FIPS 140-3 Non-Proprietary Security Policy

WaveLogic 5 Extreme Encryption Modem

By

Ciena Corporation

[012 (P/Ns 174-0506-841) with components Mech Kit 500-0506-020 Version 001]

[012 (P/Ns 174-0506-842) with components Mech Kit 500-0506-020 Version 001]

[014 (P/N 174-0506-843) with components Mech Kit 500-0506-020 Version 001]

[007 (P/N 174-0506-844) with components Mech Kit 500-0506-020 Version 001]

Firmware Version: 12.3

Date: 11/28/2024

Prepared by:

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

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 WaveLogic 5 Extreme Encryption Modem 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 WaveLogic 5 Extreme Encryption Modem may also be referred to as the “module” or “modem” in this document.

Disclaimer

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

Notices

Table Of Contents

List Of Tables

List Of Figures

1. General

Scope

This document describes the cryptographic module non-proprietary security policy for the WaveLogic 5 Extreme Encryption Modem (Hardware versions: 007, 012 and 014) (Firmware Version 12.3) by Ciena Corporation. 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 WaveLogic 5 Extreme Encryption Modem is an optical transponder daughter card installed within a Ciena optical transponder service module. It consists of a multiple chip-embedded application specific integrated circuit (ASIC) along with optical components and supporting circuitry.

All security-relevant communications to the module via its management interface (Ethernet) are encrypted using TLS v1.3. The module also supports a client input and output data interface and optical connector. All traffic entering and exiting the module via the optical connector is encrypted/decrypted using AES GCM. The module provides fully secure cryptographic functionality, including peer authentication, key derivation, datapath encryption, physical security, and identification and authentication of the module's Crypto Officer (CO). This module is configured and monitored by a Ciena Control Processor Module.

The module operates in Approved mode by default. No additional configuration is needed for rendering or operating the module in the Approved mode.

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	2
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-tests	2
11	Life-cycle Assurance	2
12	Mitigation of Other Attacks	N/A

Table 1 – Security Levels

The module meets the requirements of an overall Security Level 2.

2. Cryptographic Module Specification

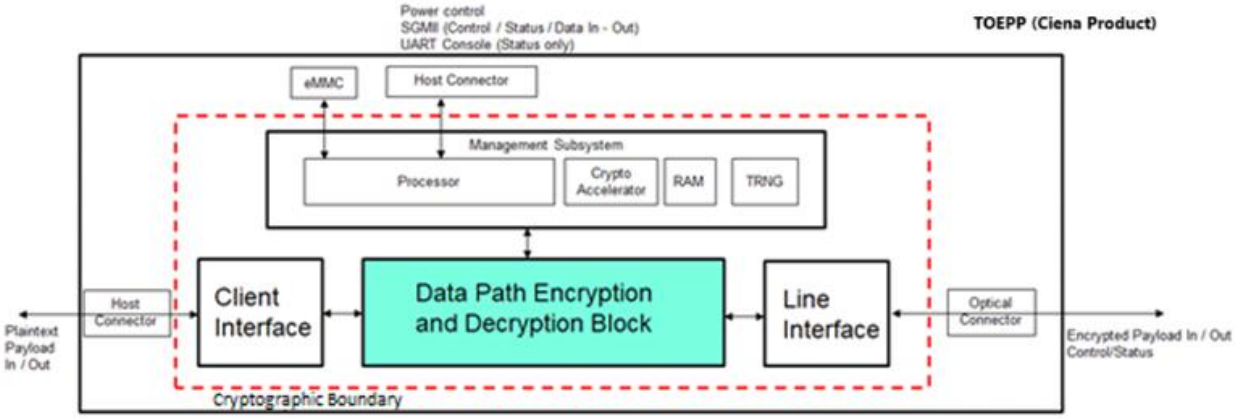

Figure 1: High level module block diagram

As shown in the above block diagram, the module consists of an ARM A53 quad core processor with internal RAM. The firmware running on the processor performs all the monitoring/control activities related to the datapath encryption feature.

The crypto accelerator is a security co-processor. It contains hardware cryptographic engines and firmware for the WaveLogic 5e Encryption Modem Crypto library.

The datapath encryption and decryption block performs the AES-GCM encryption and decryption function on the client payload data.

The module is packaged within other Ciena products to form a complete encryption transport solution. The Ciena product forms the Trusted Operational Environment's Physical Perimeter (TOEPP) for the module.

Figure 2 below shows the cryptographic boundary of the module (highlighted in red).

