GigaVUE-HC3 Visibility Appliance *by* Gigamon Inc.

FIPS 140-2 Non-Proprietary Security Policy

Hardware Versions: GVS-HC3A1 *and* GVS-HC3A2 (Chassis) *with* SMT-HC3-C05 (GigaSMART), CTL-HC3-002 (Controller) and GVS-HC3-EXT; FIPS Tamper Label SKU: ACC-HC0-FIPS

Firmware Version: 5.9.00.05

Multi-chip Standalone, Level 2 Validation
February 5, 2021

Document Version 1.0

1 Introduction

The GigaVUE-HC3 visibility appliance provides intelligent traffic visibility in a modular, mid-sized form factor, to address complex network visibility requirements for both enterprise and service provider networks. With a broad spectrum of traffic management capabilities and a versatile, high-performance, multi-purpose design, GigaVUE-HC3 helps to future-proof IT.

There are two hardware models represented under this validation, which are specified by their respective unique hardware versions, stated below. Both hardware versions are validated with the same firmware version, share the same physical appearance, and only differ in terms of their power supplies. The firmware image applied to both hardware versions originates from the factory and the firmware status service identifies the module as version **5.9.00.05**

The cryptographic module is defined as a multiple-chip standalone module with the following details:

Table 1 – GigaVUE-HC3 Module Configurations

Model	Hardware Versions	Firmware	Tested Configuration
1	GVS-HC3A1 (Chassis) SMT-HC3-C05 (GigaSMART) CTL-HC3-002 (Controller) GVS-HC3-EXT	5.9.00.05	***Slot 1:*** GigaSMART PN: SMT-HC3-C05 **Slot 2:** Blank (Faceplate Affixed) ***Slot 3:*** Blank (Faceplate Affixed) ***Slot 4:*** Blank (Faceplate Affixed) **Lower Slot:** GVS-HC3-EXT ***Internal:*** Controller PN: CTL-HC3-002 ***Power Supply:*** AC
2	GVS-HC3A2 (Chassis) SMT-HC3-C05 (GigaSMART) CTL-HC3-002 (Controller) GVS-HC3-EXT	5.9.00.05	***Slot 1:*** GigaSMART PN: SMT-HC3-C05 ***Slot 2:*** Blank (Faceplate Affixed) ***Slot 3:*** Blank (Faceplate Affixed) ***Slot 4:*** Blank (Faceplate Affixed) **Lower Slot:** GVS-HC3-EXT ***Internal:*** Controller PN: CTL-HC3-002 ***Power Supply:*** DC
All	FIPS Tamper Labels SKU: ACC-HC0-FIPS	N/A	Tamper-Evident Seals

* **Note**: The Controller (PN: CTL-HC3-002) is inserted into the chassis by Gigamon and is not physically accessible by operators.

The modules are designed to meet FIPS 140-2 Level 2 overall:

Table 2 – Security Level of Security Requirements

Area	Description	Level
1	Module Specification	2
2	Ports and Interfaces	2
3	Roles and Services	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Key Management	2
8	EMI/EMC	2
9	Self-test	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	2

The modules have a non-modifiable operational environment as per the FIPS 140-2 definition. They include a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into these modules is out of the scope of this validation and require a separate FIPS 140-2 validation.

The modules do not implement any mitigations of other attacks as defined by FIPS 140-2.

1.1 Hardware, Physical and Logical Cryptographic Boundary

The physical forms of the two models are depicted in the figures below. For both models, the cryptographic boundary is defined as the outer edge of the chassis. The modules do not rely on external devices for input and output. The logical boundary is the same as the physical boundary.

Figure 1 - GVS-HC3A1 *and* GVS-HC3A2 (Front of Module Chassis)

Figure 2 – SMT-HC3-C05 (Populated in Slot 1 of Module Chassis)

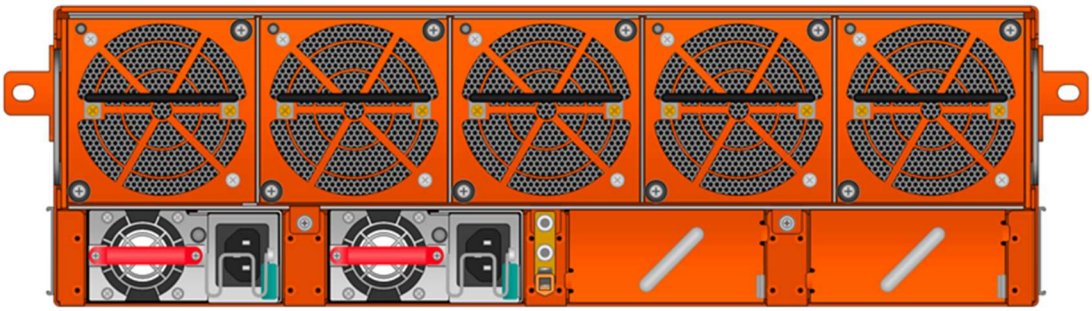

Figure 3 - GVS-HC3A1 *and* GVS-HC3A2 (Rear Chassis)

