Arista Networks Inc.

EOS MACsec Alpha Hybrid Module

Non-Proprietary FIPS 140-2 Security Policy

Document Version: v1.4

Date: April 4, 2019

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Security Policy for the Arista Networks Inc. EOS MACsec Alpha Hybrid Module, hereafter denoted the Module. The Module is a hybrid firmware/hardware means of performing secure encryption, hashing, and RNG operations. The firmware portion is intended to provide a flexible means of performing arbitrary cryptographic operations while the disjoint hardware portion is capable of performing accelerated cryptographic functions for MACsec operations at line rate speeds. The Module is intended for use by US Federal agencies or other markets that require FIPS 140-2 validated Firmware Hybrid Modules.

Table 1 – Firmware Hybrid Cryptographic Module Components

Component	Description	Type	Version # / PN
EOS MACsec Alpha	LibSSL and LibCrypto libraries and OpenSSH daemon	Firmware	1.0
MACsec Chip	Broadcom cryptographic accelerator for MACsec	Hardware	BCM82391
Security Chip	Renesas security chip for entropy source and TRNG	Hardware	R5H30211 or N313X

1.1 Module Description and Cryptographic Boundary

The Module is a multi-chip standalone firmware-hybrid cryptographic module. The logical cryptographic boundary in Figure 1 surrounds the Arista Networks firmware and hardware consisting of the MACsec chip (Broadcom cryptographic accelerator for MACsec) and the Security chip (Renesas security chip for entropy source and TRNG).

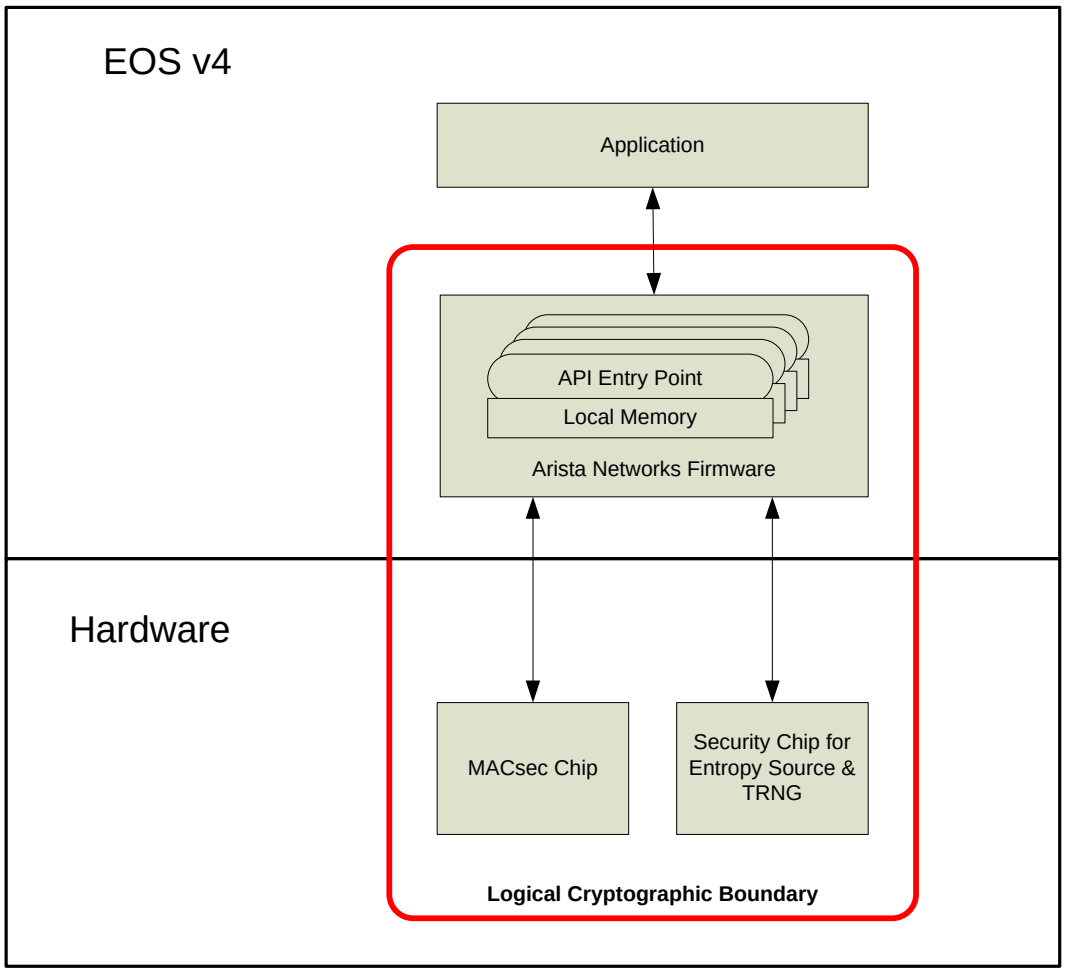

Figure 1 – Logical Cryptographic Boundary

The operational environment is non-modifiable firmware that runs on the hardware configurations as shown in Table 2 and Table 3 below.

Table 2 – Modular Chassis Hardware Configurations

Hardware	Type	Processor	Hardware Version #	Firmware Version #
DCS-7508N	Chassis	N/A	06.00	N/A
DCS-7512N	Chassis	N/A	00.06	N/A
DCS-7516N	Chassis	N/A	10.00	N/A
DCS-7500E-SUP	Supervisor	Intel “Sandy Bridge” Xeon E3	01.02	1.0
DCS-7500-SUP2	Supervisor	Intel “Broadwell-DE” Xeon D-1500	03.03	1.0
DCS-7516-SUP2	Supervisor	Intel “Broadwell-DE” Xeon D-1500	10.00	1.0

DCS-7500RM-36CQ-LC	MACsec linecard	BCM82391	11.01 (in DCS-7512N) 10.02 (in DCS-7512N) 10.01 (in DCS-7508N)	N/A
DCS-7500R-8CFPX-LC	MACsec linecard	BCM82391	11.02	N/A

The module is also capable of running on the Arista Networks 7050CX3M-32S platform and is vendor affirmed to behave in the same manner. Also, the module is capable of running in the DCS-7504N chassis (hardware v1.0) and is vendor affirmed to behave in the same manner. The module was not tested in these hardware configurations. As this has only been affirmed by the vendor, the CMVP itself does not provide assurances to the correct operation of the module or the strength of generated keys.

The following optional linecards are not security relevant, do not perform any security related services nor do they process any CSPs and are outside the scope of the FIPS 140-2 validation.

Table 3 – Optional Linecards which are not security relevant

Linecard
DCS-7500R-36Q
DCS-7500R-48S2CQ
DCS-7500R2A-36CQ
DCS-7500R2-36CQ
DCS-7500R2-18CQ
DCS-7500R2AK-48YCQ

Images of the hardware used in operational testing appear in the figures below.