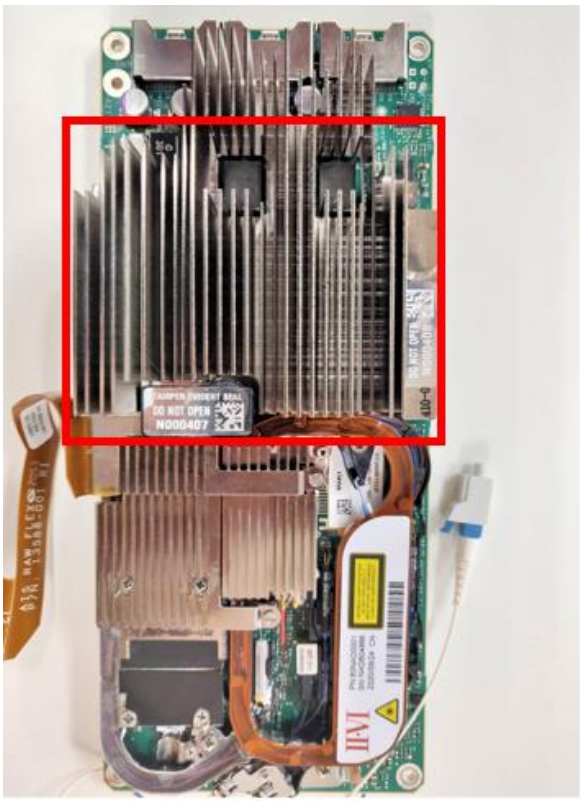

Figure 2: Cryptographic Boundary of WaveLogic 5 Extreme Encryption Modem (represents all P/Ns in Table 2)

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
WaveLogic 5 Extreme Encryption Modem	[012 (P/Ns 174-0506-841) with components Mech Kit 500-0506-020 Version 001]	12.3	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
WaveLogic 5 Extreme Encryption Modem	[012 (P/Ns 174-0506-842) with components Mech Kit 500-0506-020 Version 001]	12.3	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
WaveLogic 5 Extreme Encryption Modem	[014 (P/Ns 174-0506-843) with components Mech Kit 500-0506-020 Version 001]	12.3	The part numbers are equivalent and just used to differentiate the manufacturing process and sites
WaveLogic 5 Extreme Encryption Modem	[007 (P/Ns 174-0506-844) with components Mech Kit 500-0506-020 Version 001]	12.3	The part numbers are equivalent and just used to differentiate the manufacturing process and sites

Table 2 – Cryptographic Module Tested Configuration

CAVP Cert1	Algorithm And Standard		Mode/ Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A3379	AES	FIPS PUB 197 NIST SP 800-38A	CBC ECB CTR	CBC (256) ECB (256) CTR (128, 192, 256)	Encryption/ Decryption
		FIPS PUB 197 NIST SP 800-38D	GCM	GCM (128, 192, 256)	Authenticated Encryption/ Decryption
		NIST SP 800-38F	KW KWP	KW (128, 192, 256) KWP (128, 192, 256)	Key Wrapping
	ECDSA	FIPS 186-4	Key Generation Key Verification Signature Generation Signature Verification	Key Generation (P-384/521) Key Verification (P-384/521) Signature Generation (P-384/521; SHA2-256, SHA2-384, SHA2-512) Signature Verification (P-384/521; SHA2-256, SHA2-384, SHA2-512)	Key Gen/ Key Ver Sign/Verify
	HMAC	FIPS PUB 198-1	SHA2-256 SHA2-384 SHA2-512	SHA2-256 SHA2-384 SHA2-512	Keyed-Hash Message Authentication
	SHS	FIPS PUB 180-4 (SHA-1 and SHA-2 functions)	SHA2-256 SHA2-384 SHA2-512	SHA2-256 SHA2-384 SHA2-512	Hashing
	KAS-ECC-SSC	NIST SP800-56arev3	Scheme(s): Ephemeral Unified and onePassUnified	KAS-ECC-SSC: Domain Parameter Generation Methods: P-384, P-521	Key Agreement
	KAS-ECC[1]	NIST SP800-56arev3	Scheme(s): Ephemeral Unified	KAS-ECC: Domain Parameter Generation Methods: P-384, P-521	Key Agreement
	KDF SP 800-108	NIST SP 800-108	Kdf Mode: Counter Mac Mode: HMAC SHA2-256	HMAC SHA2-256 Supported Lengths: 96, 256 bits	Key Derivation
	CVL	RFC8446	TLS 1.3 KDF:	TLS 1.3 KDF:	Key Derivation