Table 3 – Ports and Interfaces

Port	Device (# of ports)	Description	Logical Interface Type
Power Switch	SMT-HC3-C05 • H/S (Hot Swap status)	On/Off Switch	• Control Input
LEDs	GVS-HC3A1 *and* GVS-HC3A2 (GVS-HC3-EXT) RDY (HC3 status), PTP (Ethernet status), PPS (clock status), M/S (HC3 standalone or part of cluster), FAN, PWR SMT-HC3-C05 Power, RDY, H/S	Status LEDs	• Status Output
RJ45	GVS-HC3A1 *and* GVS-HC3A2 (GVS-HC3-EXT) • Management Port • PTP Port	Chassis Management Ports	• Data Input • Data Output • Control Input • Status Output
Serial	GVS-HC3A1 *and* GVS-HC3A2 (GVS-HC3-EXT) • Console Port	Chassis Console Port	• Data Input • Data Output • Control Input • Status Output
QSFP+	SMT-HC3-C05 • GigaSMART 5 x 40Gb (QSFP+)	LAN Communications	• Data Input • Data Output
SFP+/SFP	GVS-HC3A1 *and* GVS-HC3A2 (GVS-HC3-EXT) • STACK, P/S 3 x 10Gb/1Gb (SFP+/SFP)	Chassis Ports	• Data Input • Data Output

USB	GVS-HC3A1 and GVS-HC3A2 • USB	Data Transfer	• Data Input • Data Output
PPS(IN)	GVS-HC3A1 *and* GVS-HC3A2	Pulse-per-second	• Data Input
Power	GVS-HC3A1 *and* GVS-HC3A2 The chassis is powered by two separate power modules, providing redundant, load sharing power. The **GVS-HC3A1** uses an AC power supply configuration with the following specification: 100-115V 200-240V 14A@100V 10A @200V 50/60Hz The **GVS-HC3A2** uses a DC power supply configuration with the following specification: -40V to -72V 48A@-40V	Power Supply GVS-HC3A1 (AC) GVS-HC3A2 (DC)	• Power • Power Switch Control Input

1.2 Mode of Operation

The module implements both exclusive FIPS Approved and non-FIPS Approved modes, however an exception to this are some non-Approved security functions which are available in the exclusive FIPS Approved mode but will cause the module to operate in a non-Approved mode (by policy) if executed. These additional non-Approved security functions are listed accordingly in Table 9 of this security policy.

The Crypto-Officer (admin) shall prepare the module for the FIPS Approved mode of operation by performing the following tasks:

1. The module will ship using a firmware other than the intended FIPS validated firmware version **5.9.00.05**. The firmware shall first be upgraded to this version by fetching firmware image **5.9.00.05** from Gigamon using either http(s) or ftp(s) as documented in the User Guide.

2. The module firmware shall be loaded onto the module in the non-active partition using the **"image install <image name>"** command.

3. The module firmware shall be loaded onto the module in the non-active partition. Once the load process is complete, it is imperative to ensure that the partition holding firmware version **5.9.00.05** is the one being initialized. Switching partitions to enable **5.9.00.05** may be accomplished by specifying **"image boot next"** from the CLI (or may be selected at power-up from the menu).

4. To ensure that no authentication data is carried over from any previous session, the operator shall issue the command **"reset factory all"** after the **"image boot next"** command is issued.

5. The operator may then login using the default administrator account using the default credentials "admin" with password "admin123A!". The operator will be presented with the option of executing the wizard.

6. Once the wizard executes, the operator **shall** change the default password.

7. Once the setup configuration is complete, the operator shall ensure that the module is running firmware version **5.9.00.05** by issuing the CLI command **"show version".** ***Failure to execute the firmware version 5.9.00.05 will result in a non-FIPS validated module***.

8. To configure the module to use the FIPS Approved mode, the operator is required to perform "**system security fips"**. Upon confirmation of this command, the module will automatically perform all necessary steps including reloading the module, which will then enter the Approved mode. For the selection of the non-Approved mode, the operator would use the command **"no system security fips"**. This will result in complete key and CSP zeroization of those keys and CSPs which were generated in the FIPS Approved mode and will also leave the operator in a limited state of operation; whereby only a limited set of non-cryptographic services are available. (Switching from the non-Approved mode to the Approved mode will also zeroize all keys and CSPs.) Tables 11 and 12 of this security policy provides details about the available FIPS Approved and non-FIPS Approved services respectively.

9. The Crypto-Officer (CO) shall follow the instructions in Section 5 to apply the tamper seals to the module. The module may be configured to operate in an Approved mode of operation as specified in the instructions below. The module will be operating in the Approved mode once all instructions are completed and the module has successfully passed all power-on self-tests.

1.3 Zeroization

The module has 6 specific methods of zeroizing keys/CSPs as follows:

1. System Power Cycle (All ephemeral keys are lost from RAM);
2. End of Protocol Session (All ephemeral keys are lost from RAM);
3. When operator deletes Key/CSP and saves configuration (persistent keys);
4. When FIPS Mode is enabled;
5. When FIPS Mode is disabled; and

6. When Factory Reset of module is selected.

There are no restrictions when plaintext secret and private cryptographic keys and CSPs can be zeroized, and all keys are capable of being zeroized. The zeroization methods for each key are shown in Table 12. The time it takes to zeroize a key is approximately one second. Keys cannot be recovered after zeroization, since the configuration is saved after the deletion, such that the persistent keys are removed from the disk and there is no means to recover them afterward. Ephemeral keys are lost when power to the module ceases. Using the factory reset service will wipe the entire configuration of the module, including all keys and CSPs. If invoked, an operator will have to begin the configuration process again and create new operator accounts.

Note: The Cryptographic Officer shall retain control of the module while zeroization is in process.

2 Cryptographic Functionality

The module implements FIPS Approved, non-FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 4, 5, 6, 7, 8 and 9 below.

Table 10 summarizes the high-level protocol algorithm support.

2.1 Approved Algorithms

References to standards are given in square bracket [ ]; see the References table.