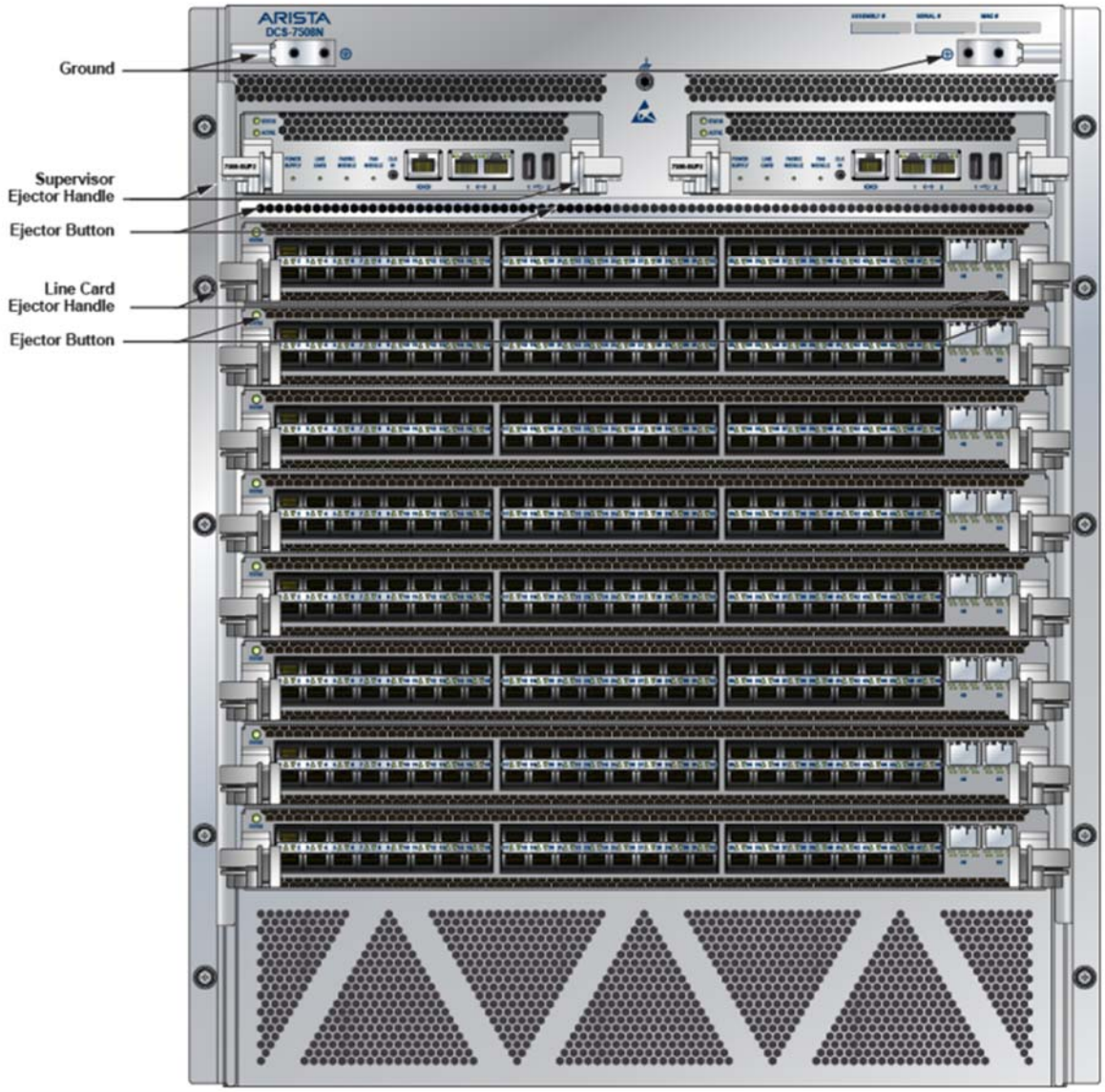

Figure 2 - DCS-7508N Front

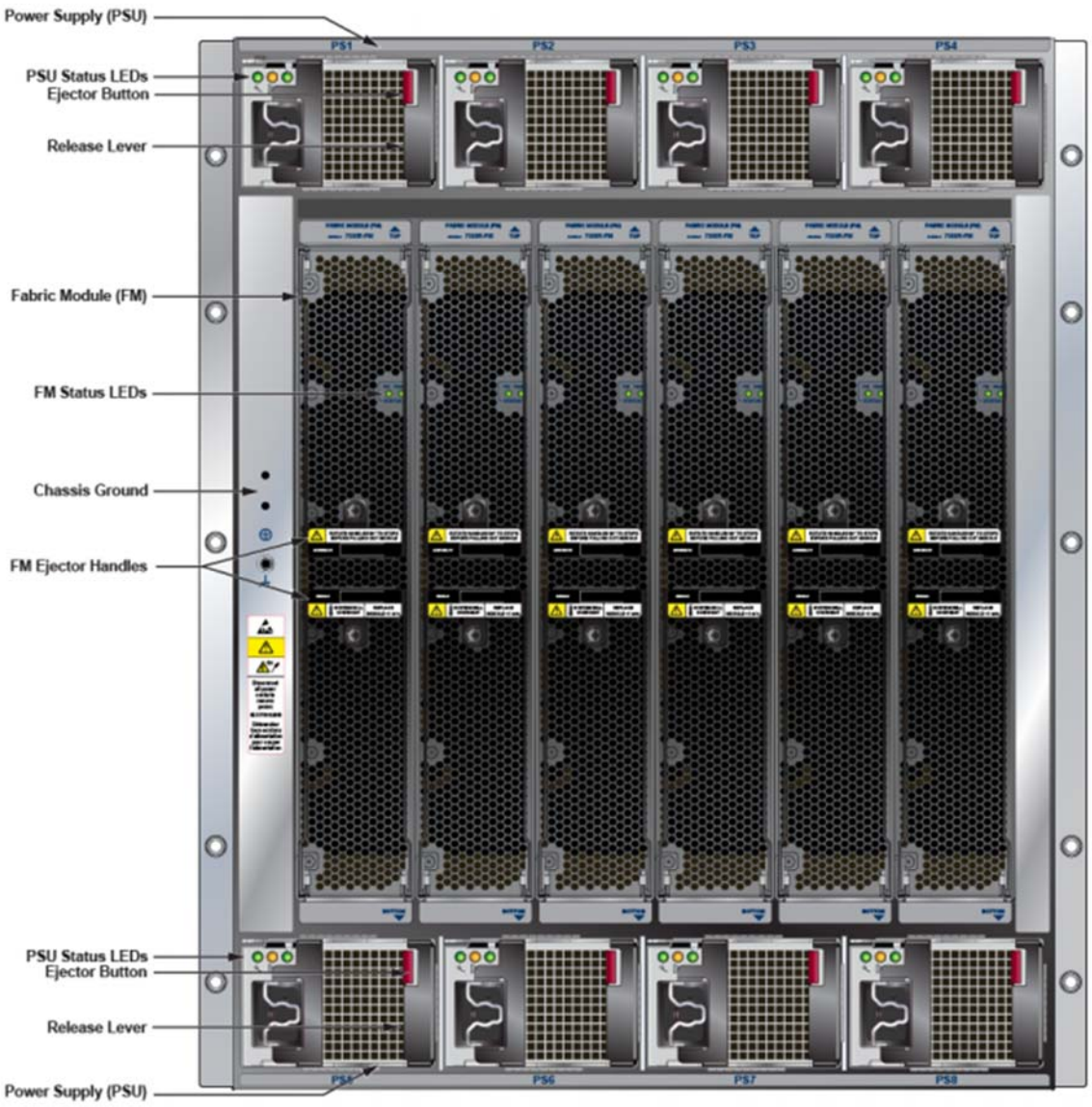

Figure 3 - DCS-7508N Rear

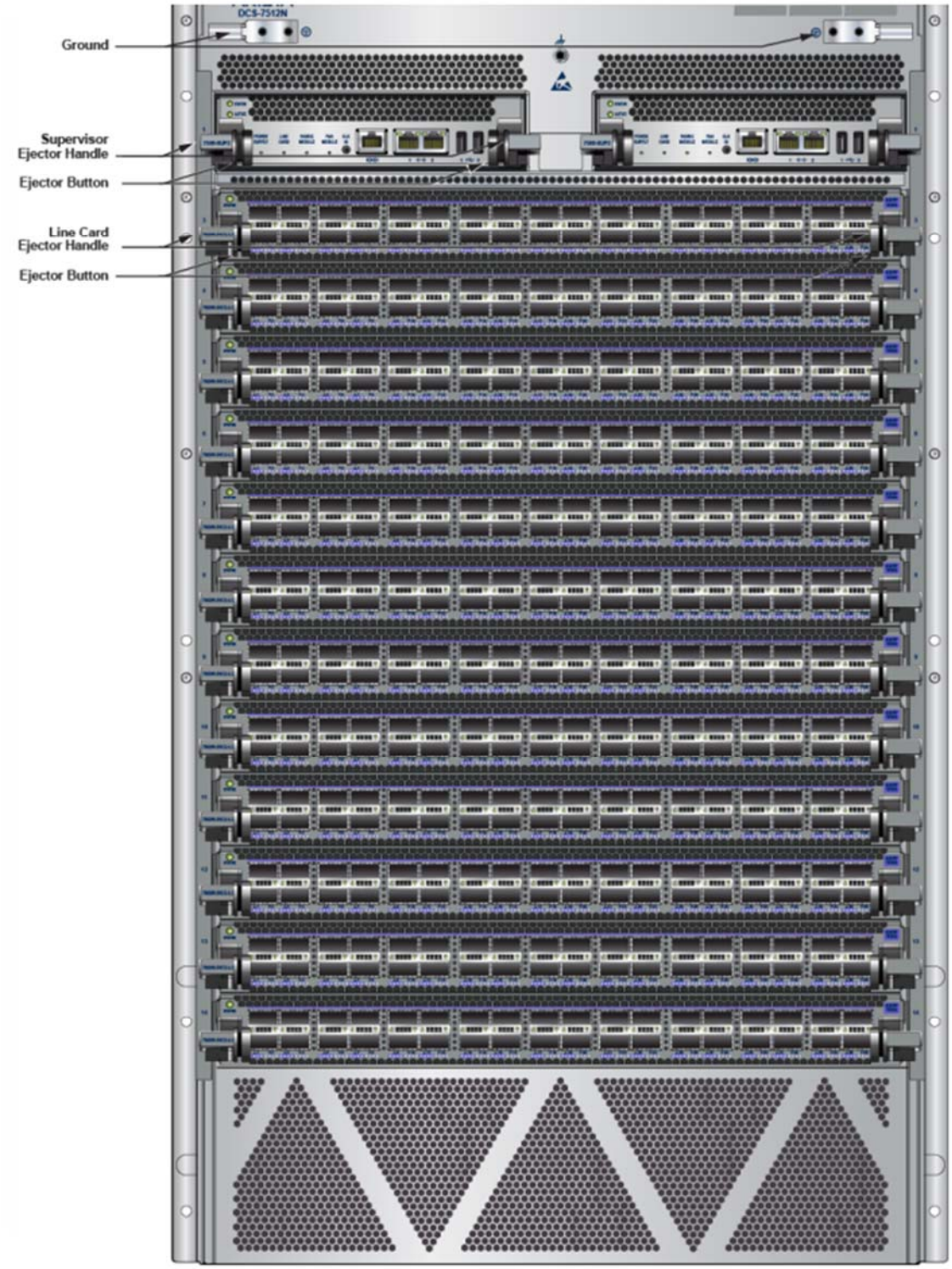

Figure 4 - DCS-7512N Front

 Document Version 1.4

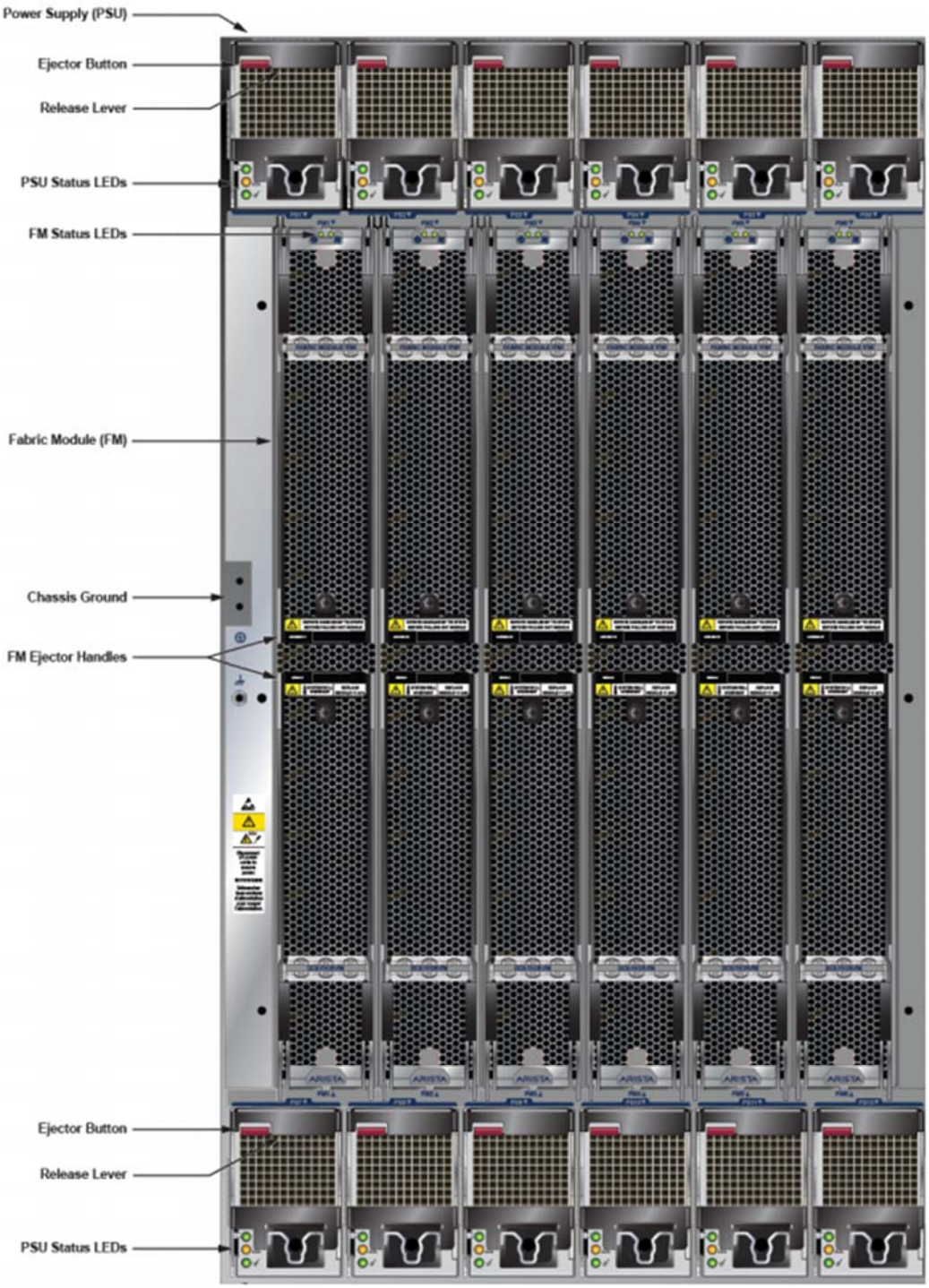

Figure 5 - DCS-7512N Rear

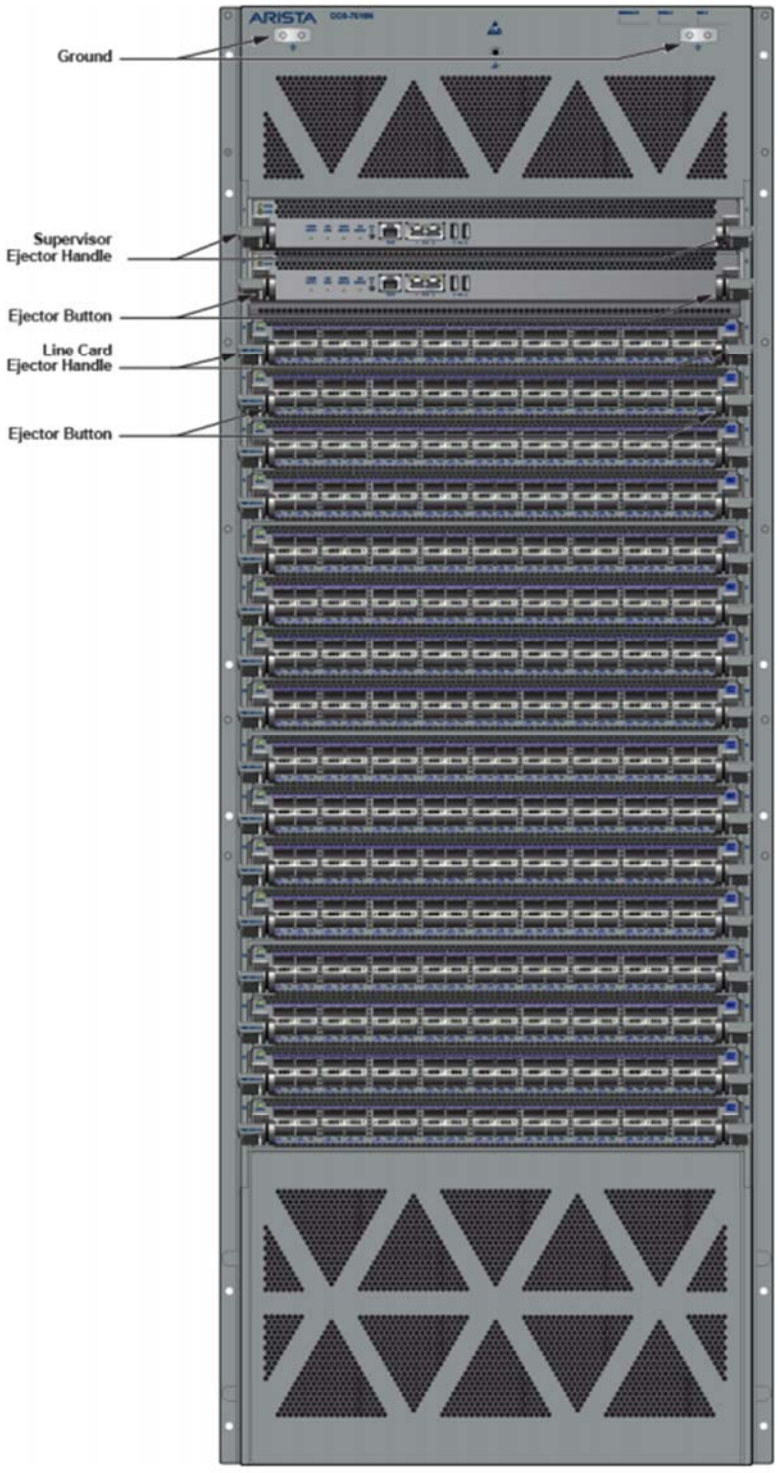

Figure 6 - DCS-7516N Front

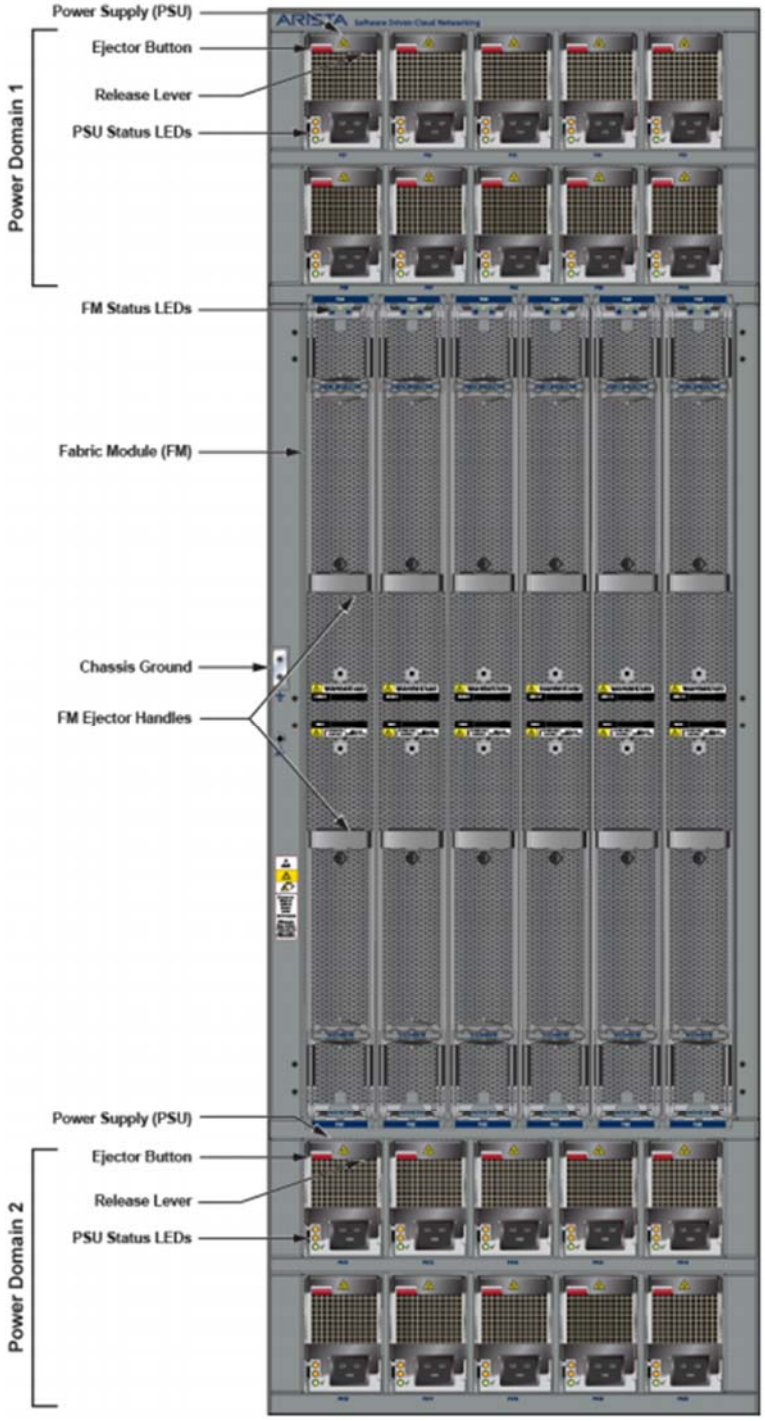

Figure 7 - DCS-7516N Rear

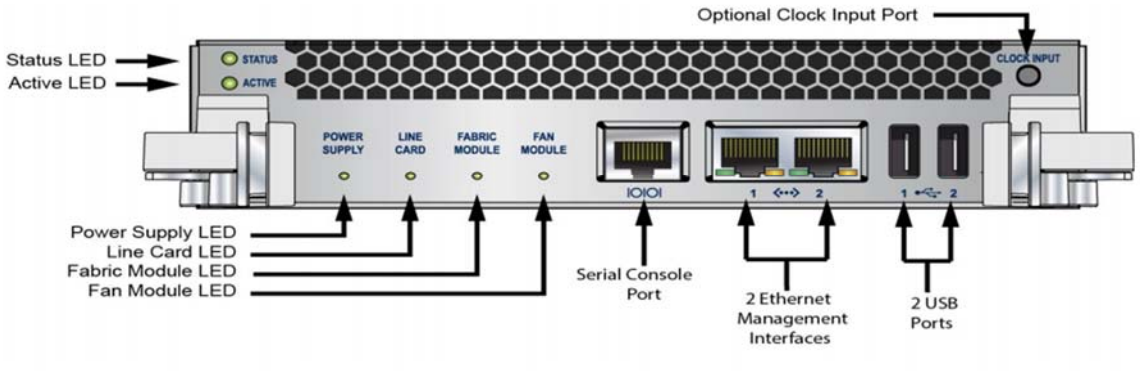

Figure 8 - DCS-7500E-SUP

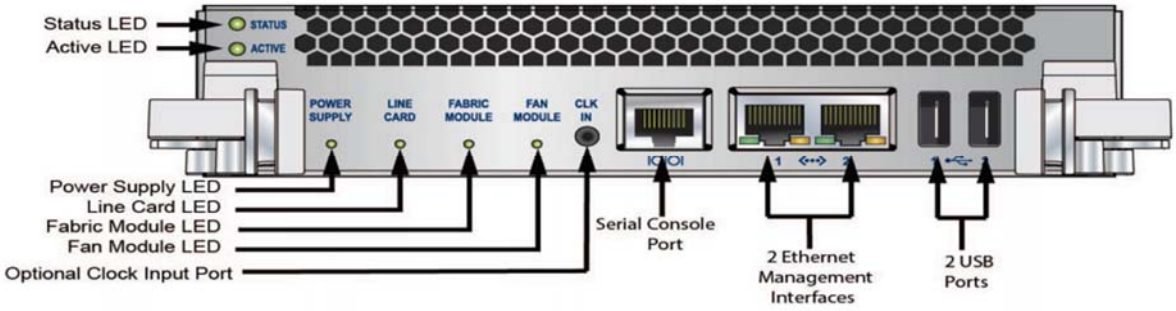

Figure 9 - DCS-7500-SUP2

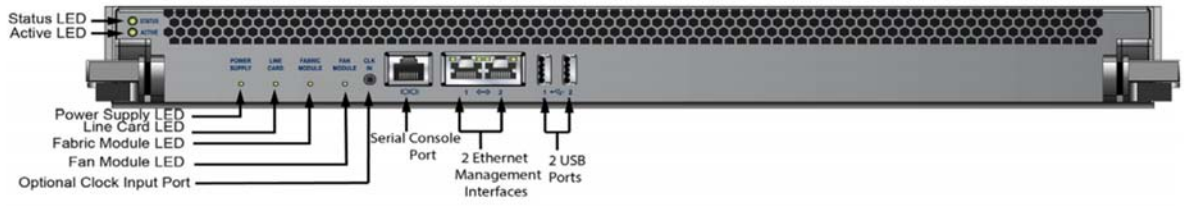

Figure 10 - DCS-7516-SUP2

 Document Version 1.4

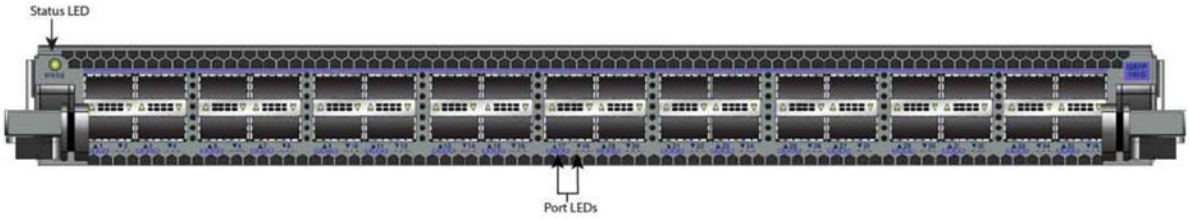

Figure 11 - DCS-7500RM-36CQ-LC

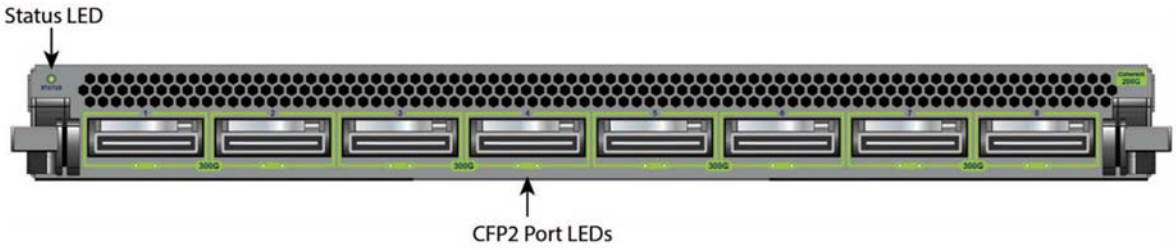

Figure 12 - DCS-7500R-8CFPX-LC

The FIPS 140-2 security levels for the Module are as follows:

Table 4 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall	1

1.2 Ports and Interfaces

The module has logical interfaces and physical ports listed in Table 5.

Table 5 – Ports and Interfaces

Logical Interface Type	Physical Port	Description
Power	Hardware Power Ground Connector (may be present on power supply and/or chassis)	Physical power supply port and electrical ground for Hardware
Control In	Serial Console Port Ethernet Management Port 1 Ethernet Management Port 2 Optional Clock Input Port	Firmware API entry point and physical ports control input
