Ciena 3926 Platform

FIPS 140-2 Level 2
Non-Proprietary Security Policy

Document Version Number: 1.2

Table of Contents

1. Module Overview

The Product is Ciena 3926 Service Access and Aggregation Platform. It uses MACSec for traffic encryption/decryption. It provides routing/switching functionalities for various use cases including enterprise, mobility, and converged network architectures.

The module is a Multi-Chip Standalone module. FIPS 140-2 conformance testing was performed at Security Level 2. The following configurations were tested by the lab.

Table 1: Configurations tested by the lab.

Module Name and Version	Firmware version
Ciena 3926 Platform	Ciena Service Aware Operating System (SAOS 10.7.0)

The Cryptographic Module meets FIPS 140-2 Level 2 requirements.

Table 2: Module Security Level Statement.

FIPS Security Area	Security Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

The cryptographic boundary of the module is the enclosure that contains components of the module. The enclosure of the cryptographic module is opaque within the visible spectrum. The module uses tamper evident labels to provide the evidence of tampering.

Figure 1: Ciena 3926 Platform

The module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

2. Modes of Operation

The module is intended to always operate in the FIPS approved mode.

The Crypto Officer must invoke the user interface using default password. Crypto Officer must change the default password during the installation.

Configuring any of the following features disables the FIPS mode:

- SNMP
- FTP or HTTP for file transfers
- Disabling firmware signing for firmware updates
- TLS version 1.0 and 1.1

2.1 Approved Cryptographic Functions

The following approved cryptographic algorithms are used in FIPS approved mode of operation.

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
AES 4550	AES Library	AES	FIPS 197, SP 800-38D	ECB, CTR, GCM[1]	128, 256	Data Encryption/ Decryption;

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A2492	Ciena Cryptographic library for 3926	AES	FIPS 197, SP 800-38B, SP 800-38D	ECB, CBC, CMAC, CTR, GCM[1]	128, 192, 256	Data Encryption/ Decryption; Generation/ Verification (CMAC) KTS[4]
A2492	Ciena Cryptographic library for 3926	HMAC	FIPS 198-1	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	160, 256, 384, 512	Message Authentication KTS[4]
A2492	Ciena Cryptographic library for 3926	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384 SHA-512		Message Digest
A2492	Ciena Cryptographic library for 3926	DRBG	SP 800-90A	CTR_DRBG	128, 192, 256	Deterministic Random Bit Generation[3]
A2492	Ciena Cryptographic library for 3926	ECDSA	FIPS 186-4		PP-256, P-384, P-521	Digital Signature Generation and Verification, Key Generation and Key Verification
A2492	Ciena Cryptographic library for 3926	RSA	FIPS 186-4	SHA-1 [SigVer only], SHA-224, SHA-256, SHA-384, SHA-512 ANSIX9.31, PKCS1 v1.5, PSS	2048, 3072	Key Generation Digital Signature Generation and Verification
A2492	Ciena Cryptographic library for 3926	KAS-ECC-SSC	SP800-56Ar3	ECC Ephemeral Unified Scheme	P-256,P-384, P-521 corresponds to 128 to 256 bits of security	TLS, SSH Shared Secret Computation

CAVP Cert	Library	Algorithm	Standard	Model/ Method	Key Lengths, Curves or Moduli	Use
A2492	Ciena Cryptographic library for 3926	KAS	SP800-56Ar3 and SP800-135	ECC Ephemeral Unified Scheme	P-256,P-384, P-521	TLS, SSH Shared Secret Computation TLS, SSH Key Derivation
A2492	Ciena Cryptographic library for 3926	CVL SSH, TLS 1.2	SP 800-135			Key Derivation[2]
A2492	Ciena Cryptographic library for 3926	KBKDF	SP 800-108	CMAC-AES128, CMAC-AES256		Key Derivation
CKG (vendor affirmed)	Ciena Cryptographic library for 3926	Cryptographic Key Generation	SP 800-133			Key Generation[3]

Table 3: Approved Cryptographic Functions

Note 1: not all CAVS tested modes of the algorithms are used in this module.

Note 2: any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

[1]The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288. AES-GCM is only used in TLS version 1.2 and MACsec. The module's AES-GCM implementation complies with IG A.5 scenario 1 and RFC 5288, and supports acceptable GCM cipher suites from Section 3.3.1 of SP 800-52 Rev 1 or SP 800-52 Rev 2. AES-GCM is only used in TLS version 1.2. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, that encounters this condition will trigger a handshake to establish a new encryption key. New AES-GCM keys are generated by the module if the module loses power.

[2]No parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

[3]CKG is only used to generate asymmetric keys. The module directly uses the output of the DRBG. Section 4, example 1, of SP800-133r2 "Using the Output of a Random Bit Generator" is applicable.

The module takes on the role of Peer in the MACsec protocol. The AES GCM IV construction is performed in compliance with IEEE 802.1AE and its amendments.

The link between the Peer and Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network.

When supporting the MACsec protocol in the approved mode, the module should only be used together with the CMVP-validated modules providing the remaining MACsec functionalities.