Table 4 – Approved Algorithms – Gigamon Linux-Based Cryptographic Library

CAVP Cert.	Algorithm	Mode	Description	Functions
5554	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		ECB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CFB1 [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CFB8 [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CFB128 [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CMAC [38B]	Key Sizes: 128, 192, 256	Generate, Verify
		CCM [38C]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
3702	HMAC [198]	SHA-1	KS < BS KS = BS KS > BS MAC: 10 12 16 20	Message Authentication
		SHA-224	KS < BS KS = BS KS > BS MAC: 14 16 20 24 28	
		SHA-256	KS < BS KS = BS KS > BS MAC: 16 24 32	
		SHA-384	KS < BS KS = BS KS > BS MAC: 24 32 40 48	
		SHA-512	KS < BS KS = BS KS > BS MAC: 32 40 48 56 64	
4457	SHS [180]	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 (All Byte Oriented)		Message Digest Generation

2795	Triple-DES [67][1]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt
		TCFB1 [38A]	Key Size: 192	Encrypt, Decrypt
		TCFB8 [38A]	Key Size: 192	Encrypt, Decrypt
		TCFB64 [38A]	Key Size: 192	Encrypt, Decrypt
		TOFB [38A]	Key Size: 192	Encrypt, Decrypt
		TECB [38A]	Key Size: 192	Encrypt, Decrypt
		CMAC [38B]	Key Size: 192	Verification Using 3-Key
1991[2]	CVL	[56A]	ECC CDH Primitive (Section 5.7.1.2) Component: Curves tested: P-224 P-256 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 KAS ECC: Domain Parameter Generation, Domain Parameter Validation, Full Public Key Validation, Key Pair Generation EC: Curve: P-256, SHA: SHA-256 ED: Curve: P-384, SHA: SHA-384 EE: Curve: P-521, SHA: SHA-512	Key Agreement

[1] As per the SP 800-67rev1 Transition specified in the CMVP Implementation Guidance, please be advised that this module shall not be used to perform more than 2^20 encryptions with the same Triple-DES key when generated as part of a recognized IETF protocol. If the key is not generated as part of a recognized IETF protocol, then the limit of 2^16 encryptions shall apply.

[2] Note: Not all modes/key lengths specified in the CAVP certificate are used by the module, Specifically KAS-FFC is not used by the module

C1325	CVL	[800-135]	SSH	SSH Key Derivation Component
2209	DRBG [90A]	Hash	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	Random Number Generation Symmetric Key Generation
		HMAC	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512	
		CTR	AES-128, AES-192 and AES-256	
1428	DSA [186-4]	PQG Generation	L= 2048, 3072 N= 224, 256 SHA = 224, 256, 384 and 512 *(**Note1**: N= 224 is only approved for L= 2048)* *(**Note2**: SHA-224 is only approved for L=2048 N=224.)*	Digital Signature Operations
		PQG Verification	L= 1024, 2048, 3072 N= 160, 224, 256 SHA = 1,224, 256, 384 and 512 *(**Note1**: SHA-1 is only approved for L= 1024)* *(**Note2**: SHA-224 is only approved for L= 1024 and L=2048)* *(**Note3:** N=160 is only approved for L=1024, N=224 is only approved for L=2048, N=256 is only approved for L=2048 and 3072)*	
		Key Pair	L= 2048, 3072 N= 224, 256 (**Note:** N=224 is only	

			approved for L=2048)	
		Signature Generation	L= 2048, 3072 N= 224, 256 SHA = 224, 256, 384 and 512 (**Note:** N=224 is only approved for L=2048)	
		Signature Verification	L= 1024, 2048, 3072 SHA=1,224, 256, 384, 512 N= 160, 224 and 256 (**Note:** N=160 is only approved for L=1024 and N=224 is only approved for L=2048)	
1497	ECDSA [186-4][3]	Key Pair	Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	Elliptic Curve Digital Signature Operations (The Module supports only NIST defined curves for use with ECDSA and ECDH.)
		Public Key Validation	Curves: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K- 571, P-224, P-256, P-384, P-521	
		Signature Generation	Curve/SHA pairs tested: P = 224, 256, 384 and 521 /w SHA-224, 256, 384 and 512. K = 233, 283, 409 and 571 /w SHA-224, 256, 384 and 512. B = 233, 283, 409 and 571 /w SHA-224, 256, 384 and 512.	

[3] ECDSA, B-163, K-163 and P-192 are non-Approved because the security strength they provide is less than the required 112 bits. SHA-1 is not to be used for signature generation.

		Signature Verification	Curve/SHA pairs tested: P = 224, 256, 384 and 521 /w SHA-1, 224, 256, 384 and 512. K = 233, 283, 409 and 571 /w SHA-1, 224, 256, 384 and 512. B = 233, 283, 409 and 571 /w SHA-1, 224, 256, 384 and 512.	
2984	RSA [186-2]	Signature Verification 9.31	Modulus lengths: 1024, 1536, 2048, 3072, 4096 SHAs: SHA-1, SHA-256, SHA-384, SHA-512	RSA Digital Signature Operations
		Signature Verification PKCS1.5	Modulus lengths: 1024, 1536, 2048, 3072, 4096 SHAs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
		Signature Verification PSS	Modulus lengths: 1024, 1536, 2048, 3072, 4096 SHAs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
2984	RSA [186-4]	Signature Generation 9.31	Mod 2048 SHA: SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-256, SHA-384, SHA-512	
		Signature Generation PKCS1.5	Mod 2048 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-224, SHA-256, SHA-384, SHA-512	
		Signature Generation PSS	Mod 2048: SHA-224: Salt Length: 0 SHA-256: Salt Length: 0 SHA-384: Salt Length: 0 SHA-512: Salt Length: 0 Mod 3072: SHA-224: Salt Length: 0 SHA-256: Salt Length: 0 SHA-384: Salt Length: 0 SHA-512: Salt Length: 0	