[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 Cert1	Algorithm And Standard		Mode/ Method	Description / Key Size(s) / Key Strength(s)	Use / Function
		NIST SP 800-135rev1	Running Mode: DHE and PSK-DHE	HMAC Algorithm: SHA2-256 and SHA2-384	
	KDA	NIST SP 800-56Crev1	Two Step KDF Mode: counter MAC Modes: HMAC-SHA2-256	Supported Lengths: 256 Counter Lengths: 8 Derived Key Length: 256 Shared Secret Length: 256	Key Derivation
	DRBG	NIST SP 800-90Arev1	AES CTR DRBG	AES CTR DRBG 256 with prediction resistance enabled; derivation function disabled	Random Bit Generation
KAS-ECC-SSC Sp800-56Ar3/ **A3379** TLS v1.3 KDF/ **A3379**	KAS-1	NIST SP 800-56Arev3	KAS-ECC-SSC with TLS v1.3 KDF per IG D.F Scenario 2 path (2)	P-384 and P-521 curves providing 192 bits and 256 bits of encryption strength	Key Agreement
KAS-ECC-SSC Sp800-56Ar3/ **A3379** KDA TwoStep Sp800-56Cr1/ **A3379**	KAS-2	NIST SP 800-56Arev3	KAS-ECC-SSC with NIST SP 800-56Crev1 KDA TwoStep per IG D.F Scenario 2 path (2)	P-384 and P-521 curves providing 192 bits and 256 bits of encryption strength	Key Agreement
KAS-ECC Sp800-56Ar3/ **A3379**	KAS-3	NIST SP 800-56Arev3	KAS-ECC per IG D.F Scenario 2 path (1)	P-384 and P-521 curves providing 192 bits and 256 bits of encryption strength	Key Agreement
AES-KW/ **A3379** AES-KWP/ **A3379**	KTS-1	SP 800-38D and SP 800-38F	KTS (key wrapping) per IG D.G	128, 192, and 256- bit keys providing 128, 192, or 256 bits of encryption strength	Key Wrapping
AES-GCM/ **A3379**	KTS-2	SP 800-38F	KTS (key wrapping) per IG D.G	128, 192, and 256- bit keys providing 128, 192, or 256 bits of encryption strength	Key Wrapping in the context of TLS v1.3
A3305	AES	FIPS PUB 197 NIST SP 800-38A	ECB	256 bits	Tested as a pre-requisite for AES GCM
		FIPS PUB 197	GCM	256 bits	Encryption/ Decryption

CAVP Cert1	Algorithm And Standard		Mode/ Method	Description / Key Size(s) / Key Strength(s)	Use / Function
		NIST SP 800-38D			
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 Section 6.2.1 Symmetric Keys Generated Using Key-Agreement Schemes Section 6.2.2 Symmetric Keys Derived from a Pre-existing Key	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 6.2.2 Symmetric Keys Derived from a Pre-existing Key	Cryptographic Key Generation

Table 3 – Approved Algorithms

Algorithm	Caveat	Use / Function
AES	Cert. A3379, key unwrapping. Per IG D.G.	Symmetric key unwrapping

Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use / Function
AES-CBC (256 bits)	No Security Claimed	Boot image encryption
AES-XTS (256 bits)	No Security Claimed	Filesystem encryption

Table 5 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

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

Overall security design and the rules of operation

- No parts of the TLS 1.3 protocol, other than the KDF, have been tested by the CAVP and CMVP per FIPS 140-3 IG D.C.
- 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'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 protocol's implementation is contained within the boundary of the module under test.

- 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 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/host connector (providing status output only)
- SGMII/host connector (providing connectivity to external Ethernet port)
- Client interfaces using host connector
- Line port interface using optical connector for datapath encryption
- Host connector (providing connectivity to clocks and status indicators)

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
UART/Host Connector	Status Output	Status Output port
SGMII/Host Connector	Data Input, Data Output, Control Input and Status Output	TLS 1.3 communication
Host Connector (providing connectivity to client interface)	Data Input and Data Output	Plaintext Non-Security User Data
Optical Connector (providing connectivity to Line port interface)	Data Input, Data Output Control Input, Control Output And Status Output	Control and status input and output encrypted using TLS 1.3 and client payload encrypted with AES-GCM
Host connector (providing connectivity to power interface)	Power Interface	Power Input
eMMC	Data Input	Firmware Load

Table 6 – Ports and Interfaces

4. Roles, Services, and Authentication

The module supports one authorized role (i.e., 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 assumed explicitly by the Ciena Control Processor Module that configures and monitors the module. The Ciena Control Processor Module authenticates to the module using TLS 1.3 certificate-based authentication.

Role	Service	Input	Output
CO	Initialize the module	SSPs, Command	Command response
CO	Configure PSK and certificate	SSPs, Command	Command response
CO	Zeroise (Perform zeroisation.)	Command	Command response
CO	Datapath Encryption/ Decryption Service (Perform approved security functions)	SSPs, Command	Command response
CO	Report the firmware version, alarms, Status and Statistics (Show status, Show module's versioning information)	Command	Command response
CO	Perform a firmware upgrade	Command	Command response
CO	Perform operator re-authentication	SSPs, Command	Command response
CO	Issue re-authentication command	SSPs, Command	Command response
CO	Perform on demand self-tests (Perform self-tests)	Reboot	N/A

Table 7 – Roles, Service Commands, Input and Output

The services that require operator to assume an authorized role are listed in Table 9 below. Please note that the Sensitive Security Parameters (SSPs) listed in Table 9 use the following indicators to show the type of access required:

