

Ciena Corporation

WaveLogic 5 Extreme Encryption Modem

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

1 General	5
1.1 Overview	5
1.2 Security Levels	6
1.3 Additional Information	6
2 Cryptographic Module Specification	6
2.1 Description	6
2.2 Tested and Vendor Affirmed Module Version and Identification	8
2.3 Excluded Components	9
2.4 Modes of Operation	9
2.5 Algorithms	9
2.6 Security Function Implementations	13
2.7 Algorithm Specific Information	18
2.8 RBG and Entropy	19
2.9 Key Generation	19
2.10 Key Establishment	19
2.11 Industry Protocols	20
3 Cryptographic Module Interfaces	20
3.1 Ports and Interfaces	20
4 Roles, Services, and Authentication	20
4.1 Authentication Methods	20
4.2 Roles	22
4.3 Approved Services	23
4.4 Non-Approved Services	32
4.5 External Software/Firmware Loaded	32
4.6 Cryptographic Output Actions and Status	32
5 Software/Firmware Security	32
5.1 Integrity Techniques	32
5.2 Initiate on Demand	33
6 Operational Environment	33
6.1 Operational Environment Type and Requirements	33
7 Physical Security	33
7.1 Mechanisms and Actions Required	33
8 Non-Invasive Security	34
8.1 Mitigation Techniques	34
9 Sensitive Security Parameters Management	34

9.1 Storage Areas	34
9.2 SSP Input-Output Methods	34
9.3 SSP Zeroization Methods	35
9.4 SSPs	35
10 Self-Tests	44
10.1 Pre-Operational Self-Tests	44
10.2 Conditional Self-Tests	44
10.3 Periodic Self-Test Information	48
10.4 Error States	50
11 Life-Cycle Assurance	52
11.1 Installation, Initialization, and Startup Procedures	52
11.2 Administrator Guidance	52
11.3 Non-Administrator Guidance	52
11.4 End of Life	52
11.5 Additional Information	52
12 Mitigation of Other Attacks	53
12.1 Attack List	53

List of Tables

Table 1: Security Levels	6
Table 2: Tested Module Identification – Hardware	9
Table 3: Modes List and Description	9
Table 4: Approved Algorithms	12
Table 5: Vendor-Affirmed Algorithms	12
Table 6: Non-Approved, Allowed Algorithms with No Security Claimed.....	13
Table 7: Security Function Implementations.....	18
Table 8: Entropy Certificates	19
Table 9: Entropy Sources.....	19
Table 10: Ports and Interfaces	20
Table 11: Authentication Methods.....	22
Table 12: Roles.....	22
Table 13: Approved Services	32
Table 14: Mechanisms and Actions Required	33
Table 15: Storage Areas	34
Table 16: SSP Input-Output Methods.....	35
Table 17: SSP Zeroization Methods.....	35
Table 18: SSP Table 1	40
Table 19: SSP Table 2.....	43
Table 20: Pre-Operational Self-Tests	44
Table 21: Conditional Self-Tests	48
Table 22: Pre-Operational Periodic Information.....	48
Table 23: Conditional Periodic Information.....	50
Table 24: Error States.....	51

List of Figures

Figure 1: Block Diagram.....	7
Figure 2: Cryptographic Boundary of WaveLogic 5 Extreme Encryption Modem (represents all P/Ns in Table 2)	8

1 General

1.1 Overview

Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140-3 program. The NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program>.

About this Document

This non-proprietary Cryptographic Module Security Policy for the 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 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 document describes the cryptographic module non-proprietary security policy for the WaveLogic 5 Extreme Encryption Modem (Firmware Version 14.1) 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.

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 Module.

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

1.2 Security Levels

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

Table 1: Security Levels

1.3 Additional Information

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The WaveLogic 5 Extreme Encryption Modem is an optical transponder daughter card installed within a Ciena optical transponder service module. 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).

Module Type: Hardware

Module Embodiment: Multi-Chip Embedded

Cryptographic Boundary:

Figure 1 below shows the cryptographic boundary of the module (highlighted in red).

Tested Operational Environment's Physical Perimeter (TOEPP):

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.

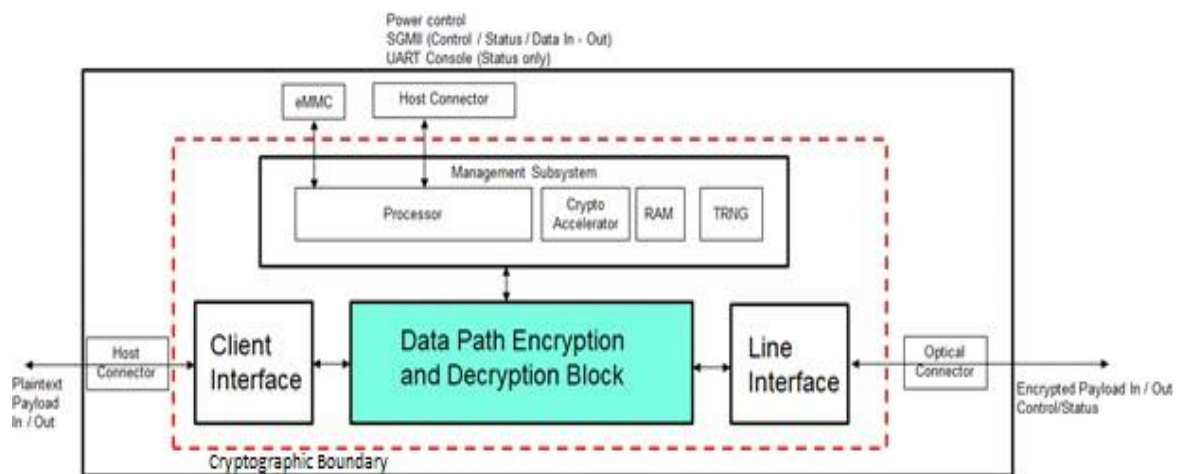


Figure 1: Block Diagram



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

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
P/N 174-0506-844 with components Mech Kit 500-0506-020 Version 001	005, 006, 007, 008	14.1	ARM Cortex A53 (Quad Core)	The part numbers are equivalent
P/N 174-0506-841 with components Mech Kit 500-0506-020 Version 001	008, 009, 010, 012 , 013, 014, 015 and 016	14.1	ARM Cortex 53 (Quad Core)	The part numbers are equivalent
P/N 174-0506-842 with components Mech Kit 500-0506-020 Version 001	007, 008, 009, 010, 012, 013, 014, 015 and 016	14.1	ARM Cortex 53 (Quad Core)	The part numbers are equivalent
P/N 174-0506-843 with components Mech Kit 500-0506-020 Version 001	014 , 015, 016, 017 and 018	14.1	ARM Cortex 53 (Quad Core)	The part numbers are equivalent