Status Out	Serial Console Port Ethernet Management Port 1 Ethernet Management Port 2 All LEDs	Firmware API return values, status output stack parameters, and physical ports status output
Data In	Serial Console Port Ethernet Management Port 1 Ethernet Management Port 2 Network USB 1 USB 2 Linecard Transceiver Ports	Firmware API input stack parameters, physical ports input
Data Out	Serial Console Port Ethernet Management Port 1 Ethernet Management Port 2 Network USB 1 USB 2 Linecard Transceiver Ports	Firmware API output stack parameters, physical ports output

1.3 Modes of Operation

The Module supports a FIPS 140-2 Approved mode and a non-Approved mode. The Approved mode is invoked by calling FIPS_mode_set() and using only Approved and allowed algorithms. Table 6 and Table 7 list the Approved and non-Approved but allowed algorithms, respectively.

The Hardware portion of the module only implements approved algorithms.

2. Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 6 – Approved Algorithms for Firmware Portion of Hybrid Module

Cert	Algorithm	Mode	Description	Functions/Caveats
5482	AES [197]	ECB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CCM [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128, 192, 256	External Counter Source
		CMAC [38B]	Key Sizes: 128, 192, 256 Tag Len: 16, 64, 128	Message Authentication
		GCM [38D][1]	Key Sizes: 128, 192, 256 Tag Len: 32, 64, 80, 96, 112, 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
Vendor Affirmed	CKG [IG D.12]	[133] Section 6.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133] Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		
