
   - ECDSA P-521 with SHA2-384 Verify KAT
   - RSA 2048 bits with SHA2-256 using PKCS1 v1.5 Sign KAT
   - RSA 2048 bits with SHA2-256 using PKCS1 v1.5 Verify KAT
   - SP800-132 PBKDF (HMAC SHA2-256) KAT
   - SP800-108 KBKDF (HMAC SHA2-256) KAT
   - SP800-135rev1 TLS 1.2 KDF KAT
   - SP800-135rev1 KDF SSH KAT
   - KDF TLS 1.3 (HMAC SHA2-256) KAT

   Ciena Waveserver Crypto Library 2 Implementation:

- AES-GCM 256-bit KAT (Decrypt)

- 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.

c. Conditional pairwise-consistency test: Whenever an RSA and ECDSA key pair of any valid size is generated on the module (RSA and/or ECDSA key pairs for use in signature generation/verification and ECDSA key pairs for use in SSP agreement), before the operation is completed and the keys are made available for use to the operator, a pair-wise consistency test is executed on the key pair.

d. Conditional firmware load test: When firmware is updated on the module, the update image must be validated before the underlying firmware on the device is updated. This is accomplished through an ECDSA P-521 with SHA2-384 signature validation on the update image.

The CASTs for the cryptographic algorithms used to perform the Approved integrity technique, ECDSA P-521 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. Pre-operational 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.

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 <algorithm> (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.

a. Life-cycle Assurance

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.

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

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 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.

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.

b. Mitigation of Other Attacks

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

End of Document