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
P/N 174-0506-84x-EB with components Mech Kit 500-0506-021 Version 001	002	14.1	ARM Cortex 53 (Quad Core)	The part numbers are equivalent
P/N 174-0506-85x-EB with components Mech Kit 500-0506-021 Version 001	002	14.1	ARM Cortex 53 (Quad Core)	The part numbers are equivalent

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

No components have been excluded from the module boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved Mode	The module operates in Approved mode by default. No additional configuration is needed for rendering or operating the module in the Approved mode.	Approved	Global Approved mode indicator (show status indicator)

Table 3: Modes List and Description

2.5 Algorithms

Approved Algorithms:

Algorithm	CAV P Cert	Properties	Reference
AES-CBC, AES-ECB	A3379	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CTR	A3379	Direction - Decrypt, Encrypt Key Length - 128, 192, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A

Algorithm	CAV P Cert	Properties	Reference
AES-ECB	A330 5	Direction - Encrypt Key Length - 256	SP 800-38A
AES-GCM	A330 5	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 256, 128 AAD Length - AAD Length: 0, 256	SP 800-38D
AES-GCM	A337 9	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - 8.2.1 Key Length - 128, 192, 256 Tag Length - 128 IV Length - IV Length: 128 Payload Length - Payload Length: 256-1024 Increment 256 AAD Length - AAD Length: 256-1024 Increment 256	SP 800-38D
AES-KW	A337 9	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 256, 192, 128	SP 800-38F
AES-KWP	A337 9	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 192, 256 Payload Length - Payload Length: 296	SP 800-38F
Counter DRBG	A337 9	Prediction Resistance - No Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - No Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 384 Nonce - Nonce: 0 Personalization String Length - Personalization String Length: 0 Returned Bits - 128	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A337 9	Curve - P-384, P-521 Secret Generation Mode - Extra Bits	FIPS 186-4
ECDSA KeyVer (FIPS186-4)	A337 9	Curve - P-384, P-521	FIPS 186-4
ECDSA SigGen (FIPS186-4),	A337 9	Curve - P-384, P-521 Hash Algorithm - SHA2-256, SHA2-384, SHA2-512	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
ECDSA SigVer (FIPS186-4)			
HMAC-SHA2-256	A3379	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-384	A3379	MAC - MAC: 32-384 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
HMAC-SHA2-512	A3379	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 256-448 Increment 8	FIPS 198-1
KAS-ECC Sp800-56Ar3	A3379	Domain Parameter Generation Methods - P-256, P-384, P-521 iutId - 123456ABCD Scheme - ephemeralUnified - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Auxiliary Function Methods - Auxiliary Function Name - SHA2-256 MAC Salting Methods - default Fixed Info Pattern - algorithmId uPartyInfo vPartyInfo Fixed Info Encoding - Concatenation Key Length - 256	SP 800-56A Rev. 3
KAS-ECC-SSC Sp800-56Ar3	A3379	Domain Parameter Generation Methods - P-256, P-384, P-521 Hash Function Z - SHA2-512 Scheme - ephemeralUnified - KAS Role - initiator, responder onePassUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDA TwoStep Sp800-56Cr1	A3379	MAC Salting Methods - default, random Supported Lengths - Supported Lengths: 256 Fixed Info Encoding - concatenation Fixed Info Pattern - literal[123456789CAFECAFE123456789CAFECAFE] uPartyInfo vPartyInfo KDF Mode - counter MAC Modes - HMAC-SHA2-256 Counter Lengths - 8 Fixed Data Order - after fixed data The KDF supports an empty IV - Yes The KDF requires an empty IV - Yes Derived Key Length - 256 Shared Secret Length - Shared Secret Length: 256	SP 800-56C Rev. 2

Algorithm	CAV P Cert	Properties	Reference
KDF SP800-108	A337 9	KDF Mode - Counter MAC Mode - HMAC-SHA2-256 Supported Lengths - Supported Lengths: 256, 96 Fixed Data Order - After Fixed Data Counter Length - 8 Supports Empty IV - Yes Custom Key In Length - 0	SP 800-108 Rev. 1
SHA2-256, SHA2-384, SHA2-512	A337 9	Message Length - Message Length: 128-65528 Increment 8	FIPS 180-4
TLS v1.3 KDF (CVL)	A337 9	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK-DHE	SP 800-135 Rev. 1

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG - Section 4	Key Type:Symmetric and Asymmetric	N/A	NIST SP800-133r2 Section 4: Using the Output of a Random Bit Generator Option 1 (Symmetric keys and seed for asymmetric keys (Option 1)); Section 5.1: Key Pairs for Digital Signature Schemes; Section 5.2: Key Pairs for Key Establishment; Section 6.2.1: Symmetric Keys Generated Using Key Agreement Schemes; Section 6.2.2 Symmetric Keys Derived from a Pre-existing Key

Table 5: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

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

Non-Approved, Allowed Algorithms with No Security Claimed:

Name	Caveat	Use and Function
AES-CBC (256 bits)	No Security Claimed	Boot Image Encryption
AES-XTS (256 bits)	No Security Claimed	Filesystem Encryption

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

Non-Approved, Not Allowed Algorithms:

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

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Initialize	AsymKeyPair- KeyGen AsymKeyPair- KeyVer BC-Auth BC-UnAuth CKG DigSig- SigGen DigSig-SigVer DRBG SHA	Perform initialization of the module.		AES-GCM: (A3379) HMAC- SHA2-256: (A3379) Counter DRBG: (A3379) CKG - Section 4: () Key Type: Symmetric and Asymmetric ECDSA KeyGen (FIPS186-4): (A3379) HMAC- SHA2-384: (A3379) AES-ECB: (A3379) ECDSA SigGen (FIPS186-4): (A3379) ECDSA SigVer (FIPS186-4): (A3379) ECDSA KeyVer (FIPS186-4): (A3379) AES-CTR: (A3379)
Configure PSK and certificate	AsymKeyPair- KeyGen	Set to PSK mode and provision the		ECDSA KeyGen