		Signature Verification 9.31	Mod 1024 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Mod 2048 SHA: SHA-1, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-1, SHA-256, SHA-384, SHA-512	
		Signature Verification PKCS1.5	Mod 1024 SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Mod 2048 SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	
		Signature Verification PSS	Mod 1024: SHA-1: Salt Length: 0 (bits) SHA-224: Salt Length: 0 (bits) SHA-256: Salt Length: 0 (bits) SHA-384: Salt Length: 0 (bits) SHA-512: Salt Length: 0 (bits) Mod 2048: SHA-1: Salt Length: 0 (bits) SHA-224: Salt Length: 0 (bits) SHA-256: Salt Length: 0 (bits) SHA-384: Salt Length: 0 (bits) SHA-512: Salt Length: 0 (bits) Mod 3072: SHA-1: Salt Length: 0 (bits) SHA-224: Salt Length: 0 (bits) SHA-256: Salt Length: 0 (bits) SHA-384: Salt Length: 0 (bits) SHA-512: Salt Length: 0 (bits)	

Table 4a – Vendor Affirmed Security Functions – Gigamon Linux-Based Cryptographic Library

CAVP Cert.	Algorithm	Mode	Description	Functions
N/A	CKG	NIST SP 800-133	Key generation using unmodified DRBG output	Symmetric & Asymmetric Key Generation (RSA key generation non-Approved)

Table 5 – Approved Algorithms – Cavium Hardware Libraries (CN7890)

CAVP Cert.	Algorithm	Mode	Description	Functions
819	DRBG [90A][4]	Counter	AES-256	Random Bit Generation
3301	AES [197][5]	CBC, ECB	128, 192, 256	Encrypt/Decrypt
2095	HMAC [198]	SHA-1	HMAC-SHA-1 Key Size = Block Size	Message Authentication, KDF Primitive
		SHA-224	HMAC-SHA-224 Key Size = Block Size	
		SHA-256	HMAC-SHA-256 Key Size = Block Size	
		SHA-384	HMAC-SHA-384 Key Size = Block Size	
		SHA-512	HMAC-SHA-512 Key Size = Block Size	
2737	SHS [180]	SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512		Message Digest Generation
1745	RSA [186-4]	Signature Generation PKCS1.5	Mod 2048 SHA: SHA-224, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-224, SHA-256, SHA-384, SHA-512	RSA Digital Signature Operations
		Signature Verification PKCS1.5	Mod 1024 SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Mod 2048 SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 Mod 3072 SHA: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	

[4] Note: Not all modes/key lengths specified in the CAVP certificate are used by the module,

[5] Note: Not all modes/key lengths specified in the CAVP certificate are used by the module.

Table 6 – Approved Algorithms – Cavium OpenSSL Library 1.1.1b (CN7890)

CAVP Cert.	Algorithm	Mode	Description	Functions
C1666	CVL	[800-56A]	ECC CDH: Primitive Curves: P-224, P-256, P-384, P-521	ECC CDH Primitive Component
C1666	CVL	[800-135]	TLS: Supports TLS 1.0/1.1 Supports TLS 1.2: SHA Functions: SHA-256	TLS Key Derivation Component
C1666	ECDSA[6] [186-4]	Key Pair	Curves: P-224, P- 256, P-384, P-521	Elliptic Curve Digital Signature Operations
		Public Key Validation	Curves: P-224, P-256, P-384, P-521	
		Signature Generation	Curve/SHA pairs tested: P = 224, 256, 384 and 521 /w SHA-224, 256, 384 and 512.	
		Signature Verification	Curve/SHA pairs tested: P = 224, 256, 384 and 521 /w SHA-1, 224, 256, 384 and 512.	

2.2 Allowed Algorithms

[6] ECDSA, P-192 is non-Approved because the security strength it provides is less than the required 112 bits. SHA-1 is not to be used for signature generation.

Table 7 – Allowed Cryptographic Functions

Algorithm	Caveat	Use	Library	CAVP Cert. #
Elliptic Curve Diffie-Hellman [IG] D.8	Provides between 112 and 256 bits of encryption strength.	key agreement; key establishment	Gigamon Linux Crypto Library 1.0	Cert. #1991 Cert. #C1325
Elliptic Curve Diffie-Hellman [IG] D.8	Provides between 112 and 256 bits of encryption strength.	key agreement; key establishment	Cavium OpenSSL 1.1.1b	Cert. #C1666

Table 7a – Entropy Sources

Algorithm	Use
NDRNG1	Underlying OS based NDRNG (Allowed in the Approved mode) provides at least 256 bits of entropy per second
NDRNG2	Internal Hardware Cavium based NDRNG (Allowed in the Approved mode) provides full entropy per call (if x bits are requested then the x bits have x bits of entropy)

Table 7b – other non-Approved algorithms

Algorithm	Use
AES-GCM 128,192,256	Only used in non-Approved mode for encryption/decryption of data
AES-XTS 128,256	Only used in non-Approved mode for encryption/decryption of data for storage applications only

The algorithms in Table 7b are not to be use in the Approved mode by policy. These two algorithms are not disabled when the module is in the Approved mode.