- 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

Role	Authentication Method	Authentication Strength
CO	Datapath Customer Enrolled Certificate	The module supports ECDSA P-384 and P-521 digital certificate authentication of Peers for

Role	Authentication Method	Authentication Strength
		Datapath Encryption. Using conservative estimates and equating the use of ECDSA P-384-bit certificate to 128 bits of security, the probability for a random attempt to succeed is: 1:2^192 or 1: 6.277 x 10^57 which is less than 1:1,000,000. The fastest network connection supported by the modules over Management interfaces is 10MBits/s; Hence, at most 10 ×10^6 × 60 = 6 × 10^8 = 600,000,000 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: (2^192 possible keys) / ((6 × 10^8 bits per minute) / 192 bits per key)) 1: (2^192 possible keys / 3125000 keys per minute) 1: (2 × 10^51) which is less than 1:100,000 within one minute
CO	Datapath Customer Enrollment Pre-Shared Key (PSK)	The module supports the use of a pre-Shared key for Datapath Encryption peer authentication for Users; The Pre-Shared key is 32 bytes in length. Using conservative estimates, the probability for a random attempt to succeed is: 1:2^256 or 1: 1.579 × 10^77 which is less than 1:1,000,000. The fastest network connection supported by the modules over the management interface is 10 MBits/s; Hence, at most 10 ×10^6 × 60 = 6 × 10^8 = 600,000,000 bits of data can be transmitted in one minute;

Role	Authentication Method	Authentication Strength
		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 × 10^8 bits per minute) / 256 bits per key)) 1: (2^256 possible keys / 2,343,750 keys per minute) 1: 4.94 × 10^70 which is less than 1:100,000 within one minute
CO	Initial Device ID (iDevID) and Local Device ID (LDevID) Public Key	The module supports ECDSA digital certificate authentication of COs over the TLS 1.; Using conservative estimates and equating the use of ECDSA with P-521 elliptic curve to a 256-bit strength, the probability for a random attempt to succeed is: 1:2^256 or 1: 1.579 × 10^77 which is less than 1:1,000,000 The fastest network connection supported by the modules over Management interfaces is 2.5 GB/s; Hence, at most 2.5 ×10^9 × 60 = 15 × 10^10 = 150,000,000,000 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 / ((15 × 10^10 bits per minute) / 256 bits per key)) 1: (2^256 possible keys / 585,937,500 keys per minute) 1: 1.97 × 10^68 which is less than 1:100,000 within one minute

Table 8 – Roles and Authentication

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 7). None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

- Authentication

The module supports identity-based authentication. Module operators must authenticate to the module before being allowed access to services that require the assumption of an authorized role. The CO authenticates to the module from the Control Processor module using the TLS 1.3 protocol. The TLS 1.3 uses an ECDSA (P-521) public key.