Name	Type	Description	Properties	Algorithms
	AsymKeyPair- KeyVer BC-Auth BC-UnAuth CKG DigSig- SigGen DigSig-SigVer MAC SHA	PSK or set to certificate mode and provision the certificate 32-256 bytes		(FIPS186-4): (A3379) CKG - Section 4: () Key Type: Symmetric and Asymmetric HMAC- SHA2-384: (A3379) AES-GCM: (A3379) AES-ECB: (A3379) ECDSA SigGen (FIPS186-4): (A3379) ECDSA SigVer (FIPS186-4): (A3379) ECDSA KeyVer (FIPS186-4): (A3379)
Zeroise		Power Down (Zeroise)		
Datapath Encryption/ Decryption	AsymKeyPair- KeyGen AsymKeyPair- KeyVer BC-Auth BC-UnAuth CKG DigSig- SigGen DigSig-SigVer KDKDF MAC SHA	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 KeyGen (FIPS186-4): (A3379) ECDSA KeyVer (FIPS186-4): (A3379) ECDSA SigGen (FIPS186-4): (A3379) ECDSA SigVer (FIPS186-4): (A3379) KDF SP800- 108: (A3379) CKG (SP800- 133Rev2) -

Name	Type	Description	Properties	Algorithms
				Sections 4 and 5.1: () HMAC-SHA2-384: (A3379) AES-GCM: (A3379) AES-ECB: (A3379)
Firmware Upgrade	DigSig-SigVer SHA	Initiate the upgrade of the modem firmware when directed by the CO via control input interface (SGMII)		ECDSA SigVer (FIPS186-4): (A3379) SHA2-512: (A3379)
Perform operator re-authentication	AsymKeyPair-KeyGen AsymKeyPair-KeyVer BC-Auth BC-UnAuth CKG DigSig-SigVer MAC SHA	Authenticate the CO with the module and replace the authentication material; This is performed when received via the optical control input interface		ECDSA SigVer (FIPS186-4): (A3379) HMAC-SHA2-384: (A3379) AES-GCM: (A3379) AES-ECB: (A3379) ECDSA KeyGen (FIPS186-4): (A3379) ECDSA KeyVer (FIPS186-4): (A3379) CKG - Section 4: () Key Type: Symmetric and Asymmetric
Issue re-authentication command	AsymKeyPair-KeyGen AsymKeyPair-KeyVer BC-Auth BC-UnAuth CKG DigSig-SigVer	Send command to remote modem to initiate a re-authentication with the CO via optical control output interface.		ECDSA SigVer (FIPS186-4): (A3379) HMAC-SHA2-384: (A3379) AES-GCM: (A3379)

Name	Type	Description	Properties	Algorithms
	MAC SHA			AES-ECB: (A3379) CKG - Section 4: () Key Type: Symmetric and Asymmetric ECDSA KeyGen (FIPS186-4): (A3379) ECDSA KeyVer (FIPS186-4): (A3379)
Perform on demand self- tests (Perform self-tests)	AsymKeyPair- KeyGen AsymKeyPair- KeyVer BC-Auth BC-UnAuth DigSig- SigGen DigSig-SigVer DRBG KAS-SSC KDKDF MAC SHA	Perform pre- operational self-tests on demand via module restart		ECDSA SigGen (FIPS186-4): (A3379) ECDSA SigVer (FIPS186-4): (A3379) AES-CBC: (A3379) AES-GCM: (A3379, A3305) SHA2-256: (A3379) SHA2-384: (A3379) SHA2-512: (A3379) HMAC- SHA2-256: (A3379) HMAC- SHA2-384: (A3379) HMAC- SHA2-512: (A3379) Counter DRBG: (A3379) TLS v1.3 KDF: (A3379)

Name	Type	Description	Properties	Algorithms
				KDA TwoStep Sp800-56Cr1: (A3379) KDF SP800-108: (A3379) KAS-ECC-SSC Sp800-56Ar3: (A3379) AES-ECB: (A3305) AES-CTR: (A3379)
KAS-1	KAS-Full	NIST SP 800-56Ar3 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	IG :IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800- 135rev1 CVL Caveat :Key establishment methodology provides between 192 and 256 bits of security strength	KAS-ECC- SSC Sp800- 56Ar3: (A3379) TLS v1.3 KDF: (A3379)
KAS-2	KAS-Full	NIST SP 800-56Ar3 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	IG :IG D.F Scenario 2, path (2), split Key confirmation:no Key derivation:IG 2.4.B SP 800- 135rev1 CVL Caveat:Key establishment methodology provides between 192 and 256 bits of security strength	KDA TwoStep Sp800- 56Cr1: (A3379) KAS-ECC- SSC Sp800- 56Ar3: (A3379)
KAS-3	KAS-Full	NIST SP 800-56Ar3 KAS-ECC per IG D.F Scenario 2 path (1); P-384 and P-521	IG :IG D.F Scenario 2, path (1) Key confirmation	KAS-ECC Sp800- 56Ar3: (A3379)

Name	Type	Description	Properties	Algorithms
		curves providing 192 bits and 256 bits of encryption strength	:no Key derivation: Caveat :Key establishment methodology provides between 192 and 256 bits of security strength	
KTS-1	KTS-Wrap	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	Standard:SP 800- 38F IG D.G :approved method from IG D.G Key confirmation:no Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-KW: (A3379) AES-KWP: (A3379)
KTS-2	KTS-Wrap	SP 800-38F KTS (key wrapping) in the context of TLS 1.3 per IG D.G; 128, 192, and 256- bit keys providing 128, 192, or 256 bits of encryption strength	Standard :SP 800- 38D IG D.G:approved method from IG D.G Key confirmation :no Caveat:Key establishment methodology provides between 128 and 256 bits of security strength	AES-GCM: (A3379)
Entropy Source	ENT-ESV	NIST SP 800-90B validated entropy source		

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

- In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133rev2 (vendor affirmed). The

resulting symmetric keys and seed value for asymmetric keys are the unmodified output from the Approved DRBG.

- The module'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.
- In accordance with IG 2.4.B, the CVLs i.e. TLS 1.3 KDF shall only be used in the context of the respective protocols.
- The module supports Scenario 1 (a) described in FIPS 140-3 IG 9.3.A. The entropy source produces an overall 256-bit entropy output with full i.e., 256 bits of entropy. This is sufficient to generate keys of the largest size supported by the module i.e. 256 bits.

2.8 RBG and Entropy

Cert Number	Vendor Name
E39	Ciena Corporation

Table 8: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Ciena Corporation	Physical	ARM Cortex A53 on Ciena WL5e	256 bits	Full Entropy (256 bits)	SHA2-256 CAVP Cert. #A3379

Table 9: Entropy Sources

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 an overall 256-bit entropy output with full i.e., 256 bits of entropy. This is sufficient to generate keys of the largest size supported by the module i.e. 256 bits.

2.9 Key Generation

The module generates keys as described in 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.

2.10 Key Establishment

The module supports the key establishment mechanisms as defined in the Security Functions Implementation Table in this document, namely: KAS-1, KAS-2, KAS-3, KTS-1 and KTS-2.