2.3 Protocols

Table 8 – Protocols Allowed and Disallowed in FIPS Mode

Protocol	Key Exchange	Auth	Ciphers	Integrity
SSH	EC Diffie-Hellman: P-224 P-256 P-384 P-521 (Allowed in the Approved mode) **SSH KDF:** *CMVP Cert. #C1325*	ECDSA	AES-128-CBC AES-256-CBC Triple-DES-CBC AES-128-CTR AES-256-CTR AES-192-CTR	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512

TLS HTTPS, FTPS, SMTP/S POP3/S	EC Diffie-Hellman: P-224 P-256 P-384 P-521 (Allowed in the Approved mode) **TLS KDF:** *CMVP Cert. #C1666*	ECDSA RSA	Triple-DES AES 128 AES 256	SHA-1 SHA-256 SHA-384
SCP	EC Diffie-Hellman: P-224 P-256 P-384 P-521 (Allowed in the Approved mode)	ECDSA RSA	Triple-DES AES 128 AES 256	SHA-1 SHA-256 SHA-384
SFTP	EC Diffie-Hellman: P-224 P-256 P-384 P-521 (Allowed in the Approved mode)	ECDSA RSA	Triple-DES AES 128 AES 256	SHA-1 SHA-256 SHA-384
TACACS+	Use of this TACACS+ protocol will cause the module to operate in a ***non-Approved mode***, due to its use of MD5.	HMAC-MD5	N/A	N/A
SNMP	Use of this SNMP protocol will cause the module to operate in a ***non-Approved mode***, due to its use of MD5 and DES.	MD5 SHA-1 DES AES	N/A	N/A
LDAP	Use of this SNMP protocol will cause the module to operate in a ***non-Approved mode***, due to its use of MD5.	HMAC-MD5	N/A	N/A
RADIUS	Use of this RADIUS protocol will cause the module to operate in a ***non-Approved mode***, due to its use of MD5.	MD5	N/A	N/A

No part of these protocols, other than the KDF, have been tested by the CAVP and CMVP. The SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In reference to the Protocols in Table 8 above: each column of options for a given protocol is independent and may be used in any viable combination.

2.4 **No Security Claimed but allowed protocols**

The module supports the following non-Approved but allowed protocols with no security claimed:

ARP, CDP, DHCP, DHCPv6, FTP, GRE (disabled in FIPS Mode), GTP (disabled in FIPS Mode), HTTP, IGMP, ICMP, ISL, IPv4, IPv6, LLDP, MPLS (disabled in FIPS Mode), NTP, PDP, SNMP, TCP, Telnet, TFTP and UDP

2.5 **Disallowed Algorithms**

These algorithms are non-Approved algorithms that are disabled when the module is operated in an Approved mode of operation. They are all available when the module is not configured to operate in the Approved mode.

- DES;
- IDEA;
- RC2;
- RC4;
- MD5;
- CAMELLIA128;
- CAMELLIA256;
- PSK;
- SEED;
- KRB5; and
- RSA (KeyGen) not compliant to FIPS 184-4

2.6 Critical Security Parameters

All CSPs and public keys used by the module are described in this section. The access type for each is specified as: ***R=Read, W=Write or D=Delete***.

Table 9 – Critical Security Parameters (CSPs)

Keys / CSPs	Storage	Origin	Method	Input	Output	Zeroization (RAM)	Zeroization (Disk)	Access
AES Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
Triple-DES Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
RSA Public Key	RAM (Active) Disk (Persistent)	Non-compliant	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
RSA Private Key	RAM (Active) Disk (Persistent)	Non-compliant	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD

DSA Public Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
DSA Private Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
HMAC Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
NDRNG1 entropy	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
NDRNG2 entropy	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	API Call	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
ECDSA Private Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD

ECDSA Public Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
EC Diffie-Hellman Public Components	RAM (Active) Disk (Persistent)	Internally Generated using FIPS 186-4 methods, Established	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
EC Diffie-Hellman Private Components	RAM (Active) Disk (Persistent)	Internally Generated using FIPS 186-4 methods	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
HMAC DRBG Entropy	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
HMAC DRBG V Value (Seed Length)	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
HMAC DRBG Key	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode	CO: RWD U: RWD

						• Mode • Factory Reset	• Factory Reset	
HMAC DRBG init_seed	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
Hash DRBG Entropy	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
Hash DRBG V Value (Seed Length)	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
Hash DRBG C Value	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
Hash DRBG init_seed	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
CTR DRBG Entropy	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD

						• Factory Reset		
CTR DRBG V Value (Seed Length)	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
CTR DRBG Key Value	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
CTR DRBG init_seed	RAM (Active) Disk (Persistent)	Internally Generated	Plaintext	None	None	• Reboot • Session End • User Deletes Key • Disable/Enable FIPS Mode • Factory Reset	• User Deletes Key/Saves Config • Disable/Enable FIPS Mode • Factory Reset	CO: RWD U: RWD
TLS premaster secret	RAM (Active)	Internally Generated/ Established	Plaintext	None	None	• Destroyed after master secret is calculated.	N/A	CO: RWD U: RWD
TLS master secret	RAM	Internally Generated/ Established	Plaintext	None	None	• Destroyed when SSL session keys are derived or stored in session cache which will be power cycle cleansed later.	N/A	CO: RWD U: RWD
TLS session keys	RAM	Internally Generated/ Established	Plaintext	None	None	• Destroyed when SSL session is closed.	N/A	CO: RWD U: RWD
Crypto-Officer Password	Disk (Persistent)	Entered	Plaintext	API Call	None	• N/A	• Destroyed upon deletion of account or factory reset.	CO: RWD U: RWD

User Password	Disk (Persistent)	Entered	Plaintext	API Call	None	• N/A	• Destroyed upon deletion of account or factory reset.	CO: RWD U: RWD

3 Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

The module supports two roles: Cryptographic Officer (CO) and User. The module supports concurrent operators but does not support a maintenance role or bypass capability. The module enforces the separation of roles using identity-based operator authentication.

The Crypto-Officer can create additional operators which have either “regular” or “monitor” capabilities, and thus the roles in the module are Admin (Crypto-Officer), Regular User (User) and Monitor User (User).

3.2 Authentication Methods

The module implements two methods of authentication. The first method involves Identity-Based authentication, in the form of username and password. The Crypto-Officer can change the password lengths of the module, however the lower threshold enforced by the module is 8-characters. The password length can go as high as 30 characters. Additionally, the module enforces the following password requirements:

- At least 1 numeric character;
- At least 1 upper case character;
- At least 1 lower case character; and
- At least 1 special character.