		[133] Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
		[133] Section 7.4 Derivation of symmetric keys from a pre-shared key		
		[133] Section 7.5 Derivation of symmetric keys from a password		
		[133] Section 7.6 Combining multiple keys and other data		
1935	CVL: ECDSA SigGen [186]		P-256 SHA(1, 224, 256, 384, 512) P-384 SHA(1, 224, 256, 384, 512) P-521 SHA(1, 224, 256, 384, 512)	SigGen
1934	CVL: RSADP [56B]		n=2048	

[1] IG A.5 is met in Section 8.1 User Guide.

Cert	Algorithm	Mode	Description	Functions/Caveats
1933	CVL: TLS [135]	v1.0, v1.1	SHA-1	Key Derivation
		v1.2	SHA(256, 384, 512)	
	CVL: SSH [135]	v2	SHA(1, 224, 256, 384, 512)	
2158	DRBG [90A]	CTR	Use_df AES-256	Deterministic Random Bit Generation Security Strength = 256
1469	ECDSA [186]		P-256, P-384, P-521	KeyGen
			P-256, P-384, P-521	PKV
			P-256 SHA(1, 224, 256, 384, 512) P-384 SHA(1, 224, 256, 384, 512) P-521 SHA(1, 224, 256, 384, 512)	SigGen
			P-256 SHA(1, 224, 256, 384, 512) P-384 SHA(1, 224, 256, 384, 512) P-521 SHA(1, 224, 256, 384, 512)	SigVer
3636	HMAC [198]	SHA-1	MAC Sizes: 10, 12, 16, 20	Message Authentication, KDF Primitive, Password Obfuscation
		SHA-224	MAC Sizes: 14, 16, 20, 24, 28	
		SHA-256	MAC Sizes: 16, 24, 32	
		SHA-384	MAC Sizes: 24, 32, 40, 48	
		SHA-512	MAC Sizes: 32, 40, 48, 56, 64	
183	KAS FFC [56A]	dhEphem	FB, FC	Key Agreement
	KAS ECC [56A]	Ephemeral Unified	P-256, P-384, P-521	
235	KBKDF [108]	Counter	CMAC(AES-128, AES-256)	Key Based Key Derivation