[4] KTS: KTS (AES Cert. #A2492 and HMAC Cert. #A2492; key establishment methodology provides 128 or 256 bits of encryption strength)

2.2 Non-Approved and non-Allowed algorithms

Table 4: Non-Approved and non-Allowed algorithms

Algorithm	Use
MD5	SSH, TLS
Chacha20-poly1305	SSH
DES and 3DES	SSH, TLS
Curve25519	SSH
DH	SSH, TLS
HMAC-MD5	SSH
ED25519	SSH
RSA keys < 1024	TLS, CSR
RC4	TLS
DSA	CSR

3. Ports and interfaces

The following table describes physical ports and logical interfaces of the module.

Ports and Interfaces of Ciena 3926 Platform

Port Name	Count	Interface(s)
Ethernet Ports 1-2	2	2 SFP ports of 1 GbE/100 MbE using standard SFP modules. Data Input, Data Output, Control Input, Status Output. 2 LEDS status/activity and speed

Port Name	Count	Interface(s)
Ethernet Ports 3-8	6	6 SFP+ ports of 10/1 GbE using standard SFP+ modules. Data Input, Data Output, Control Input, Status Output. Port 7-8 are the MACSec ports. 2 LEDS status/activity and speed
CONSOLE	1	Serial EIA-561 (RJ45) port. Management port
MGMT	1	RJ45 10/100/100 MbE. Management port. 2 LEDs for status and speed
CLK	1	1 Mini coax (10 MHz/1544 kHz/2048 kHz) frequency SMB Port in or out (SW selectable
1PPS	1	1 Mini coax one pulse per second phase clock SMB interface in or out (SW selectable)
BITS	1	1 RJ48C BITS (E1/T1/2048 kHz), in or out. 2 LEDs for BITS in and out
SYNC	1	1 RJ45 ITU-T G.703 1PPS in or out, ToD in or out (SW selectable)
USB Ports	1	Not used
Power Port	2	Power Input. AC or DC power modules. No power switch. 2 LEDs for input and output status
LEDs	5	Status information for status, alarms, power and sync

4. Roles, Services and Authentication

The module supports role-based authentication. The module supports a Crypto Officer role and a User Role. The Crypto Officer installs and administers the module. The Users use the cryptographic services provided by the module. The module supports concurrent operators. The module provides the following services.

Table 5: Roles and Services

Service	Corresponding Roles	Types of Access to Cryptographic Keys and CSPs R – Read E - Execute W – Write or Create Z – Zeroize
Run Self-test	Crypto Officer	N/A
Reboot	Crypto Officer	N/A
Zeroize	Crypto Officer	All: Z
Firmware update	Crypto Officer	Firmware update RSA public key: R, E
Show status	Crypto Officer User	SSH Keys: R,W,E DRBG CSPs: R,W
SSH Login	Crypto Officer	Password: R, W SSH Keys: R,W, E DRBG CSPs: R, W
TLS Tunnel	Crypto Officer	TLS Keys: R,W,E DRBG CSPs: R, W
Configuration	Crypto Officer	Password: R, W SSH Keys: R,W, E TLS RSA Keys: R,W
MACSec Tunnel	User	MACSec AES Keys: R,W,E

Note:

TLS Keys means: TLS master secret, TLS pre-master secret, TLS AES key, TLS HMAC key, TLS RSA public and private keys, TLS ECC Diffie-Hellman SP800-56Ar3 public and private keys.

SSH Keys means: SSH AES key, SSH HMAC key, SSH ECDSA public and private keys, SSH ECC Diffie-Hellman SP800-56Ar3 public and private keys.

The module supports the following authentication mechanisms.

Table 6: Authentication Mechanisms

Roles	Authentication Mechanisms
CO Role / User	Passwords (Minimum 8 characters) The module can be configured to use passwords of at least 8 printable characters. Total number of password permutations with eight characters is 94^8 = 6.095e+15. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The system is configured to lockout policy of fail-limit=3 and lockout-time=60sec only 3 password attempts per minute are allowed by the module. The likelihood of success after one minute is well below one in 100,000. RSA/ECDSA key (at least 112 bits of security bits) 2^-112 is significantly less than 1/1,000,000. Therefore the probability is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur. The system is configured to lockout policy of fail-limit=3 and lockout-time=60sec only 3 password attempts per minute are allowed by the module. The likelihood of success after one minute is well below one in 100,000

5. Cryptographic Keys and CSPs

The table below describes cryptographic keys and CSPs used by the module.