The chance of a random password attempt succeeding is 94^8 which is consistent with the number (94) of keyboard selections on a standard US keyboard, as applied to an 8-character password, which is the minimum allowed. The odds of randomly guessing the password supersedes the FIPS 140-2 requirement of 1 in 1,000,000.

The module also ensures that the probability is less than 1 in 100,000 that a random attempt will succeed, or a false acceptance will occur within one minute. The module locks out the login process for 15 seconds after 5 incorrect login attempts. Assuming the attacker could make one attempt per second, they would reach the lockout threshold after 5 seconds, resulting in a 15 second delay. This process could only be repeated 3 times within 60 seconds; therefore, the attacker could realistically only make 15 attempts within one minute. This equates to 15 in 94^8 attempts.

When a user logs in, the feedback mechanism does not provide information that could be used to guess or determine the authentication data and the strength of the authentication is not weakened.

For the SSH session, the module uses ECDSA public/private key authentication. The odds of guessing the value of the private key would well exceed the threshold of 1 in 1,000,000 or 1 in 100,000 within a minute, since guessing the value of the key would be equivalent to guessing a value of $2^{112.}$.The user creates an ECDSA public/private key pair using one of the Approved elliptic curves. The smallest size of the elliptic curves is p-224 which has a security strength of 112 bits. Assuming 512 attempts per second could be made (an overestimate by a wide margin) the probability of guessing the key pair in a 1 minute period is 1 in 60*512/2^112 which is smaller than 1 in 64*512/2^112 = 1 in 2^(112-9-6) = 1 in 2^97 which easily exceeds the requirement of 1 in 100,000.

The implemented ECDSA uses the NIST recommended curves (specified in Table 4); which effectively provide encryption strengths in the range of 112, 128, 192 and >256 respectively. Please see [NIST 186-4, Table D-1] for more information.

3.3 Services

All services implemented by the module are listed in the tables below. Table 15 lists the access to CSPs by each service.

Table 10 – Approved Services

Service	Description	CO (admin)	User (regular)	User (monitor)
Status	Show status	X	X	X
Module Self-Tests	Self-Tests performed automatically	X		
Zeroize	Destroy all CSPs	X		
SSH Connect	Initiate SSH connection for SSH monitoring and control (CLI)	X	X	
Console Access	Console monitoring and control (CLI)	X	X	
Factory Reset	Reset module to factory defaults	X		
Backup/Restore Configuration File	Write Mem/Config Switch-to	X	X	
Firmware Upgrade	Install Firmware Image	X		
Logging controls	Show Log/Log File Rotation	X	X	X (View Only)
Configure	Configure module parameters	X		
Account Controls	Creation and Administration of users and roles	X		
Traffic Operation	Creating traffic through data path	X		
Run On-Demand Self-Tests	Execute self-test on demand (power cycle)	X		
Configure Security	Configure Security Related Parameters Including Key Chain Password	X		
Group Controls	(RBAC/AAA Control)	X		
Establish Keys	Key establishment methodology (EC Diffie-Hellman)	X		
Encrypt/Decrypt	Encrypt/Decrypt operation (invoked as part of protocols)	X		
Generate Keys	Key generation service DRBG	X		
Signature Generation	Signature generation service (RSA)	X		

Signature Verification	Verification signature service (DSA, RSA, ECDSA)	X		
TLS Connect	Connecting to the module (CC) over TLS	X		
SCP Connect	Copy image and log configuration files through secure channel	X	X	
SFTP Connect	Copy image and log configuration files through secure channel	X	X	

3.4 Non-Approved Services

The following services are available in the non-Approved mode of operation. These services are generally the same as the Approved services, with the exception that they may utilize cryptography which the module disallows in the Approved mode.

Table 11 – non-Approved Services

Service	Description	CO (admin)	User (regular)	User (monitor)
Status	Show status	X	X	X
Zeroize	Destroy all CSPs	X		
SSH Connect	Initiate SSH connection for SSH monitoring and control (CLI)	X	X	
Console Access	Console monitoring and control (CLI)	X	X	
Factory Reset	Reset module to factory defaults	X		
Backup/Restore Configuration File	Write Mem/Config Switch-to	X	X	
Firmware Upgrade	Install Firmware Image	X		
Logging controls	Show Log/Log File Rotation	X	X	X (View Only)
Configure	Configure modules parameters	X		
Account Controls	Creation and Administration of users and roles	X		
Traffic Operation	Creating traffic through data path	X		
Run On-Demand Self-Tests	Execute self-test on demand (power cycle)	X		
Configure Security	Configure Security Related Parameters Including Key Chain Password	X		
Group Controls	(RBAC/AAA Control)	X		
Establish Keys	Key establishment methodology (EC Diffie-Hellman , RSA)	X		
Encrypt/Decrypt	Encrypt/Decrypt operation	X		
Generate Keys	Key generation service DRBG	X		

Signature Generation	Signature generation service (RSA)	X		
Signature Verification	Verification signature service (DSA, RSA, ECDSA)	X		
Traffic Operation	Creating traffic through data path	X		
Run On-Demand Self-Tests	Execute self-test on demand (power cycle)	X		
Configure Security	Configure Security Related Parameters Including Key Chain Password	X		
TACACS+	Authentication Server to all roles	X	X	X
SNMP	Configuring SNMP to all roles	X	X	
LDAP	Authentication Server to all roles	X	X	X
RADIUS	Authentication Server to all roles	X	X	X