N/A	KTS	AES-128, AES-256	AES Cert. #5482 and HMAC Cert. #3636	Key establishment methodology provides

Cert	Algorithm	Mode	Description	Functions/Caveats
				128 or 256 bits of encryption strength
2944	RSA [186]	X9.31	n = 2048 n = 3072 All primes are probable primes using random primality tests calculated via Table C.2	KeyGen
		X9.31	n = 2048 SHA(1, 256, 384, 512) n = 3072 SHA(1, 256, 384, 512)	SigGen
		PKCS1_v1.5	n = 2048 SHA(1, 224, 256, 384, 512) n = 3072 SHA(1, 224, 256, 384, 512)	SigGen
		PSS	n = 2048 SHA(1, 224, 256, 384, 512) n = 3072 SHA(1, 224, 256, 384, 512)	SigGen
		X9.31	n = 1024 SHA(1, 256, 384, 512) n = 1536 SHA(1, 256, 384, 512) n = 2048 SHA(1, 256, 384, 512) n = 3072 SHA(1, 256, 384, 512)	SigVer
		PKCS1_v1.5	n = 1024 SHA(1, 224, 256, 384, 512) n = 2048 SHA(1, 224, 256, 384, 512) n = 3072 SHA(1, 224, 256, 384, 512)	SigVer
		PSS	n = 1024 SHA(1, 224, 256, 384, 512) n = 2048 SHA(1, 224, 256, 384, 512) n = 4096 SHA(1, 224, 256, 384, 512)	SigVer
4399	SHS [180]	SHA-1 SHA-224 SHA-256 SHA-384 SHA-512		Message Digest Generation, Password Obfuscation, Verification of Integrity

Note: There are algorithms, modes, and key lengths that have been CAVs tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in these tables are used by the module, except where noted otherwise. DSA (Cert. #1410) is tested but not used in FIPS mode and can be used in non-FIPS mode. Triple-DES (Cert. #2759) is tested but not used in FIPS mode and can be used in non-FIPS mode.