2.11 Industry Protocols

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.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
UART/Host Connector	Status Output	Status Output port
SGMII/Host Connector	Data Input Data Output Control Input Status Output	TLS 1.3 communication
Host Connector (providing connectivity to client interface)	Data Input Data Output	Plaintext Non-Security User Data
Optical Connector (providing connectivity to Line port interface)	Data Input Data Output Control Input Control Output 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	Power Input
eMMC	Data Input	Firmware Load

Table 10: Ports and 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)

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Datapath Customer Enrolled Certificate	The module supports ECDSA P-384 and P-521 digital certificate authentication of Peers for Datapath Encryption	ECDSA KeyVer (FIPS186-4) (A3379)	The module supports ECDSA P-384 and P-521 digital certificate authentication of Peers for Datapath Encryption. Using conservative estimates and equating the use of ECDSA P-384- bit certificate to 192 bits of security, the probability for a random attempt to succeed is: $1:2^{192}$ or $1: 6.277 \times 10^{57}$ which is less than 1:1,000,000. The fastest network connection supported by the modules over Management interfaces is 10MBits/s.	At most $10 \times 10^6 \times 60 = 6 \times 10^8 = 600,000,000$ 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: $1: (2^{192} \text{ possible keys}) / ((6 \times 10^8 \text{ bits per minute}) / 192 \text{ bits per key})$ $1: (2^{192} \text{ possible keys} / 3125000 \text{ keys per minute})$ $1: (2 \times 10^{51})$ which is less than 1:100,000 within one minute
Datapath Customer Enrolled Pre-Shared Key (PSK)	The module supports the use of a pre-Shared key for Datapath Encryption peer authentication for Users		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 $1: 1.579 \times 10^{77}$ which is less than 1:1,000,000. The fastest network connection supported by the modules over the management interface is 10 MBits/s	At most $10 \times 10^6 \times 60 = 6 \times 10^8 = 600,000,000$ 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: $1: (2^{256} \text{ possible keys} / ((6 \times 10^8 \text{ bits per minute}) / 256 \text{ bits per key}))$ $1: (2^{256} \text{ possible keys} / 2,343,750 \text{ keys per minute})$ $1: 4.94 \times 10^{70}$ which is less than 1:100,000 within one minute

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Initial Device ID (iDevID) and Local Device ID (LDevID) Public Key	The module supports ECDSA digital certificate authentication of COs over TLS 1.3		The module supports ECDSA digital certificate authentication of COs over the TLS 1.3; 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 $1:1.579 \times 10^{77}$ which is less than $1:1,000,000$. The fastest network connection supported by the modules over Management interfaces is 2.5 GB/s	At most $2.5 \times 10^9 \times 60 = 15 \times 10^{10} = 150,000,000,000$ 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: $1: (2^{256} \text{ possible keys} / ((15 \times 10^{10} \text{ bits per minute}) / 256 \text{ bits per key}))$ $1: (2^{256} \text{ possible keys} / 585,937,500 \text{ keys per minute})$ $1: 1.97 \times 10^{68}$ which is less than $1:100,000$ within one minute

Table 11: Authentication Methods

The module supports role-based authentication. Module operators must authenticate the module before being allowed access to services that require the assumption of an authorized role. The CO authenticates the module from the Control Processor (validated) 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.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
CO	Role	Crypto Officer	Datapath Customer Enrolled Certificate Datapath Customer Enrolled Pre-Shared Key (PSK) Initial Device ID (iDevID) and Local Device ID (LDevID) Public Key

Table 12: Roles

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 Module that configures and monitors the module. The Ciena Control Module authenticates to the module using TLS 1.3 certificate-based authentication.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Initialize the module	Perform initialization of the module	Event Log and a Global Approved mode indicator (show status indicator)	SSPs, Command	Command response	Initialize KAS-1 KAS-2 KAS-3 KTS-1 KTS-2 Entropy Source	CO - Hardware Unique Key (HUK) : E - HYDRA_KDK : G,E - BLOB_KEY: G,E - DRBG Seed : G,E,Z - DRBG V : G,E,Z - DRBG Key : G,E,Z - Entropy Input : G,E,Z - TLS 1.3 pre shared key (TLS- PSK): G,E,Z - TLS 1.3 Pre-Master Secret : G,E,Z - TLS 1.3 Master Secret: G,E,Z - TLS 1.3 Authentication Key: G,E,Z - TLS Session Key: G,E,Z - Datapath Customer Enrolled Certificate: W,E - Datapath

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Customer Enrolled Preshared key (PSK) : W,E - IDEVID public key: E - IDEVID private key: E - COID Public : W,E - Logical Device ID Public Key : G,R,E - Logical Device ID Private Key : G,E
Configure PSK and certificate	Set to PSK mode and provision the PSK or set to certificate mode and provision the certificate 32-256 bytes	Event logs and 'show' commands and a Global Approved mode indicator (show status indicator)	SSPs, Commands	Command response	Configure PSK and certificate KAS-1 KAS-2 KTS-1 KTS-2	CO - Datapath Customer Enrolled Preshared key (PSK) : W,E - Datapath pre shared key (DPE-PSK): G,E - TLS 1.3 pre shared key (TLS- PSK): G,E,Z - TLS 1.3 Pre-Master Secret : G,E,Z - TLS 1.3 Master Secret: G,E,Z - TLS 1.3 Authentication Key: G,E,Z - TLS Session Key: G,E,Z - Datapath Customer Enrolled Certificate: W,E - BLOB_KEY:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						E - DRBG Seed : G,E,Z - DRBG V : G,E,Z - DRBG Key : G,E,Z - Entropy Input : G,E,Z - IDEVID public key: E - IDEVID private key: E - COID Public : W,E - Logical Device ID Public Key : G,R,E - Logical Device ID Private Key : G,E
Zeroise (Perform zeroisation)	Zeroise - Power down	"Show" commands and successful completion of service and a Global Approved mode indicator (show status indicator)	Command	Command response	Zeroise	CO - HYDRA_KDK : Z - BLOB_KEY: Z - DRBG Seed : Z - DRBG V : Z - DRBG Key : Z - Entropy Input : Z - Datapath Customer Enrolled Preshared key (PSK) : Z - Datapath Customer Enrolled Certificate: Z - TLS 1.3 pre shared key (TLS- PSK): Z - COID Public :