Service	CSPs																						
	AES Key	Triple-DES Key	RSA Public Key	RSA Private Key	DSA Public Key	DSA Private Key	HMAC Key	NDRNG1 entropy	NDRNG2 entropy	ECDSA Private Key	ECDSA Public Key	EC Diffie-Hellman Public Components	EC Diffie-Hellman Private Components	DRBG Entropy	DRBG V Value (HMAC & CTR DRBG)	DRBG Key Value (HMAC & CTR DRBG)	DRBG init_seed (All DRBG types)	DRBG C Value (Hash DRBG)	TLS premaster secret	TLS master secret	TLS session keys	CO-Password	User-Password
Traffic Operation	--	--	RWG	GR	--	--	GR	GZR	GZR	GR	GWR	GR	GR	GR	--	GR	GR	--	GR	GR	GR	--	--
Configure Security	REWG	--	GWR	GW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	GW	GW
Status	--	--	R	--	--	--	--	--	--	--	R	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z		
SSH Connect	--	--	--	--	--	--	--	--	--	RWG	RWG	--	--	--	--	--	--	--	--	--	--	RE	RE
Console Access	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	RE	RE
Factory Reset	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZ	WZG	WZ
Backup/Restore Configuration File	RW	--	RW	RW	--	--	--	--	--	RW	RW	--	--	--	--	--	--	--	--	--	--	RW	RW

Firmware Upgrade	--	--	--	--	--	--	R	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Logging controls	--	--	--	--	--	--	R	--	--	--	R	--	--	--	--	--	--	--	--	--	--	--	--
Group Controls	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Establish Keys	RW	--	RW	RW	--	--	--	--	--	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW	RW	--	--	--
Encrypt/Decrypt	RW	RW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Generate Keys	G	G	G	G	--	--	G	G	G	G	G	G	G	G	G	G	G	G	G	G	G	--	--
Signature Generation	--	--	--	W	--	--	--	--	--	W	--	--	W	--	--	--	--	--	--	--	--	--	--
Signature Verification	--	--	R	--	--	--	--	--	--	--	R	R	--	--	--	--	--	--	--	--	--	--	--
Module Self-Tests (Automatic POST)	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Run On-Demand Self-Tests	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
TLS Connect	--	--	--	--	--	--	--	--	--	RW	RW	RW	RW	--	--	--	--	--	RW	RW	RW	--	--
SCP Connect	--	--	RW	RW	RW	RW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
SFTP Connect	--	--	RW	RW	RW	RW	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Account Controls	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	RW	RW

Table 12 – CSP Access Rights within Services

Legend

G = Generate: The module generates the CSP
R = Read: The CSP is read from the module (e.g. the CSP is output)
E = Execute: The module executes using the CSP
W = Write: The CSP is updated or written to the module
Z = Zeroize: The module zeroizes the CSP.

4 Self-tests

Each time the module is powered up, it tests that the cryptographic algorithms still operate correctly, and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module. When power is applied to the module, it requires no operator intervention to execute the power-up self-tests. The firmware integrity test located on the CC card side, verifies all firmware components used within the module. This includes all files on both the CC card and the GS card. If no error message is displayed on the console after the FIPS Approved mode has been invoked and after self-tests have successfully executed, the status of the module is considered to be operating in the FIPS Approved mode.

On power up or reset, the module performs the self-tests described below. All self-tests must be completed successfully prior to any other use of cryptography by the module. If one of the tests fails, the module enters the Critical Failure error state. An operator may attempt to clear a self-test error by power-cycling the module, however a persistent error in the firmware integrity test or known answer tests will likely require the operator to contact Gigamon for service.

The module performs the following power-up self-tests:

Table 13 – Module Self-Tests

Algorithm	Card	CAVP Library	CAVP Cert. #	Test Type
DRBG Health	**GS**	**Cavium Hardware**	Cert. #819	Power-Up – Critical
CTR_DRBG	**GS**	**Cavium Hardware**	Cert. #819	Power-Up KAT
Entropy Check	**GS**	**Cavium Hardware**	Cert. #819	Conditional - CRNGT
AES	**GS**	**Cavium Hardware**	Cert. #3301	Power-Up KAT (E/D)
SHA-1	**GS**	**Cavium Hardware**	Cert. #2737	Power-Up KAT
SHA-224	**GS**	**Cavium Hardware**	Cert. #2737	Power-Up KAT
SHA-256	**GS**	**Cavium Hardware**	Cert. #2737	Power-Up KAT
SHA-384	**GS**	**Cavium Hardware**	Cert. #2737	Power-Up KAT
SHA-512	**GS**	**Cavium Hardware**	Cert. #2737	Power-Up KAT
HMAC-SHA-1	**GS**	**Cavium Hardware**	Cert. #2095	Power-Up KAT
HMAC-SHA-224	**GS**	**Cavium Hardware**	Cert. #2095	Power-Up KAT
HMAC-SHA-256	**GS**	**Cavium Hardware**	Cert. #2095	Power-Up KAT
HMAC-SHA-384	**GS**	**Cavium Hardware**	Cert. #2095	Power-Up KAT
HMAC-SHA-512	**GS**	**Cavium Hardware**	Cert. #2095	Power-Up KAT
RSA	**GS**	**Cavium Hardware**	Cert. #1745	Power-Up KAT
ECDSA	**GS**	**Cavium SSL Library**	Cert. #C1666	Power-Up KAT
ECDSA	**GS**	**Cavium SSL Library**	Cert. #C1666	Conditional - PWCT
EC Diffie-Hellman	**GS**	**Cavium SSL Library**	Cert. #C1666	Power-Up KAT
SHA-256	**CC**	**Gigamon Linux Lib**	Cert. #4457	Power-Up - FW Integrity
SHA-1	**CC**	**Gigamon Linux Lib**	Cert. #4457	Power-Up KAT
SHA-224	**CC**	**Gigamon Linux Lib**	Cert. #4457	Power-Up KAT
SHA-256	**CC**	**Gigamon Linux Lib**	Cert. #4457	Power-Up KAT
SHA-384	**CC**	**Gigamon Linux Lib**	Cert. #4457	Power-Up KAT
SHA-512	**CC**	**Gigamon Linux Lib**	Cert. #4457	Power-Up KAT
HMAC-SHA-1	**CC**	**Gigamon Linux Lib**	Cert. #3702	Power-Up KAT