The Firmware Portion of the Module implements the following NIST-specified algorithms, which are non-Approved but allowed, either from algorithm transitions (e.g., SP800-131A) or from not being tested:

Table 7 – Non-Approved but Allowed Cryptographic Functions for Firmware Portion of Hybrid Module

Algorithm	Description
Key Agreement Using DH (Diffie-Hellman) or MQV but Not Fully Compliant with SP 800-56A (e.g., DH or ECDH)[2]	[IG D.8]
Key Transport (Encapsulation) Using RSA but Not Fully Compliant with SP 800-56B (e.g., RSA Key Wrap)[3]	[IG D.9]
NDRNG or TRNG	[FIPS 140-2, Section 4.7.1]
MD5 within TLS	[IG 1.23]

Table 8 – Security Relevant Protocols[4] Used in FIPS Mode for Firmware Portion of Hybrid Module

Protocol	Reference
EAP-FAST	[RFC 4851]
SSHv2	[IG D.8 and SP 800-135]
TLS v1.0/v1.1/v1.2	[IG D.8, IG D.9 and SP 800-135]

Table 9 – Security Relevant Protocols[5] Used in FIPS Mode

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
DTLS [IG D.9]	See TLS entry in this table.			

[2] DH or ECDH key establishment methodology provides between 128 and 256 bits of encryption strength.

[3] RSA key establishment methodology provides between 112 and 128 bits of encryption strength.

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

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

Protocol	Key Exchange	Server/ Host Auth	Cipher	Integrity
SSHv2 [IG D.8 and SP 800-135]	ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256, diffie-hellman-group14-sha1	ECDSA P-256, RSA	AES-CBC-128/256 AES-CTR-128/256	hmac-sha2-512 hmac-sha2-256 hmac-sha1
TLS [IG D.8 and SP 800-135]	TLS_RSA_WITH_AES_256_CBC_SHA for TLS v1.0, v1.1, v1.2			
	RSA	RSA	AES-CBC-256	HMAC-SHA-1
	TLS_RSA_WITH_AES_256_CBC_SHA256 for TLS v1.0, v1.1, v1.2			
	RSA	RSA	AES-CBC-256	HMAC-SHA-256
	TLS_RSA_WITH_AES_128_CBC_SHA for TLS v1.0, v1.1, v1.2			
	RSA	RSA	AES-CBC-128	HMAC-SHA-1
	TLS_RSA_WITH_AES_128_CBC_SHA256 for TLS v1.0, v1.1, v1.2			
	RSA	RSA	AES-CBC-128	HMAC-SHA-256
EAP-FAST	See TLS above.			

Table 10 – Untested and Transition-Disallowed Cryptographic Functions for Firmware Portion of Hybrid Module

Function	Algorithm	Options
Digital Signature and Asymmetric Key Generation	RSA key size < 2048 (Disallowed)	GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS (<2048)
	DSA[6] key size <2048 (Disallowed)	PQG Gen, Key Pair Gen, Sig Gen (<2048)
Key Encryption, Decryption	RSA key size < 2048 (Disallowed)	RSA key encryption/decryption (<2048)

The algorithms in Table 10 must not be used when operating in the FIPS mode of operation.

The Firmware Portion of the Module also implements the following algorithms, which are non-Approved:

[6] DSA (Cert. #1410) is tested but not used in FIPS mode and can be used in non-FIPS mode.

Table 11 –Other non-Approved Cryptographic Functions not Allowed in FIPS mode for Firmware Portion of the Hybrid Module

Function	Algorithm
Encryption and Decryption	AES/Triple-DES KW (non-compliant)
	Blowfish
	Camellia 128/192/256
	CAST5
	DES
	DES-X
	IDEA
	RC2
	RC4
	RC5
	SEED
Message Digests	MD4
	MD5
	RIPEMD-160
	Whirlpool
	Triple-DES MAC
Keyed Hash	HMAC-MD5

The algorithms in Table 11 are automatically disabled when in the FIPS mode of operation.

The Hardware Portion of the Hybrid Module only functions in an Approved mode using the following algorithms listed in Table 12.

Table 12 –Approved Algorithms for Hardware Portion of Hybrid Module

Cert	Algorithm	Mode	Description	Functions/Caveats
4545	AES [197]	ECB [38A]	Key Sizes: 128, 256	Encrypt
		CTR [38A]	Key Sizes: 128, 256	External Counter Source
		GCM [38D]	Key Sizes: 128, 256 Tag Len: 64, 96, 104, 112, 120, 128	Encrypt, Decrypt
		XPN [IEEE Std. 802.1AEbw-2013]	Key Sizes: 128, 256 Tag Len: 64, 96, 104, 112, 120, 128	Encrypt, Decrypt

2.1 Critical Security Parameters

All CSPs used by the Module are described in Table 13. All usages of these CSPs by the Module (including all CSP lifecycle states) are described in the services detailed in Section 3.

Table 13 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG-EI	DRBG entropy input of 3072 bytes containing 384 bits of entropy based on entropy assessment
AES EDK	AES encrypt / decrypt key (128/192/256)
AES CMAC	AES CMAC generate / verify key (128/192/256)
AES CCM	AES encrypt / decrypt / generate / verify key for CCM (128/192/256)
AES GCM (FW)	AES encrypt / decrypt / generate / verify key for GCM in firmware (128/192/256)
CMAC EDK	CMAC symmetric encrypt/decrypt key (128/256) used in KBKDF PRF
CTR_DRBG CSPs	V (128 bits) and Key (AES 256)
ECDSA SGK	ECDSA signature generation key - P-256 SHA (1, 224, 256, 384, 512) P-384 SHA (1, 224, 256, 384, 512) P-521 SHA (1, 224, 256, 384, 512)
EC Diffie-Hellman Private	EC Diffie-Hellman private key agreement key – key length dependent upon the receiving algorithm
HMAC Key	Keyed hash key (160/224/256/384/512)
RSA SGK	RSA signature generation key n = 2048 SHA (1, 256, 384, 512) n = 3072 SHA (1, 256, 384, 512)
RSA KDK	RSA key decryption (private key transport) key (2048/3072)
AES GCM (HW)	AES encrypt / decrypt / generate / verify key for GCM in hardware (128/256)
AES-CTR Counter (HW)	AES counter mode counter in hardware (128/256)
AES-GCM-XPN Salt (HW)	Salt for AES-GCM-XPN in hardware (96)
SSH-DH-Priv	(SSHv2 Diffie-Hellman ephemeral) 2048 DH private portion
SSH-Host-Priv	(SSHv2 Host Key) RSA n=2048 Private Key
SSH-SENC	(SSHv2 Session Encryption Key) AES CBC 128/256 keys
SSH-SMAC	(SSHv2 Session Authentication Keys) HMAC-SHA-1 160 bit key
MACsec-SENC	MACsec AES 128/256 keys
TLS-Host-Priv	(TLS Host Key) RSA n=2048 Private Key
TLS-MS	(TLS Master Secret) 384 bit secret key material
TLS-PMS	(TLS Pre-Master Secret) 2048/384 bit secret key material
TLS-SENC	(TLS Session Encryption Key) AES CBC 128/256 keys
TLS-SMAC	(TLS Session Authentication Keys) HMAC-SHA-1 (160 bit) or HMAC-SHA-256 (256 bit)

2.2 Public Keys

Table 14 –Public Keys

Key	Description / Usage
SSH-Host-Pub	(SSHv2 Host Key) RSA 2048 public key
SSH-DH-SRV-Pub	SSHv2 Diffie-Hellman 2048 server public key
SSH-DH-CLI-Pub	SSHv2 Diffie-Hellman 2048 client public key
ECDSA SVK	ECDSA signature verification key – P-256 SHA(1, 224, 256, 384, 512) P-384 SHA(1, 224, 256, 384, 512) P-521 SHA(1, 224, 256, 384, 512)
EC Diffie-Hellman Public	EC Diffie-Hellman public key agreement key - – key length dependent upon the receiving algorithm
RSA SVK	RSA signature verification public key – n = 1024 SHA(1, 256, 384, 512) n = 1536 SHA(1, 256, 384, 512) n = 2048 SHA(1, 256, 384, 512) n = 3072 SHA(1, 256, 384, 512)
RSA KEK	RSA key encryption (public key transport) key (2048/3072)
TLS-Host-Pub	(TLS Host Key) RSA 2048 public key

3. Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). Operator authentication is not performed.