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - Logical Device ID Public Key : Z - Logical Device ID Private Key : Z - TLS 1.3 Pre-Master Secret : Z - TLS 1.3 Master Secret: Z - TLS 1.3 Authentication Key: Z - TLS Session Key: Z - DPE_ECDH Public Key : Z - DPE_ECDH Private Key : Z - DPE "Z" Value : Z - DPE Mac Key: Z - DPE_KDK : Z - Datapath Cipher Encrypt/D encrypt keys (x16) (DDEK/DD DK): Z Unauthenticated
Datapath Encryption/Decryption Service (Perform approved security function)	Initiate the TLS session to the peer modem, perform the key agreement protocol and configure the	Event logs and a Global Approve mode indicator (show status indicator)	SSPs, Command	Command response	Datapath Encryption/Decryption KAS-1 KAS-2 KTS-1 KTS-2	CO - Datapath pre shared key (DPE-PSK): G,E - TLS 1.3 pre shared key (TLS- PSK): G,E,Z - TLS 1.3 Pre-Master Secret : G,E,Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	datapath keys; Perform approved security functions Automatically performed when PSK or certificate is provisioned.					- TLS 1.3 Master Secret: G,E,Z - TLS 1.3 Authentication Key: G,E,Z - TLS Session Key: G,E,Z - Datapath Customer Enrolled Certificate: W,E - DPE_ECDH Public Key : G,R,E,Z - DPE_ECDH Private Key : G,E,Z - DPE "Z" Value : G,E,Z - DPE Mac Key: G,E,Z - DPE_KDK : G,E - Datapath Cipher Encrypt/D encrypt keys (x16) (DDEK/DD DK): G,E - Datapath Customer Enrolled Preshared key (PSK) : W,E - BLOB_KEY: E - DRBG Seed : G,E,Z - DRBG V : G,E,Z - DRBG Key : G,E,Z - Entropy Input : G,E,Z - IDEVID public key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IDEVID private key: E - COID Public : W,E - Logical Device ID Public Key : G,R,E - Logical Device ID Private Key : G,E
Report the firmware version, alarms, Status and Statistics s (Show status, Show module's versioning information - Show Version)	View the firmware version, encryption related alarms, status and performance monitoring statistics	Show Command Response and a Global Approved mode indicator (show status indicator)	Command	Command Response and a Global Approved mode indicator (show status indicator)	None	CO
Perform a firmware upgrade	Initiate the upgrade of the modem firmware when directed by the CO via control input interface (SGMII)	Event Log and "show" commands to verify the updated version	Command	Command response	Firmware Upgrade	CO - VAULT_PUBLIC: E - BOOT_PUB: E - FIT_PUBLIC: E - ROOTFS_PUB: E - LOAD_KEY: E
Perform operator re-authentication	Authenticate the CO with the module and replace the authentication material; This is performed	Event Log	SSPs, Command	Command response	Perform operator re-authentication KAS-1 KAS-2 KTS-1 KTS-2	CO - COID Public : W,E - IDEVID public key: E - IDEVID private key: E - TLS 1.3 pre shared key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	when received via the optical control input interface					(TLS- PSK): G,E,Z - TLS 1.3 Pre-Master Secret : G,E,Z - TLS 1.3 Master Secret: G,E,Z - TLS 1.3 Authentication Key: G,E,Z - TLS Session Key: G,E,Z - Datapath Customer Enrolled Certificate: W,E - Datapath Customer Enrolled Preshared key (PSK) : W,E - BLOB_KEY: E - DRBG Seed : G,E,Z - DRBG V : G,E,Z - DRBG Key : G,E,Z - Entropy Input : G,E,Z - Logical Device ID Public Key : G,R,E - Logical Device ID Private Key : G,E
Issue re-authentication command	Send command to remote modem to initiate a re-authentication with the CO via	Event Log	SSPs, Command	Command response	Issue re-authentication command KAS-1 KAS-2 KTS-1 KTS-2	CO - COID Public : W,E - IDEVID public key: E - IDEVID private key: E - TLS 1.3 pre

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	optical control output interface					shared key (TLS- PSK): G,E,Z - TLS 1.3 Master Secret: G,E,Z - TLS 1.3 Authentication Key: G,E,Z - TLS Session Key: G,E,Z - Datapath Customer Enrolled Certificate: W,E - Datapath Customer Enrolled Preshared key (PSK) : W,E - BLOB_KEY: E - DRBG Seed : G,E,Z - DRBG V : G,E,Z - DRBG Key : G,E,Z - Entropy Input : G,E,Z - Logical Device ID Public Key : G,R,E - Logical Device ID Private Key : G,E
Perform on demand self-tests (Perform self-tests)	Perform pre-operational self-tests on demand via module restart	Event Log and a Global Approved mode indicator (show status indicator	Reboot	N/A	Perform on demand self-tests (Perform self-tests)	CO Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
External Key Service	Import keys generated external to the module	Approved Mode Indicator	IP of the external server	Key retrieved from the server	KAS-1 KAS-2 KTS-1 KTS-2	CO - BLOB_KEY: E - DRBG Seed : G,E,Z - DRBG V : G,E,Z - DRBG Key : G,E,Z - Entropy Input : G,E,Z - Datapath Customer Enrolled Preshared key (PSK) : W,E - Datapath Customer Enrolled Certificate: W,E - TLS 1.3 pre shared key (TLS- PSK): G,E,Z - TLS 1.3 Master Secret: G,E,Z - TLS 1.3 Pre-Master Secret : G,E,Z - TLS 1.3 Authentication Key: G,E,Z - TLS Session Key: G,E,Z - Logical Device ID Public Key : G,R,E - Logical Device ID Private Key : G,E - COID Public : W,E - IDEVID public key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- IDEVID private key: E

Table 13: Approved Services

The services that require operators 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 = Zeroize: The module zeroizes the SSP.

In Approved mode, the module provides a limited number of services for which the operator is not required to assume an authorized role (see Table 14). None of the services listed in the table disclose cryptographic keys and CSPs or otherwise affect the security of the module.

4.4 Non-Approved Services

The module does not support any Non-Approved Services.

4.5 External Software/Firmware Loaded

For the firmware load test, the module runs ECDSA P-521 with SHA2-512 check. Please note that the module does not support a complete image replacement. Any firmware/software loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-3 validation.

4.6 Cryptographic Output Actions and Status

The module supports self-initiated cryptographic output 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

5.1 Integrity Techniques

The module uses ECDSA P-521 using SHA2-512 for the firmware integrity testing/verification. 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. The FIT_PUBLIC, an ECDSA P-521 SHA2-512 Public key, is used to authenticate the Linux kernel.