The module can be configured to use either a Pre-Shared Key or X.509 Certificate for module peer authentication. The pre-shared key is a 256-bit key. The X.509 certificate is P-384 or P-521.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
Initialize the module	Perform initialization of the module	HMAC-SHA2-256 #A3379; AES-GCM, ECB, 256 bits, #A3379; KDA TwoStep Sp800-56Cr1 #A3379; CKG; CTR_DRBG #A3379; ECDSA P-521 #A3379; KDA TwoStep Sp800-56Cr1 #A3379; CKG;	HUK HYDRA_KDK, BLOB_KEY, DRBG Seed, DRBG Key, DRBG V, Entropy Input, DRBG Output TLS 1.3 pre shared key (TLS-PSK), TLS 1.3 Pre-Master Secret, TLS 1.3 Master Secret, TLS 1.3 Authentication Key, TLS Session Key, DPE_ECDH Public Key,	CO	(E) (G) (R, G, E),	Event Log and a Global Approved mode indicator (show status indicator)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
		KDF TLS 1.3 #A3379; HMAC SHA2-384 #A3379; AES GCM, ECB 256-bit keys #A3379; KTS-2 #A3379; KAS-ECC P-384, P-521 #A3379	DPE_ECDH Private Key, DPE "Z" Value, DPE MacKey, Datapath Customer Enrolled Certificate			
Configure PSK and certificate	Set to PSK mode and provision the PSK or set to certificate mode and provision the certificate 32-256 bytes	ECDSA P-521 #A3379; KDA TwoStep Sp800-56Cr1 #A3379; CKG; KDF TLS 1.3 #A3379; HMAC SHA2-384 #A3379; AES GCM, ECB 256-bit keys #A3379; KTS-2 #A3379;	Datapath Customer Enrolled Preshared key (PSK), Datapath pre shared key (DPE-PSK), TLS 1.3 pre shared key (TLS-PSK) TLS 1.3 Pre-Master Secret, TLS 1.3 Master Secret, TLS 1.3 Authentication Key, TLS	CO	(W) (G) (G) (E)	Event logs and 'show' commands and a Global Approved mode indicator (show status indicator)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
		KAS-ECC P-384, P-521 #A3379	Session Key, DPE_ECDH Public Key, DPE_ECDH Private Key, DPE "Z" Value, DPE MacKey, Datapath Customer Enrolled Certificate Or TLS 1.3 pre shared key (TLS-PSK), TLS 1.3 Pre-Master Secret, TLS 1.3 Master Secret, TLS 1.3 Authentication Key, TLS Session Key, DPE_ECDH Public Key, DPE_ECDH Private Key, DPE "Z" Value, DPE MacKey, Datapath Customer Enrolled Certificate		Or (W) (E)	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
Zeroise (Perform zeroisation)	Power Down	All SSPs except those loaded at the factory	N/A	CO	N/A	"Show" commands and successful completion of service and a Global Approved mode indicator (show status indicator)
Datapath Encryption/ Decryption Service (Perform approved security functions)	Initiate the TLS session to the peer modem, perform the key agreement protocol and configure the datapath keys; Automatically performed when PSK or certificate is provisioned	ECDSA P-521 #A3379; KDF SP800-108 #A3379; KDA TwoStep Sp800-56Cr1 #A3379; CKG; KDF TLS 1.3 #A3379; HMAC SHA2-384 #A3379; AES GCM, ECB 256-bit keys #A3379; KTS-2 #A3379; KAS-ECC P-384, P-521	Datapath pre shared key (DPE-PSK) TLS 1.3 pre shared key (TLS-PSK), TLS 1.3 Pre-Master Secret, TLS 1.3 Master Secret, TLS 1.3 Authentication Key, TLS Session Key, Datapath Customer Enrolled Certificate DPE_ECDH Public Key, DPE_ECDH Private Key,	CO	(E) (R, G,E) (G, E, W) (G, E, Z)	Event logs and a Global Approved mode indicator (show status indicator)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
		#A3379	DPE “Z” Value, DPE MacKey, DPE_KDK, Datapath Cipher Encrypt/Decrypt keys (x16) (DDEK/DDDK)			
Report the firmware version, alarms, Status and Statistics (Show status, Show module’s versioning information)	View the firmware version, encryption related alarms, status and performance monitoring statistics	N/A	N/A	CO	N/A	Show Command Response and a Global Approved mode indicator (show status indicator)
Perform a firmware upgrade[2]	Initiate the upgrade of the modem firmware when directed by the CO via control input interface (SGMII)	ECDSA P-521 SHA2-512	LOAD_KEY	CO	N/A	Event Log and “show” commands to verify the updated version

[2] For firmware load test, the module runs ECDSA P-521 with SHA2-512 check. Please note that the module does not support complete image replacement.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
Perform operator re-authentication	Authenticate the CO with the module and replace the authentication material; This is performed when received via the optical control input interface	ECDSA P-521 #A3379; CKG; KDA TwoStep Sp800-56Cr1 #A3379; KDF TLS 1.3 #A3379; HMAC SHA2-384 #A3379; AES GCM, ECB 256-bit keys #A3379; KTS-2 #A3379; KAS-ECC P-384, P-521 #A3379	COID Public, IDEVID public key, IDEVID private key, Logical Device ID public key, Logical Device ID private key, TLS 1.3 pre shared key (TLS-PSK), TLS 1.3 Pre-Master Secret, TLS 1.3 Master Secret, TLS 1.3 Authentication Key, TLS Session Key, DPE_ECDH Public Key, DPE_ECDH Private Key, DPE “Z” Value, DPE MacKey, Datapath Customer Enrolled Certificate	CO	(W) (E, R) (G, W) (W, E, R)	Event Log

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSPs	Indicator
Issue re-authentication command	Send command to remote modem to initiate a re-authentication with the COvia optical control output interface	ECDSA P-521 #A3379; KDA TwoStep Sp800-56Cr1 #A3379; CKG; KDF TLS 1.3 #A3379; HMAC SHA2-384 #A3379; AES GCM, ECB 256-bit keys #A3379; KTS-2 #A3379; KAS-ECC P-384, P-521 #A3379	TLS 1.3 pre shared key (TLS-PSK), TLS 1.3 Pre-Master Secret, TLS 1.3 Master Secret, TLS 1.3 Authentication Key, TLS Session Key, DPE_ECDH Public Key, DPE_ECDH Private Key, DPE "Z" Value, DPE MacKey, Datapath Customer Enrolled Certificate	CO	(W, E, R)	Event Log
Perform on demand self-tests (Perform self-tests)	Perform pre-operational self-tests on demand via module restart	ECDSA P-521 SHA2-512	FIT_PUBLIC	CO, Unauthorised	N/A	Event Log and a Global Approved mode indicator (show status indicator)

Table 9 – Approved Services

Self-initiated Cryptographic Output

The module supports self-initiated cryptographic output functionality via the Datapath Encryption/ Decryption Service. Before enabling this service, the CO must configure and perform two independent internal actions in order for the service to get activated. The independent internal actions are as follows:

1) The CO must authenticate with the modem.
2) The CO must perform the service to activate PSK or install a certificate authentication.