Table 15 lists all operator roles supported by the module. The Module does not support a maintenance role nor bypass capability. The Module does not support concurrent operators.

Table 15 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – Installation of the Module on the host computer system and calling of any API functions.	None	N/A
User	User – Loading the Module and calling any of the API functions.	None	N/A

3.2 Services

All services implemented by the Module are listed in the table below.

Table 16 – Authenticated Services

Service	Description	CO	U
Initialize	Module initialization. Does not access CSPs.	X	X
Self-test	Perform self-tests (FIPS_selftest). Does not access CSPs.	X	X
Show status	Functions that provide module status information: 1. Version (as unsigned long or const char *) 2. FIPS Mode (Boolean) Does not access CSPs.	X	X
Zeroize	Functions that destroy CSPs: 1. fips_drbg_uninstantiate: for a given DRBG context, overwrites DRBG CSPs (Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs.) All other services automatically overwrite CSPs stored in allocated memory. Stack cleanup is the responsibility of the calling application.	X	X
Random number generation	Used for random number and symmetric key generation. • Seed or reseed a DRBG instance • Determine security strength of a DRBG instance • Obtain random data Uses and updates Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs.	X	X
Asymmetric key generation	Used to generate ECDSA and RSA keys: RSA SGK, RSA SVK;RSA KEK, ECDSA SGK, ECDSA SVK, SSH-Host-Priv, SSH-Host-Pub; and TLS-Host-Pub	X	X
Symmetric encrypt/decrypt	Used to encrypt or decrypt data. Executes using any symmetric encryption key from Table 13: AES EDK, AES CMAC, AES CCM, AES GCM, (FW), CMAC EDK, AES GCM (HW), AES-CTR Counter (HW), AES-GCM-XPN Salt (HW), SSH-SENC, and MACsec-SENC (passed in by the calling process).	X	X
Symmetric digest	Used to generate or verify data integrity with CMAC. Executes using AES CMAC (passed in by the calling process).	X	X
Message digest	Used to generate a SHA-1 or SHA-2 message digest. Does not access CSPs.	X	X
Keyed Hash	Used to generate or verify data integrity with HMAC. Executes using HMAC Key, SSH-SMAC, and TLS-SMAC (passed in by the calling process).	X	X

Service	Description	CO	U
SSH connection	Used to establish an SSH connection. Executes using EC Diffie-Hellman Private, EC Diffie-Hellman Public, SSH-DH-Priv, SSH-Host-Priv, SSH-SENC, and SSH-SMAC.	X	X
TLS connection	Used to establish a TLS connection. Executes using RSA KDK, RSA KEK, TLS-MS, TLS-PMS, TLS-SMAC, TLS-SENC, TLS-DH-Pub, and TLS-Host-Pub.	X	X
Key derivation	Used to perform key derivation primitives as per SP800-135: TLS KDF and SSH KDF (this service does not establish keys into the module).	X	X
Digital signature	Used to generate or verify RSA or ECDSA digital signatures. Executes using RSA SGK, RSA SVK; ECDSA SGK, ECDSA SVK, SSH-Host-Priv, SSH-Host-Pub, and TLS-Host-Pub (passed in by the calling process).	X	X
Utility	Miscellaneous helper functions. Does not access CSPs.	X	X

Since Operator Authentication is not performed, both the CO and U have the ability to perform all operations. The differentiation between the two roles is that the Crypto Officer would be the one responsible for installation of the crypto module. The above table applies to both the Firmware and Hardware portions of the module.

Table 17 – Table 20 define the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The service generates the CSP.
- O = Output: The service outputs the CSP.
- E = Execute: The service uses the CSP in an algorithm.
- I = Input: The service inputs the CSP.
- Z = Zeroize: The service zeroizes the CSP.

(Tables 17, 18, and 19 are split due to the maximum size of the page they appear on.)

Table 17 – Security Parameters Access by Service excluding Public Keys

Service / CSP	DRBG-EI	AES EDK	AES CMAC	AES CCM	AES GCM (FW)	CMAC EDK	CTR DRBG CSPs	Hash_DRBG CSPs	HMAC_DRBG CSPs	ECDSA SGK
Initialize	-	-	-	-	-	-	-	-	-	-

Self-test	-	-	-	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Random Number Generation	IE	-	GO	GO	-	-	E	E	E	-
Asymmetric key generation	-	-	-	-	-	-	I	I	I	GO
Symmetric encrypt/decrypt	-	IE	IE	IE	IE	IE	-	-	-	-
Symmetric digest	-	-	IE	-	-	-	-	-	-	-
Message Digest	-	-	-	-	-	-	-	-	-	-
Keyed Hash	-	-	-	-	-	-	-	-	-	-
SSH connection	-	-	-	-	-	-	-	-	-	IE
TLS connection	-	-	-	-	-	-	-	-	-	-
Key derivation	-	-	-	-	-	G	-	-	-	-
Digital signature	-	-	-	-	-	-	-	-	-	IE
Utility	-	-	-	-	-	-	-	-	-	-

Table 18 – Security Parameters Access by Service excluding Public Keys

Service / CSP	EC Diffie-Hellman Private	HMAC Key	RSA SGK	RSA KDK	AES GCM (HW)	AES-CTR Counter (HW)	AES-GCM-XPN Salt (HW)
Initialize	-	-	-	-	-	-	-
Self-test	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z
Random Number Generation	-	-	-	-	-	-	-
Asymmetric key generation	-	-	GO	-	-	-	-
Symmetric encrypt/decrypt	-	-	-	-	IE	IE	IE
Symmetric digest	-	-	-	-	-	-	-

Message Digest	-	-	-	-	-	-	-
Keyed Hash	-	IE	-	-	-	-	-
SSH connection	OE	-	-	-	-	-	-
TLS connection		-	-	E	-	-	-
Key derivation	I	-	-	IE	-	-	-
Digital signature	-	-	IE	-	-	-	-
Utility	-	-	-	-	-	-	-

Table 19 – Security Parameters Access by Service excluding Public Keys

Service / CSP	SSH-DH-Priv	SSH-Host-Priv	SSH-SENC	SSH-SMAC	MACsec-SENC	TLS-DH-Priv	TLS-MS	TLS-PMS	TLS-SENC	TLS-SMAC
Initialize	-	-	-	-	-	-	-	-	-	-
Self-test	-	-	-	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Random Number Generation	-	-	-	-	-	-	-	-	-	-
Asymmetric key generation	-	GO	-	-	-	-	-	-	-	-
Symmetric encrypt/decrypt	-	-	IE	-	IE	-	-	-	IE	-
Symmetric digest	-	-	-	-	-	-	-	-	-	-
Message Digest	-	-	-	-	-	-	-	-	-	-
Keyed Hash	-	-	-	IE	-	-	-	-	-	IE
SSH connection	OE	E	E	E	-	-	-	-	-	-
TLS connection		-	-	-	-	OE	IEO	OE	E	E
Key derivation	IE	-	-	-	-	IE	-	-	-	-
Digital signature	-	IE	-	-	-	-	-	-	-	-
Utility	-	-	-	-	-	-	-	-	-	-