5.2 Initiate on Demand

The firmware integrity test is performed at startup and can be performed on demand by reloading the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

How Requirements are Satisfied:

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

7.1 Mechanisms and Actions Required

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

Table 14: Mechanisms and Actions Required

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

8.1 Mitigation Techniques

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Stored in plaintext in RAM	Dynamic
eFUSE	Read-only eFUSE in plaintext	Static
NVM	Stored in plaintext in NVM	Static
NVM (Encrypted)	SSPs stored encrypted using BLOB_KEY in the non-volatile memory	Static

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Pre-loaded at the factory and never exits the module (eFUSE)	Generated externally by the manufacturer	eFuse	Plaintext	N/A	N/A	
Loaded at the factory (NVM)	Generated externally by the manufacturer	NVM	Plaintext	N/A	N/A	
Imported via TLS 1.3 and never exits the module (RAM)	External endpoint	RAM	Encrypted	Automated	Electronic	KTS-2

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Exits in plaintext (RAM)	RAM	External endpoint	Plaintext	Automated	Electronic	
For the public component of the module: exits the module in plaintext (RAM)	RAM	External endpoint	Plaintext	Automated	Electronic	

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reboot or Power Removal	Reboot or Power Removal	SSP stored temporarily/ephemerally in RAM.	Manually by the operator, on demand
Zeroise after use	Zeroise after use	Automatic zeroisation per module design after use	Module initiated, automatically after use
Session Termination	Session Termination	SSP stored temporarily/ephemerally in RAM.	Module initiated, automatically after use
Reboot or Power Removal post programming into HW cipher	Zeroised by reboot or power removal once the SSP is programmed into HW cipher	SSPs stored temporarily/ephemerally in RAM zeroised post programming in HW cipher.	Manually by the operator, on demand
Factory Reset	Resets the module to factory default state	Zeroises SSPs (overwritten with random values) and replaces them with new SSPs	Manually by the operator, on demand

Table 17: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Hardware Unique Key (HUK)	Used to derive secondary Keys (HYDRA_KDK)	256 bits - 256 bits	Keyed hash key - CSP			HMAC-SHA2-256 (A3379)
HYDRA_KDK	Used to derive BLOB_KEY	256 bits - 256 bits	Symmetric key - CSP	KDA TwoStep Sp800-56Cr1 (A3379)		AES-GCM (A3379) KDA TwoStep Sp800-56Cr1 (A3379)
BLOB_KEY	Used for decrypting the iDevID private key (IDEVID)	256 bits - 256 bits	Symmetric key - CSP	KDA TwoStep Sp800-56Cr1 (A3379)		AES-GCM (A3379)
DRBG Seed	Used for random number generation; Considered a CSP in accordance with IG D.L Resolution	384 bits - 384 bits	DRBG Seed - CSP	Counter DRBG (A3379)		Counter DRBG (A3379)
DRBG V	Used for random number generation; Considered a CSP in accordance with IG D.L Resolution 3.	256 bits - 256 bits	DRBG State Value - CSP	Counter DRBG (A3379)		Counter DRBG (A3379)
DRBG Key	Used for random number generation; Considered a CSP in accordance with IG D.L Resolution 3.	256 bits - 256 bits	DRBG State Value - CSP	Counter DRBG (A3379)		Counter DRBG (A3379)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Entropy Input	Used for seeding the NIST SP 800-90Ar1 DRBG; Considered a CSP in accordance with IG D.L Resolution	384 bits - 384 bits	Entropy Input - CSP	Entropy Source		Counter DRBG (A3379)
Datapath Customer Enrolled Preshared key (PSK)	Used to derive the DPE- PSK and TLS- PSK	256 bits (32 bytes) - 256 bits	Pre-shared key - CSP			ECDSA SigGen (FIPS186-4) (A3379) KDA TwoStep Sp800-56Cr1 (A3379)
Datapath Customer Enrolled Certificate	Used for remote device TLS 1.3 connection	P-521 - 256 bits	Certificate - PSP			ECDSA SigVer (FIPS186-4) (A3379)
Datapath pre shared key (DPE-PSK)	Used during the datapath key agreement	P-521 - 256 bits	Pre-shared key - CSP	KDA TwoStep Sp800-56Cr1 (A3379)		ECDSA SigGen (FIPS186-4) (A3379)
TLS 1.3 pre shared key (TLS- PSK)	Used during the TLS 1.3 handshake	P-521 - 256 bits	Pre-shared key - CSP	KDA TwoStep Sp800-56Cr1 (A3379)		ECDSA SigGen (FIPS186-4) (A3379)
IDEVID public key	Default Authentication material for CO using TLS 1.3	P-521 - 256 bits	Public key - PSP			ECDSA SigVer (FIPS186-4) (A3379)
IDEVID private key	Default authentication material for CO using TLS 1.3	P-521 - 256 bits	Private key - CSP			ECDSA SigGen (FIPS186-4) (A3379)
COID Public	Used for CO to module	P-521 - 256 bits	Public key - PSP			ECDSA SigVer

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	authentication using TLS 1.3					(FIPS186-4) (A3379)
Logical Device ID Public Key	Used for CO to module authentication using TLS 1.3	P-521 - 256 bits	Public key - PSP	Counter DRBG (A3379) ECDSA KeyGen (FIPS186-4) (A3379)		ECDSA KeyGen (FIPS186-4) (A3379)
Logical Device ID Private Key	Used for CO to module authentication using TLS 1.3	P-521 - 256 bits	Private key - CSP	Counter DRBG (A3379) ECDSA KeyGen (FIPS186-4) (A3379)		ECDSA KeyGen (FIPS186-4) (A3379)
TLS 1.3 Pre-Master Secret	Establish the TLS Master Secret	256 bits - 256 bits	TLS Pre-Master Secret - CSP		KAS-1	TLS v1.3 KDF (A3379)
TLS 1.3 Master Secret	Establish the TLS Session and authentication key	256 bits - 256 bits	TLS Master Secret - CSP	TLS v1.3 KDF (A3379)		TLS v1.3 KDF (A3379)
TLS 1.3 Authentication Key	Used for authenticating TLS communication	384 bits - 384 bits	Keyed Hash Key - CSP	TLS v1.3 KDF (A3379)		HMAC-SHA2-384 (A3379)
TLS Session Key	Used for encrypting the TLS communication	256 bits - 256 bits	Symmetric key - CSP	TLS v1.3 KDF (A3379)		AES-GCM (A3379)
DPE_ECDH Public Key	Used for exchanging shared secret to derive session keys during key agreement	P-384, P-521 - 192, 256 bits	Public key - PSP	Counter DRBG (A3379) ECDSA KeyGen (FIPS186-4) (A3379)		KAS-ECC-SSC Sp800-56Ar3 (A3379)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DPE_ECDH Private Key	Used for exchanging shared secret to derive session keys during key agreement	P-384, P-521 - 192, 256 bits	Private key - CSP	Counter DRBG (A3379) ECDSA KeyGen (FIPS186-4) (A3379)		KAS-ECC-SSC Sp800-56Ar3 (A3379)
DPE "Z" Value	Shared secret resulting from the ECDHE exchange between peers	P-384, P-521 - 192, 256 bits	Shared Secret - CSP		KAS-1	TLS v1.3 KDF (A3379)
DPE Mac Key	Used to authenticate key agreement messages	P-384, P-521 - 192, 256 bits	Asymmetric Key - CSP	KDA TwoStep Sp800-56Cr1 (A3379)		KAS-ECC-SSC Sp800-56Ar3 (A3379)
DPE_KDK	Master key derivation key used to derive the datapath cipher keys and IVs	P-384, P-521 - 192, 256 bits	Key Derivation Key (Asymmetric Key) - CSP	KDA TwoStep Sp800-56Cr1 (A3379)		KAS-ECC-SSC Sp800-56Ar3 (A3379)
Datapath Cipher Encrypt/Decrypt keys (x16) (DDEK/DDDK)	Used for encryption and decryption of the datapath	256 bits - 256 bits	Symmetric key - CSP	KDF SP800-108 (A3379)		AES-GCM (A3379)
VAULT_PUBLIC	Used to authenticate the Vault firmware image	P-256 - 128 bits	Public Key - Neither			
BOOT_PUB	Used to authenticate boot image	P-521 - 256 bits	Public Key - Neither			
FIT_PUBLIC	Used to authenticate the Linux kernel	P-521 - 256 bits	Public Key - Neither			