5. Software/Firmware Security

The module uses ECDSA P-521 using SHA2-512 for firmware integrity testing/verification. The FIT_PUBLIC, an ECDSA P-521 SHA2-512 Public key, is used to authenticate the Linux kernel. This is run at startup and on demand by reloading the module. The module also runs the self-tests for ECDSA Signature verification, SHA2-256 and SHA2-512 prior to running the integrity check. The executable form of the module firmware is a pre-compiled binary.

6. Operational Environment

The module is a hardware module with the embodiment type as a multi-chip embedded cryptographic 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.

The requirements per this section do not apply to the module since the module claims to meet Physical Security Level 2 requirements.

7. Physical Security

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

Table 10 – Physical Security Inspection Guidelines

The module is shipped from the factory with the required physical security mechanisms (tamper-evident seals, metal covers and PCB layers) installed. The CO must perform a physical inspection of the unit for signs of damage and to ensure that all physical security mechanisms are in place. Additionally, the CO should check the package for any irregular tears or openings. If damage is found or tampering is suspected, the CO should follow internal security policies which include contacting Ciena. The Figure 2 in Section 2 of this document shows the placement of the tamper seals.

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

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
Hardware Unique Key (HUK) CSP	256 bits	HMAC-SHA2-256 #A3379	N/A	Preloaded at the factory Never exits the module	N/A	Read-only eFUSE in plaintext	N/A	Used to derive secondary Keys (HYDRA_KDK)
HYDRA_KDK CSP	256 bits	AES-GCM, ECB, #A3379 KDA TwoStep Sp800-56Cr1 #A3379 CKG	Derived from HUK	Never exits the module	N/A	RAM Only	Zeroised after use	Used to derive BLOB_KEY
BLOB_KEY CSP	256 bits	AES GCM, ECB #A3379, KDA TwoStep Sp800-56Cr1 #A3379 CKG	Derived from HYDRA_KDK (KDA TwoStep Sp800-56Cr1)	Never exits the module	N/A	RAM Only	Zeroised after use	Used for decrypting the iDevID private key (IDEVID)
DRBG Seed CSP	384-bits	CTR_DRBG #A3379	Generated internally using entropy input	Never exits the module	N/A	Stored in plaintext in RAM	Reboot or power removal	Used for random number generation
DRBG Key CSP	256-bits	CTR_DRBG #A3379	Generated internally using entropy input	Never exits the module	N/A	Stored in plaintext in RAM	Reboot or power removal	Used for random number generation
DRBG V CSP	256-bits	CTR_CRBG #A3379	Generated internally using entropy input	Never exits the module	N/A	Stored in plaintext in RAM	Reboot or power removal	Used for random number generation
DRBG Output CSP	128-bits	CTR_DRBG #A3379	Generated internally using	Never exits the module	N/A	Stored in plaintext in RAM	Reboot or power removal	Used for random number

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
			entropy input					generation
Entropy Input CSP	384 bits	ESV Cert. #E39	Generated internally using entropy source	Never exits the module	N/A	Stored in plaintext in RAM	Reboot or power removal	Used for random number generation
Datapath Customer Enrolled Preshared key (PSK) CSP	256-bits	ECDSA P-521 #A3379; KTS-2 #A3379	N/A	Enters the module via TLS 1.3 Never exits the module	N/A	RAM Only	Reboot or power removal	Used to derive the DPE-PSK and TLS-PSK
Datapath Customer Enrolled Certificate PSP	256-bits	ECDSA P-521 #A3379; KTS-2 #A3379	N/A	Enters the module via TLS 1.3 Never exits the module	N/A	RAM Only	Reboot or power removal	Used for remote device TLS 1.3 connection
Datapath pre shared key (DPE-PSK) CSP	256-bits	ECDSA P-521 #A3379, KDA TwoStep Sp800-56Cr1#A3379 CKG	Generated internally from the PSK using KDA TwoStep Sp800-56Cr1	Never exits the module	N/A	RAM Only	Reboot or power removal	Used during the datapath key agreement
TLS 1.3 pre shared key (TLS-PSK) CSP	256-bits	ECDSA P-521 #A3379, KDA TwoStep Sp800-56Cr1 #A3379 CKG	Generated internally from the PSK using KDA TwoStep Sp800-56Cr1	Never exits the module	N/A	RAM Only	Reboot or power removal	Used during the TLS 1.3 handshake
IDEVID public key	256-bits	ECDSA P-521	N/A	Loaded at the	N/A	Read-Only	N/A	Default authenti