HMAC-SHA-224	**CC**	**Gigamon Linux Lib**	Cert. #3702	Power-Up KAT
HMAC-SHA-256	**CC**	**Gigamon Linux Lib**	Cert. #3702	Power-Up KAT
HMAC-SHA-384	**CC**	**Gigamon Linux Lib**	Cert. #3702	Power-Up KAT
HMAC-SHA-512	**CC**	**Gigamon Linux Lib**	Cert. #3702	Power-Up KAT
AES	**CC**	**Gigamon Linux Lib**	Cert. #5554	Power-Up KAT (E/D)
AES-CCM	**CC**	**Gigamon Linux Lib**	Cert. #5554	Power-Up KAT
AES-CMAC	**CC**	**Gigamon Linux Lib**	Cert. #5554	Power-Up KAT
Triple-DES	**CC**	**Gigamon Linux Lib**	Cert. #2795	Power-Up KAT (E/D)
Triple-DES CMAC	**CC**	**Gigamon Linux Lib**	Cert. #2785	Power-Up KAT
RSA	**CC**	**Gigamon Linux Lib**	Cert. #2984	Power-Up KAT
RSA	**CC**	**Gigamon Linux Lib**	Cert. #2984	Conditional - PWCT
DSA	**CC**	**Gigamon Linux Lib**	Cert. #1428	Power-Up KAT
DSA	**CC**	**Gigamon Linux Lib**	Cert. #1428	Conditional - PWCT
CTR_DRBG	**CC**	**Gigamon Linux Lib**	Cert. #2209	Power-Up KAT
HASH_DRBG	**CC**	**Gigamon Linux Lib**	Cert. #2209	Power-Up KAT
HMAC_DRBG	**CC**	**Gigamon Linux Lib**	Cert. #2209	Power-Up KAT
Entropy Check	**CC**	**Gigamon Linux Lib**	Cert. #2209	Conditional - CRNGT
DRBG Health	**CC**	**Gigamon Linux Lib**	Cert. #2209	Power-Up – Critical
ECDSA	**CC**	**Gigamon Linux Lib**	Cert. #1497	Power-Up KAT
ECDSA	**CC**	**Gigamon Linux Lib**	Cert. #1497	Conditional - PWCT
EC Diffie-Hellman	**CC**	**Gigamon Linux Lib**	Cert. #1991	Power-Up KAT
Firmware Load Test (HMAC-SHA-256)	**CC**	**Gigamon Linux Lib**	Cert. #3702	Conditional Load Test

**__GS__=Implemented on GigaSMART Card | __CC__=Implemented on Controller Card.*

5 Physical Security Policy

The module's physical embodiment is that of a multi-chip standalone device that meets Level 2 Physical Security requirements. The module is completely enclosed in a hard metal enclosure and maintains opacity. The tamper-evident seals shall be installed for the module to operate in a FIPS mode of operation. Tamper-evident seals allow the operator to tell if the enclosure has been breached. These seals are not factory-installed and must be applied by the Cryptographic Officer. Extra seals are provided with the original kit to replace any damaged seals. Additional kits can be ordered directly from Gigamon using SKU: ACC-HC0-FIPS. Inquiries for procurement of additional tamper seals should be sent to sales@gigamon.com.

The Cryptographic Officer is responsible for securing and having control at all times of any unused seals and the direct control and observation of any changes to the module such as reconfigurations where the tamper-evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

Table 14 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper seals, opaque metal enclosure.	Periodic inspection schedule to be determined by Crypto-Officer.	Seals should be free of any tamper evidence.

If the Cryptographic Officer observes tamper evidence, it shall be assumed that the device has been compromised. The Cryptographic Officer shall retain control of the module and perform Zeroization of the module's CSPs by following the steps in Section 1.3 of the Security Policy and then follow the steps in Section 1.2 to place the module back into a FIPS-Approved mode of operation.

5.1 General Tamper Evident Label Placement and Application Instructions

For instructions regarding the placement of the tamper seals and the requisite preparation requirements, please see Appendix A of this document.

6 Security Rules and Guidance

The module design corresponds to the security rules below. The term *must* in this context specifically refers to a requirement for correct usage of the module in the Approved mode; all other statements indicate a security rule implemented by the module.

1. The module clears previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during key generation, self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not output intermediate key values.
10. The cryptographic officer must retain control of the module while zeroization is in process.
11. Per SP800-67 rev1, the User is responsible for ensuring the module's limit to 2^{20} encryptions with the same Triple-DES key.
12. Gigamon uses a bonded courier for the shipment of the hardware module to the customer. Their trusted couriers include Fedex, Expeditors and MainFreight. The latest firmware can be downloaded from the Gigamon website.
13. Using AES-XTS will put the module into the non-Approved mode
14. Using AES_GCM will put the module into the non-Approved mode

7 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – 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*
[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.
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

[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*
[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*
[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.

Table 16 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
E/D	Encrypt/Decrypt
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
MD5	Message Digest 5
RE	Routing Engine
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SHA	Secure Hash Algorithms
SSH	Secure Shell
Triple-DES	Triple - Data Encryption Standard

8 Appendix A – Tamper Seal Preparation and Placement