Table 7: Cryptographic Keys and CSPs

Key	Description/Usage	Storage
TLS master secret Established using KDF TLS	Used to derive TLS encryption key and TLS HMAC Key	RAM in plaintext
TLS pre-master secret Established using KAS-ECC-SSC	Used to derive TLS master secret	RAM in plaintext
TLS AES key Established using KDF TLS	Used during encryption and decryption of data within the TLS protocol	RAM in plaintext
TLS HMAC key Established using KDF TLS	Used to protect integrity of data within the TLS protocol	RAM in plaintext
TLS RSA public and private keys Established using DRBG or set by operators	Used during the TLS handshake	RAM in plaintext Hard drive in plaintext
TLS ECC Diffie-Hellman SP800-56Ar3 public and private keys Established using DRBG	Used during the TLS handshake to establish the shared secret	RAM in plaintext
CTR_DRBG CSPs: entropy input, V and Key Entropy is loaded externally	Used during generation of random numbers	RAM in plaintext
Passwords Set by operators	Used for operator authentication	RAM in plaintext Hard drive (SHA512)
Firmware update RSA public key Set at the factory	Used to protect integrity during firmware update	RAM in plaintext Hard drive in plaintext

Key	Description/Usage	Storage
SSH AES key Established using KDF SSH	Used during encryption and decryption of data within the SSH protocol	RAM in plaintext
SSH HMAC key Established using KDF SSH	Used to protect integrity of data within the SSH protocol	RAM in plaintext
SSH ECDSA public and private keys Established using DRBG or set by operators	Used to authenticate the SSH handshake	RAM in plaintext Hard drive in plaintext
SSH ECC Diffie-Hellman SP800-56Ar3 public and private keys Established using DRBG	Used during the SSH handshake to establish the shared secret	RAM in plaintext
MACsec AES keys Established using KBKDF	Used during encryption and decryption of data within the MACsec protocol	RAM in plaintext

Note 1: public keys are not considered CSPs

Note 2: All keys, that are generated by this module, are generated by using DRBG. Entropy is loaded externally. Minimum number of bits of entropy loaded is 256-bits, since the minimum length of the entropy field is at least 256-bits.

Note 3: Keys can be entered into and output from the module via an SSH or HTTPS connection.

6. Self-tests

The module performs the following power-up and conditional self-tests. Upon failure or a power-up or conditional self-test the module halts its operation.

The following table describes self-tests implemented by the module.

Table 8: Self-Tests

Algorithm	Power up Test
AES	KAT using ECB, CBC, GCM and CTR modes (encryption/decryption)
SHS	KAT using SHA1, SHA224, SHA256, SHA384, and SHA512
HMAC	HMAC 256 integrity test and KAT using SHA1, SHA224, SHA256, SHA384 and SHA512
KAS (ECC-SSC)	KAT per implementation guidance
SP800-90A DRBG	KAT: CTR_DRBG HASH_DRBG HMAC_DRBG
RSA	KAT using 2048 bit key, SHA-256
Firmware integrity	SHA1 and SHA256 upon startup
ECDSA	Pairwise Consistency Test (sign/verify) using P-224, K-233 and SHA512
KBKDF	KAT
TLS 1.2 KDF	KAT
SSH KDF	KAT
	Conditional Test
SP800-90A DRBG	Continuous Random Number Generator test
	DRBG health tests
RSA	Pairwise consistency test on generation of a key pair
Firmware load	RSA with SHA256 using 2048 bit key
ECDSA	Pairwise consistency test on generation of a key pair
KAS (ECC-SSC)	Private/Public Key Validation tests as per SP800-56Ar3

7. Physical Security

The cryptographic module consists of production-grade components. The enclosure of the cryptographic module is opaque within the visible spectrum. The removable covers are protected with tamper-evident seals. The tamper evident labels are applied at the factory to provide evidence of tampering if a panel is removed. The Crypto Officer must note the locations of the tamper evidence labels upon receipt of the module. The Crypto Officer must check the integrity of the tamper evident labels periodically thereafter. If the tamper-evident seals are broken or missing, the Crypto Officer must halt the operation of the module.

8. References

Table 9: References

Reference	Specification
[ANS X9.31]	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
[FIPS 140-2]	Security Requirements for Cryptographic modules, May 25, 2001
[FIPS 180-4]	Secure Hash Standard (SHS)
[FIPS 186-2/4]	Digital Signature Standard
[FIPS 197]	Advanced Encryption Standard
[FIPS 198-1]	The Keyed-Hash Message Authentication Code (HMAC)
[FIPS 202]	SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
[PKCS#1 v2.1]	RSA Cryptography Standard
[PKCS#5]	Password-Based Cryptography Standard
[PKCS#12]	Personal Information Exchange Syntax Standard
[SP 800-38A]	Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
[SP 800-38B]	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication

Reference	Specification
[SP 800-38C]	Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
[SP 800-38D]	Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
[SP 800-38F]	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
[SP 800-56A]	Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
[SP 800-56B]	Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
[SP 800-56C]	Recommendation for Key Derivation through Extraction-then-Expansion
[SP 800-67R1]	Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
[SP 800-89]	Recommendation for Obtaining Assurances for Digital Signature Applications
[SP 800-90A]	Recommendation for Random Number Generation Using Deterministic Random Bit Generators
[SP 800-108]	Recommendation for Key Derivation Using Pseudorandom Functions
[SP 800-132]	Recommendation for Password-Based Key Derivation
[SP 800-135]	Recommendation for Existing Application –Specific Key Derivation Functions