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ROOTFS_PUB	Used to authenticate the ROOTFS of the SW load	P-521 - 256 bits	Public Key - Neither			
LOAD_KEY	Used for the load check during upgrades	P-521 - 256 bits	Public Key - Neither			

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Hardware Unique Key (HUK)	Pre-loaded at the factory and never exits the module (eFUSE)	eFUSE:Plaintext		Factory Reset	HYDRA_KDK :Used to derive
HYDRA_KDK		RAM:Plaintext	While in use	Zeroise after use	Hardware Unique Key (HUK) :Derived From BLOB_KEY:Used to derive
BLOB_KEY		RAM:Plaintext	While in use	Zeroise after use	IDEVID private key:Decrypts HYDRA_KDK :Derived From
DRBG Seed		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	Entropy Input :Derived From
DRBG V		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	DRBG Key :Used With
DRBG Key		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	DRBG V :Used With
Entropy Input		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	DRBG Seed :Used to derive

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Datapath Customer Enrolled Preshared key (PSK)	Imported via TLS 1.3 and never exits the module (RAM)	RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	Datapath pre shared key (DPE-PSK):Used to derive TLS 1.3 pre shared key (TLS-PSK):Used to derive
Datapath Customer Enrolled Certificate	Imported via TLS 1.3 and never exits the module (RAM)	RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	
Datapath pre shared key (DPE-PSK)		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	Datapath Customer Enrolled Preshared key (PSK) :Derived From
TLS 1.3 pre shared key (TLS- PSK)		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	Datapath Customer Enrolled Preshared key (PSK) :Derived From
IDEVID public key	Loaded at the factory (NVM)	NVM (Encrypted) :Encrypted		Factory Reset	IDEVID private key:Paired With
IDEVID private key	Loaded at the factory (NVM)	NVM (Encrypted) :Encrypted		Factory Reset	IDEVID public key:Paired With
COID Public	Imported via TLS 1.3 and never exits the module (RAM)	RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	
Logical Device ID Public Key	Exits in plaintext (RAM)	RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	Logical Device ID Private Key :Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Logical Device ID Private Key		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal	Logical Device ID Public Key :Paired With
TLS 1.3 Pre-Master Secret		RAM:Plaintext	Until reboot, power removal or session termination	Reboot or Power Removal Session Termination	TLS 1.3 Master Secret:Used to derive
TLS 1.3 Master Secret		RAM:Plaintext	Until reboot, power removal or session termination	Reboot or Power Removal Session Termination	TLS 1.3 Pre-Master Secret :Derived From TLS 1.3 Authentication Key:Used to derive TLS Session Key:Used to derive
TLS 1.3 Authentication Key		RAM:Plaintext	Until reboot, power removal or session termination	Reboot or Power Removal Session Termination	TLS 1.3 Master Secret:Derived From
TLS Session Key		RAM:Plaintext	Until reboot, power removal or session termination	Reboot or Power Removal Session Termination	TLS 1.3 Master Secret:Derived From
DPE_ECDH Public Key	For the public component of the module: exits the module in plaintext (RAM)	RAM:Plaintext	Until reboot, power removal or session termination	Reboot or Power Removal Session Termination	DPE_ECDH Private Key :Paired With
DPE_ECDH Private Key		RAM:Plaintext	Until reboot, power removal	Reboot or Power Removal	DPE_ECDH Public Key :Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			or session termination	Session Termination	
DPE "Z" Value		RAM:Plaintext	Until reboot, power removal or session termination	Reboot or Power Removal Zeroise after use	DPE_ECDH Public Key :Derived From DPE_ECDH Private Key :Derived From
DPE Mac Key		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal post programming into HW cipher	
DPE_KDK		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal post programming into HW cipher	
Datapath Cipher Encrypt/Decrypt keys (x16) (DDEK/DD DK)		RAM:Plaintext	Until reboot or power removal	Reboot or Power Removal post programming into HW cipher	DPE_KDK :Derived From
VAULT_PUBLIC	Loaded at the factory (NVM)	NVM:Plaintext		N/A	
BOOT_PUB	Loaded at the factory (NVM)	NVM:Plaintext		N/A	
FIT_PUBLIC	Loaded at the factory (NVM)	NVM:Plaintext		N/A	
ROOTFS_PUB	Loaded at the factory (NVM)	NVM:Plaintext		N/A	
LOAD_KEY	Loaded at the factory (NVM)	NVM:Plaintext		N/A	

Table 19: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
ECDSA SigVer (FIPS186-4) (A3379)	Verify	KAT	SW/FW Integrity	Global Approved mode indicator (show status indicator)	ECDSA P-521 with SHA2-512 signature verification

Table 20: Pre-Operational Self-Tests

ISO/IEC 19790 requires the module to perform pre-operational self-tests to ensure the module integrity and the correctness of the cryptographic functionality at start-up. The algorithms supported by the module require cryptographic self-tests and these tests are run when the module is in operational state prior to the first use of algorithm. Some functions also require conditional tests during normal operation of the module. The pre-operational firmware integrity test (using ECDSA P-521 SHA2-512) can be run on demand by reloading the module.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A3379) - Encrypt - 128-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	128-bit KAT	Automatically on boot, manually on demand
AES-CBC (A3379) - Decrypt - 128-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	128-bit KAT	Automatically on boot, manually on demand
AES-GCM (A3379) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Automatically on boot, manually on demand
AES-GCM (A3379) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved	256-bit KAT	Automatically on boot,