 Document Version 1.4

Table 20 – Security Parameters Access by Service for Public Keys

Service / Public Key	SSH-Host-Pub	SSH-DH-SRV-Pub	SSH-DH-CLI-Pub	ECDSA SVK	EC Diffie-Hellman Public	RSA SVK	RSA KEK	TLS-Host-Pub	TLS-DH-Pub
Initialize	-	-	-	-	-	-	-	-	-
Self-test	-	-	-	-	-	-	-	-	-
Show Status	-	-	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z
Random Number Generation	-	-	-	-	-	-	-	-	-
Asymmetric key generation	GO	-	-	GO	-	GO	GO	GO	-
Symmetric encrypt/decrypt	-	-	-	-	-	-	-	-	-
Symmetric digest	-	-	-	-	-	-	-	-	-
Message Digest	-	-	-	-	-	-	-	-	-
Keyed Hash	-	-	-	-	-	-	-	-	-
SSH connection	-	-	-	-	IE	-		-	-
TLS connection	-	IE	IE	-		-	IE	E	IE
Key derivation	-	-	-	-	-	-	-	-	-
Digital signature	IE	-	-	IE	-	IE	-	IE	-
Utility	-	-	-	-	-	-	-	-	-

4. Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2, these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.
All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. If one of the KATs fails, the Module enters the fatal error state. In the firmware portion, this is indicated by causing the calling application to fail with a segmentation fault. In the hardware portion, this is indicated by putting the chip in an error state. Otherwise, success is indicated by the successful load of the firmware module and the chip indicating it is ready to perform operations.

The module performs the following algorithm KATs on power-up:

- Firmware Integrity: HMAC-SHA-256 digest over all the module code.
- AES-ECB-128 encrypt and decrypt KATs
- AES-CCM-128,192, and 256 Generation KATs
- AES-CCM-128,192, and 256 Verification KATs
- HW AES ECB KATs
- HW AES CTR KATs
- HW AES GCM KATs
- HW AES XPN KATs
- GCM/GMAC-128 Generation KAT
- GCM/GMAC-128 Verification KAT
- RSA KATs sign and verify
- ECDSA PCT sign and verify
- SP 800-90A CTR_DRBG KAT
- SP 800-90A Hash_DRBG KAT
- SP 800-90A HMAC_DRBG KAT
- CMAC-AES-128 Generation KAT
- HMAC-SHA-1, -224, -256, and -512 KAT
- SHA-1, -224, -256, -384, and -512 KAT
- FFC DH Primitive “Z” Computation KAT
- ECC DH Primitive “Z” Computation KAT
- KBKDF KAT

The module performs the following conditional self-tests as indicated:

- DRBG CRNGT using 128-bit block size
- DRBG: SP800-90A Health Tests
- ECDSA Pairwise consistency test on EDSA key pair generation
- RSA Pairwise consistency test on RSA key pair generation

5. Physical Security

The Module is multi-chip standalone firmware-hybrid. All the Module physical components are production-grade and are contained in a production-grade enclosure. All ICs have standard passivation. The physical boundary is the case of the switch chassis.

6. Operational Environment

The operational environment requirements are not applicable because the Module has a non-modifiable operational environment.

7. Mitigation of Other Attacks Policy

The module is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

8. Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module does not provide operator authentication.
3. The module clears previous CSPs on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output are inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.
13. The module supports key entry encrypted over SSH.
14. The module does not have any proprietary external input/output devices used for entry/output of data.
15. The module does not enter plaintext CSPs.
16. The module does not provide the output of plaintext CSPs.
17. The module does not output intermediate key values.
18. The module must be seeded, and reseeded where applicable, with 256 bits of entropy
19. The module does not provide bypass services.
20. SNMPv3 is not to be used in the FIPS mode of operations.
21. DSA is not to be used in the FIPS mode of operations.
22. Triple-DES is not to be used in the FIPS mode of operations.

8.1 User Guide

FIPS Mode of Operation Configuration

In order to invoke the FIPS mode of operation, the following steps must be taken:

1. Remove the ability for EOS to be “open” by locking down access to python shell, bash shell, etc.
2. Enable hardware based entropy.
3. For each FIPS compliant feature, enable the “fips restrictions” setting for that submode.
4. For each FIPS compliant feature, set the algorithms used to those which are FIPS approved and allowed. The EOS User Manual can specify the exact commands for each feature.
5. To securely clear and regenerate the ssh hostkeys, enter "reset ssh hostkey rsa".
6. Enable Role Based Access Controls to prevent steps 1 through 3 from being reverted.
7. Compliance can be verified via “show” commands as well as observing the running configuration.
8. TLS private keys should only be loaded after entering FIPS mode.

In order to change from FIPS mode to non-FIPS mode, the following steps must be taken:

1. Delete the TLS private keys via the following command: "delete sslkey:<key name>" where <key name> is the name of the TLS key.
2. Securely reset the SSH hostkey via "reset ssh hostkey rsa".
3. Remove the role-based access controls.
4. Enable access to the bash shell.
5. For each FIPS compliant feature, disable FIPS mode by running "no fips restrictions" for that submode.

MACsec Introduction

The Module’s role is that of Authenticator in the MACsec protocol. When supporting the MACsec protocol in the approved mode, the module should only be used together with the CMVP-validated modules providing the remaining Peer (allowing for more than one), and Authentication Server functionalities. The AES-GCM key is generated externally from the authentication server and the IV is constructed in its entirety internally deterministically.

Furthermore, the link between the Peer and the Authenticator should be secured to prevent the possibility for an attacker to introduce foreign equipment into the local area network – see Section 7.3 in IEEE Std 802.1X-2010.

MACsec Configuration Instructions

MACsec must be ran in a mode that utilizes dynamic key derivation for the Security Association Key (SAK). The static configuration of a pre-shared SAK shall not be used in the approved mode of operation. Static Connectivity Association Key (CAK) security mode, using a pre-shared CAK identified by a Connectivity Association Key Name (CKN), as well as 802.1X, provide for dynamic key derivation of the SAK.

MACsec IV Information

MACSec IV generation is done in the standard IEEE approved manner, as stated in IEEE 802.1AE-2006, Section 14.5. For IV Generation, per the standard, the 64 most significant bits of the 96-bit IV are the octets of the SCI, encoded as a binary number. The 32 least significant bits of the 96-bit IV are the octets of the PN, encoded as a binary number (Section 14.5 of the 802.1AE-2006). The PN, packet number provides a deterministic non-repetitive counter. The remaining 64 bits are used by the SCI to form a name. 48 bits of the SCI are a globally unique MAC address – see Section 8.2.1 of the IEEE Std 802.1AE-2006. As a result at least 2^{48} names are possible, exceeding the FIPS 140-2 IG A.5 requirement of at least 2^{32} names being possible.

When the deterministic non-repetitive counter has exhausted the maximum number of values, the session is aborted and a new key is generated.

In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption will be established by the Authenticator.

This meets IG A.5, per the standard MACsec IV Generation scheme in IEEE 802.1AE, Section 14.5.

9. References and Definitions

The following standards are referred to in this Security Policy.

Table 21 - References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *January 2011*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Abbreviation	Full Specification Name
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38E]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, Special Publication 800-38E, January 2010*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[56Br1]	*NIST Special Publication 800-56A Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2016.*
[RFC 4581]	*IETF, The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST), May 2007.*

Table 22 – Acronyms and Definitions

Acronym	Definition
CO	Cryptographic Officer role
EDK	Encrypt / Decrypt Key
EOS	Name of the Arista operating system for the MACsec
KDK	Key Decryption Key
KEK	Key Encryption Key
MACsec	Layer-2 Encryption Protocol whose formal name is: IEEE 802.1AE
MDIO	Management Data Input / Output – a serial bus used for communications within the MACsec linecard between the SCD FPGA and MACsec chip and other devices.
MS	Master Secret used in TLS
SCD FPGA	The System Control Device, Field Programmable Gate Array converts PCIe communications channel to the MDIO interface.
SENC	Session Encryption
SGK	Signature Generation Key
SVK	Signature Verification Key
Transceiver	Physical connection between a network cable and a switch. This translates the wires connection type to data in a standard way that the switch can consume.
VA	Vendor Affirmed cryptographic algorithms are Approved algorithms for which no CAVP tests are available yet. The vendor performs their own testing as the basis for their affirmation.