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
PSP		#A3379		factory Exits in plaintext		Stored encrypted in non-volatile memory with the BLOB_KEY		cation material for CO using TLS 1.3
IDEVID private key CSP	256-bits	ECDSA P-521 #A3379	N/A	Loaded at the factory Never exits the module	N/A	Read-Only Stored encrypted in non-volatile memory with the BLOB_KEY	N/A	Default authenti cation material for CO using TLS 1.3
COID Public PSP	256-bits	ECDSA P-521 #A3379; KTS-2 #A3379	N/A	Imported via TLS 1.3 during the first connecti on with the CO Never exits the module	N/A	RAM Only	Reboot or power removal	Used for CO to module authenti cation using TLS 1.3
Logical Device ID Public Key PSP	256-bits	ECDSA P-521 KeyGen #A3379 CKG	Generated internally using Module's DRBG and FIPS 186-4	Exits in plaintext	N/A	RAM Only	Reboot or power removal	Used for CO to module authenti cation using TLS 1.3
Logical Device ID Private Key CSP	256-bits	ECDSA P-521 KeyGen #A3379 CKG	Generated internally using Module's DRBG and FIPS 186-4	Never exits the module	N/A	RAM Only	Reboot or power removal	Used for CO to module authenti cation using TLS 1.3
TLS 1.3 Pre-Master	256 bits	KDF TLS 1.3 #A3379	Generated	Never exits the module	N/A	RAM Only	Session termination, Reboot, or	Establish the TLS

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
Secret CSP			internally by module's DRBG during session negotiation				power removal	Master Secret
TLS 1.3 Master Secret CSP	256 bits	KDF TLS 1.3 #A3379	Derived using TLS Pre-Master Secret during session negotiation	Never exits the module	During TLS 1.3 handshake	RAM Only	Session termination, Reboot, or power removal	Establish the TLS Session and authentication Key
TLS 1.3 Authentication Key CSP	256 bits	HMAC SHA2-384 #A3379, KDF TLS 1.3 #A3379, CKG	Derived using KDF TLS 1.3 during session negotiation	Never exits the module	During TLS 1.3 handshake	RAM Only	Session termination, Reboot, or power removal	Used for authenticating TLS communication
TLS Session Key CSP	256 bits	AES GCM, ECB 256-bit keys #A3379, KDF TLS 1.3 #A3379, CKG	Derived via KDF TLS 1.3 during session negotiation	Never exits the module	During TLS 1.3 handshake	RAM Only	Session termination, Reboot, or power removal	Used for encrypting the TLS communication
DPE_ECDH Public Key PSP	128 bits, 256 bits	KAS-ECC P-384, P-521 #A3379, KDF TLS 1.3 #A3379, CKG	For the public component of the module: generated internally during negotiation For the public component of a peer: generate externally and enters during the	For the public component of the module: exits the module in plaintext For the public component of a peer: never exits	During datapath encryption /decryption service	RAM Only	Session termination, reboot, or power removal	Used for exchanging shared secret to derive session keys during key agreement

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
			TLS 1.3 handshake	the module				
DPE_ECDH Private Key CSP	128 bits, 256 bits	KAS-ECC P-384, P-521 #A3379, KDF TLS 1.3 #A3379, CKG	Generated internally during TLS 1.3 negotiation	Never exits the module	During datapath encryption /decryption service	RAM	By session termination, reboot, or power removal	Used for exchanging shared secret to derive session keys during key agreement
DPE "Z" Value CSP	128 bits, 256 bits	KAS-ECC P-384, P-521 #A3379	Generated internally during key agreement negotiation	Never exits the module	During datapath encryption - decryption service	RAM	Zeroised by reboot or power removal and after use	Shared secret resulting from the ECDHE exchange between peers
DPE Mac Key CSP	128 bits, 256 bits	KAS-ECC-SSC P-384, P-521 #A3379, KDA TwoStep Sp800-56Cr1 #A3379 CKG	Generated internally during key agreement negotiation (UsingKDA TwoStep Sp800-56Cr1)	Never exits the module	N/A	RAM	Zeroised by reboot or power removal once the key is programmed into HW cipher	Used to authenticate key agreement messages
DPE_KDK CSP	128 bits, 256 bits	KAS-ECC-SSC P-384, P-521 #A3379, KDA TwoStep Sp800-56Cr1 #A3379, CKG	Generated internally during key agreement negotiation (Using KDA TwoStep Sp800-56Cr1)	Never exits the module	N/A	RAM	Zeroised by reboot or power removal once the key is programmed into HW cipher	Master key derivation key used to derive the datapath cipher keys and IVs

Key/SSP Name/ Type	Strength	Security Function and Cert. Number	Gener-ation	Import /Export	Establish-ment	Storage	Zero-isation	Use & related keys
Datapath Cipher Encrypt/Decrypt keys (x16) (DDEK/DDDK) CSP	256 bits	AES GCM, ECB 256-bit key #A3305 KDF SP800-108 #A3379 CKG	Derived internally using a KDF SP 800-108 function from the DPE_KDK	Never exits the module	N/A	RAM	Zeroised by reboot or power removal once the key is programmed into HW cipher	Used for encryption and decryption of the datapath

Table 11 – SSPs

The Module contains the following non-SSPs:

- VAULT_PUBLIC; 256 bits; ECDSA P-256 public key #A3379; Used to authenticate the Vault firmware image.
- BOOT_PUB; ECDSA P-521 Public key #A3379; Used to authenticate boot image
- FIT_PUBLIC; ECDSA P-521 Public key #A3379; Used to authenticate the Linux kernel
- ROOTFS_PUB; ECDSA P-521 Public key #A3379; Used to authenticate the ROOTFS of the SW load.
- LOAD_KEY; ECDSA P-521 Public key #A3379; Used for the load check during upgrades.