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				d mode indicator (show status indicator)		manually on demand
SHA2-256 (A3379)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit KAT	Automatically on boot, manually on demand
SHA2-384 (A3379)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	384-bit KAT	Automatically on boot, manually on demand
SHA2-512 (A3379)	Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	512-bit KAT	Automatically on boot, manually on demand
HMAC-SHA2-256 (A3379)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-256 KAT	Automatically on boot, manually on demand
HMAC-SHA2-384 (A3379)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-384 KAT	Automatically on boot, manually on demand
HMAC-SHA2-512 (A3379)	Keyed-Hash	KAT	CAST	Global Approved mode indicator (show status indicator)	SHA2-512 KAT	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Counter DRBG (A3379)	NIST SP 800-90Ar1 Section 11 Health Checks	KAT	CAST	Global Approved mode indicator (show status indicator)	256-bit CTR DRBG KAT	Automatically on boot, manually on demand
KAS-ECC-SSC Sp800-56Ar3 (A3379)	SP800-56Arev3 KAS-ECC-SSC	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-521	Automatically on boot, manually on demand
ECDSA SigVer (FIPS186-4) (A3379)	ECDSA P-521 Verify KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-521	Automatically on boot, manually on demand
ECDSA SigGen (FIPS186-4) (A3379)	ECDSA P-521 Sign KAT	KAT	CAST	Global Approved mode indicator (show status indicator)	Curve used: P-521	Automatically on boot, manually on demand
KDF SP800-108 (A3379)	KDF NIST SP 800-108	KAT	CAST	Global Approved mode indicator (show status indicator)	HMAC SHA2-256	Automatically on boot, manually on demand
KDA TwoStep Sp800-56Cr1 (A3379)	Two Step KDA	KAT	CAST	Global Approved mode indicator (show status indicator)	Two Step KDA	Automatically on boot, manually on demand
TLS v1.3 KDF (A3379)	TLS v1.3 KDF	KAT	CAST	Global Approved mode indicator (show	-	Automatically on boot, manually on demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				status indicator)		
AES-GCM (A3305) - Encrypt - 256-bit	Encrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256 bits	Automatically on boot, manually on demand
AES-GCM (A3305) - Decrypt - 256-bit	Decrypt	KAT	CAST	Global Approved mode indicator (show status indicator)	256 bits	Automatically on boot, manually on demand
NIST SP 800-90B Entropy Source Repetition Count Test	-	-	CAST	Global Approved mode indicator (show status indicator)	-	Automatically on boot and continuously, manually on demand
NIST SP 800-90B Entropy Source Adaptive Proportion Test	-	-	CAST	Global Approved mode indicator (show status indicator)	-	Automatically on boot and continuously, manually on demand
ECDSA keys generated for signature generation/verification and ECDSA keys used for key agreement	Key Agreement	PCT	PCT	Global Approved mode indicator (show status indicator)	Curve used: P-521	Automatically on boot, manually on demand
Conditional Firmware Load test	ECDSA P-521 SHA2-512 signature verification	-	SW/FW Load	Global Approved mode indicator (show status indicator)	Curve used: P-521	Automatically on boot, manually on demand
NIST SP 800-90B Developer Defined Test	. Stopping of one or more FROs	-	CAST	Global Approved mode	-	Automatically on boot and

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	will deteriorate the noise source's performance but this may not be detected by the RCT or APT. Therefore, each FRO has a lock detector to monitor correct operation of the FRO and issue an alarm when this is not the case.			indicator (show status indicator)		continuously, manually on demand

Table 21: Conditional Self-Tests

The CAST for the cryptographic algorithms used to perform the Approved integrity technique, ECDSA P521 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.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA SigVer (FIPS186-4) (A3379)	KAT	SW/FW Integrity	On every boot and on demand (Power-cycling)	Programmatically and Manually (on demand)

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3379) - Encrypt - 128-bit	KAT	CAST	On demand	Manually via reboot/power-cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A3379) - Decrypt - 128-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-GCM (A3379) - Encrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-GCM (A3379) - Decrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA2-256 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA2-384 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
SHA2-512 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA2-256 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA2-384 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
HMAC-SHA2-512 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
Counter DRBG (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
KAS-ECC-SSC Sp800-56Ar3 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
ECDSA SigVer (FIPS186-4) (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
ECDSA SigGen (FIPS186-4) (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
KDF SP800-108 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
KDA TwoStep Sp800-56Cr1 (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle
TLS v1.3 KDF (A3379)	KAT	CAST	On demand	Manually via reboot/power-cycle

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-GCM (A3305) - Encrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
AES-GCM (A3305) - Decrypt - 256-bit	KAT	CAST	On demand	Manually via reboot/power-cycle
NIST SP 800-90B Entropy Source Repetition Count Test	-	CAST	On demand	Manually via reboot/power-cycle
NIST SP 800-90B Entropy Source Adaptive Proportion Test	-	CAST	On demand	Manually via reboot/power-cycle
ECDSA keys generated for signature generation/verification and ECDSA keys used for key agreement	PCT	PCT	On demand	Manually via reboot/power-cycle
Conditional Firmware Load test	-	SW/FW Load	On demand	Manually via reboot/power-cycle
NIST SP 800-90B Developer Defined Test	-	CAST	On demand	Manually via reboot/power-cycle

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Soft Error	Upon failure of the firmware load test, the module enters "Soft Error" state. The soft error state is a nonpersistent state wherein the module resolves the error by rejecting the loading of the new firmware. Upon rejection, the error state 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	Failure of Firmware load test or conditional self-tests	Re-executing the test	Global Approved mode indicator (show status indicator)

Name	Description	Conditions	Recovery Method	Indicator
	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.			
Critical Error	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.	Failure of pre-operational self-tests or Cryptographic Algorithm Self-tests	Re-executing the test	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.

Table 24: Error States

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.

All data and control output via the data/control output interface is inhibited whenever the module is in an error state. If the error condition is not cleared, then the module is considered to be malfunctioning and should be returned to Ciena.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module only runs in an Approved mode of operation. The CO can monitor and configure the module via the TLS 1.3 management channel from the Ciena Control Module.

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 (validated) module, the Control Processor.

11.2 Administrator Guidance

Detailed instructions for monitoring and troubleshooting the module are provided in the Ciena's User's Guide and Technical Practices document.

11.3 Non-Administrator Guidance

Detailed instructions for monitoring and troubleshooting the module are provided in the Ciena's User's Guide and Technical Practices document.

11.4 Maintenance Requirements No maintenance requirements other than those defined for the Physical Security maintenance in Section 7 of this document apply.

11.4 End of Life

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.

11.5 Additional Information

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

12 Mitigation of Other Attacks

12.1 Attack List

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