Key Generation and Entropy

The module generates keys as described in SP 800-133rev2 Section 4, Option #1, 5.1, 5.2, 6.2.1 and 6.2.2. It uses an Approved CTR_DRBG (as specified in SP 800-90Arev1) to generate symmetric keys and seed for asymmetric keys. The DRBG is seeded from seeding material provided by a hardware-based (Wavelogic 5e Encryption Modem EIP-76 TRNG), which provides an entropy source and unbiased random sequence of bits to the DRBG.

The module is a hardware module with an entropy generating inside the module's cryptographic boundary compliant with Scenario 1 (a) described in FIPS 140-3 IG 9.3.A. The entropy source produces 256-bit output samples with full i.e., 256 bits of entropy.

Entropy sources	Minimum number of bits of entropy	Details
SP 800-90B ESV Cert. #E39	0.5/bit	SP 800-90B compliant entropy source with a ring oscillator - based noise source

Table 12 – Non-Deterministic Random Number Generator 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. The pre-operational firmware integrity test (using ECDSA P-521 SHA2-512) can be run on demand by reloading the module.

1. **Pre-operational self-tests**:
    a. Firmware Integrity test using ECDSA P-521/SHA2-512

2. **Conditional self-tests:**
    a. conditional cryptographic algorithm test
        - Ciena WaveLogic 5e Encryption Modem Crypto Implementation:
        - AES-CBC 128-bit KAT (Encrypt)
        - AES-CBC 128-bit KAT (Decrypt)
        - AES-GCM 256-bit KAT (Encrypt)
        - AES-GCM 256-bit KAT (Decrypt)
        - SHA2-256 KAT
        - SHA2-384 KAT
        - SHA2-512 KAT
        - HMAC-SHA2-256 KAT
        - HMAC-SHA2-384 KAT
        - HMAC-SHA2-512 KAT
        - AES-256 CTR DRBG KAT
            - SP800-90Arev1 Section 11 health tests
        - SP800-56Arev3 KAS-ECC-SSC KAT (Curve used: P-521)
            521
        - ECDSA P-521 Sign KAT
        - ECDSA P-521 Verify KAT
        - KDF NIST SP 800-108 (HMAC SHA2-256) KAT
        - One-Step KDA KAT
        - Two Step KDA KAT
        - TLS 1.3 KDF KAT

        - Ciena WaveLogic 5e Encryption Modem Datapath Ciphers Implementation:
        - AES-GCM KAT (Encrypt)
        - AES-GCM KAT (Decrypt)
        - Repetition Count Test on ENT
        - Adaptive Proportion Test on ENT

    b. Conditional pair-wise consistency test:

- ECDSA keys generated for signature generation/verification and ECDSA keys used for key agreement

c. Conditional Firmware Load test: ECDSA P-521 SHA2-512

The CAST for the cryptographic algorithms used to perform the Approved integrity technique, ECDSA P-521 SHA2-512 KATs, occur before the integrity test.

The module implements the above cryptographic algorithm self-tests which are run prior to the first use of the algorithm for the cryptographic operations and are also classified as a part of conditional self-tests.

Upon the failure of any pre-operational self-test and the cryptographic algorithm self-tests, the module goes into “Critical Error” state and disables all access to cryptographic functions and SSPs. A permanent error status will be relayed via the status output interface, which then raises an alarm and adds an entry to the system log file. In case of a firmware integrity failure, the module returns “failed loading sn kernel image” and “Cryptographic Algorithm Self-Test failure” in case of one or more CAST failures.

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 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.

11. Life-Cycle Assurance

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

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

The module is always delivered via commercial bounded carrier.

The shipment will contain a packing slip with the serial numbers of all shipped devices. Prior to deployment the receiver shall verify that the hardware serial numbers match the serial numbers listed in the packing slip. The module is shipped from the factory with the required physical security mechanisms (tamper-evident labels, metal covers and PCB layers) installed. The CO must perform a physical inspection of the unit for signs of damage and to ensure that all physical security mechanisms are in place. Additionally, the CO should check the package for any irregular tears or openings. If damage is found or tampering is suspected, the CO should immediately contact Ciena.

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

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

12. Mitigation of Other Attacks

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

End of Document